

# IP Services and Security Configuration Guide

---

## SmartEdge OS

Release 5.0.3

Part Number 220-0587-01



**Corporate Headquarters**  
Redback Networks Inc.  
300 Holger Way  
San Jose, CA 95134-1362  
USA  
<http://www.redback.com>  
Tel: +1 408 750 5000

---

© 1998–2005, Redback Networks Inc. All rights reserved.

Redback and SmartEdge are trademarks registered at the U.S. Patent & Trademark Office and in other countries. AOS, NetOp, SMS, and User Intelligent Networks are trademarks or service marks of Redback Networks Inc. All other products or services mentioned are the trademarks, service marks, registered trademarks or registered service marks of their respective owners. All rights in copyright are reserved to the copyright owner. Company and product names are trademarks or registered trademarks of their respective owners. Neither the name of any third party software developer nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission of such third party.

## Rights and Restrictions

All statements, specifications, recommendations, and technical information contained are current or planned as of the date of publication of this document. They are reliable as of the time of this writing and are presented without warranty of any kind, expressed or implied. In an effort to continuously improve the product and add features, Redback Networks Inc. ("Redback") reserves the right to change any specifications contained in this document without prior notice of any kind.

Redback shall not be liable for technical or editorial errors or omissions which may occur in this document. Redback shall not be liable for any indirect, special, incidental or consequential damages resulting from the furnishing, performance, or use of this document.

## Third Party Software

The following third party software may be included with this Software and is subject to the following terms and conditions:

The OpenLDAP Version 2.0.1 © 1999 The OpenLDAP Foundation; OpenSymphony Software License, Version 1.1 2001-2004 © The OpenSymphony Group; TOAD © 2004 Quest Software, Inc.; NuSOAP Web Services Toolkit for PHP © 2002 NuSphere Corporation; The PHP License, versions 2.02 and 3.0 © 1999 - 2002 The PHP Group; The OpenSSL toolkit Copyright © 1998-2003 The OpenSSL Project; Apache HTTP © 2000 The Apache Software Foundation; Java © 2003 Sun Microsystems, Inc.; ISC Dhcpd 3.0pl2 © 1995, 1996, 1997, 1998, 1999 Internet Software Consortium - DHCP; IpFilter © 2003 Darren Reed; Perl Kit © 1989-1999 Larry Wall; SNMP Monolithic Agent © 2002 SNMP Research International, Inc.; VxWorks © 1984-2000, Wind River Systems, Inc.; Point-to-Point Protocol (PPP) © 1989, Carnegie-Mellon University; Dynamic Host Configuration Protocol (DHCP) © 1997, 1998 The Internet Software Consortium; portions of the Redback SmartEdge Operating System use cryptographic software written by Eric Young (eay@cryptsoft.com); Redback adaptation and implementation of the UDP and TCP protocols developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. © 1982, 1986, 1988, 1990, 1993, 1995 The Regents of the University of California. All advertising materials mentioning features or use of this Software must display the following acknowledgment: "This product includes software developed by the University of California, Berkeley and its contributors."

This Software includes software developed by Sun Microsystems, Inc., Internet Software Consortium, Larry Wall, the Apache Software Foundation (<http://www.apache.org/>) and their contributors. Such software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. LICENSORS AND ITS CONTRIBUTORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL LICENSOR OR ITS CONTRIBUTORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF THE LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>. Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. The portions of this Software developed by Larry Wall may be distributed and are subject to the GNU General Public License as published by the Free Software Foundation.

## FCC Notice

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

### 1. MODIFICATIONS

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Redback could void the user's authority to operate the equipment.

### 2. CABLES

Connection to this device must be made with shielded cables with metallic RFI/EMI connector hoods to maintain compliance with FCC Rules and Regulations. (This statement only applies to copper cables, Ethernet, DS-3, E1, T1, and so forth. It does not apply to fiber cables.)

### 3. POWER CORD SET REQUIREMENTS

The power cord set used with the System must meet the requirements of the country, whether it is 100-120 or 220-264 VAC. For the U.S. and Canada, the cord set must be UL Listed and CSA Certified and suitable for the input current of the system.

For DC-powered systems, the installation instructions need to be followed.

---

---

## VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## European Community Mark



The marking on this product signifies that it meets all relevant European Union directives.

## Safety Notices

### 1. Laser Equipment:

**CAUTION!** Use of controls or adjustments of performance or procedures other than those specified herein may result in hazardous radiation exposure.

**Class 1 Laser Product**—Product is certified by the manufacturer to comply with DHHS Rule 21 Subchapter J.

**CAUTION!** Invisible laser radiation when an optical interface is open.

### 2. Lithium Battery Warnings:

It is recommended that, when required, Redback replace the lithium battery.

**WARNING!** Do not mutilate, puncture, or dispose of batteries in fire. The batteries can burst or explode, releasing hazardous chemicals. Discard used batteries according to the manufacturer's instructions and in accordance with your local regulations.

Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer's instructions.

**VARNING** Explosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

**ADVARSEL!** Lithiumbatteri—Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage til leverandøren.

**VARIOTUS** Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan valmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mukaisesti.

**ADVARSEL** Eksplosjonsfare ved feilaktig skifte av batteri. Benytt samme batteritype eller en tilsvarende type anbefalt av apparatfabrikanten. Brukte batterier kasseres i henhold til fabrikantens instruksjoner.

**WAARSCHUWING!** Bij dit produkt zijn batterijen geleverd. Wanneer deze leeg zijn, moet u ze niet weggooien maar inleveren als KCA.

---

---

---

# Contents

---

|                                    |       |
|------------------------------------|-------|
| <b>About This Guide</b>            | xix   |
| Related Publications               | xix   |
| Intended Audience                  | xxi   |
| Organization                       | xxi   |
| Conventions                        | xxi   |
| Command Modes and Privilege Levels | xxii  |
| Command Syntax                     | xxii  |
| Examples                           | xxiii |
| Task Tables                        | xxiv  |
| Online Navigation Aids             | xxiv  |
| Ordering Documentation             | xxiv  |

## Part 1: Introduction

---

|                                            |     |
|--------------------------------------------|-----|
| <b>Chapter 1: Overview</b>                 | 1-1 |
| SmartEdge OS Architecture                  | 1-1 |
| IP Protocols                               | 1-3 |
| Address Resolution Protocol                | 1-3 |
| Neighbor Discovery Protocol                | 1-3 |
| Dynamic Host Configuration Protocol        | 1-4 |
| Network Time Protocol                      | 1-4 |
| IP Services                                | 1-4 |
| Domain Name System                         | 1-5 |
| HTTP Redirect                              | 1-5 |
| Lawful Intercept                           | 1-5 |
| Access Control Lists                       | 1-5 |
| IP ACLs                                    | 1-5 |
| Policy ACLs                                | 1-5 |
| Conditional ACLs                           | 1-6 |
| IP Service Policies                        | 1-6 |
| Forward Policies                           | 1-6 |
| Network Address Translation Policies       | 1-6 |
| Service Policies                           | 1-6 |
| Quality of Service                         | 1-6 |
| Classification, Marking, and Rate-Limiting | 1-7 |
| Priority Groups                            | 1-7 |
| Policy Access Control Lists                | 1-7 |
| QoS Policing and Metering Policies         | 1-7 |

|                                                             |      |
|-------------------------------------------------------------|------|
| Scheduling .....                                            | 1-7  |
| Queue Maps .....                                            | 1-8  |
| Priority Queuing .....                                      | 1-8  |
| Enhanced Deficit Round Robin .....                          | 1-8  |
| Asynchronous Transfer Mode Weighted-Fair Queuing .....      | 1-8  |
| Priority Weighted-Fair Queuing .....                        | 1-8  |
| Hierarchical Scheduling .....                               | 1-9  |
| Hierarchical Nodes and Node Groups .....                    | 1-9  |
| Congestion Management and Avoidance .....                   | 1-9  |
| Security .....                                              | 1-10 |
| Authentication, Authorization, and Accounting .....         | 1-10 |
| Remote Authentication Dial-In User Service .....            | 1-10 |
| Terminal Access Controller Access Control System Plus ..... | 1-11 |
| Key Chains .....                                            | 1-11 |
| Command Mode Hierarchy .....                                | 1-11 |

---

## Part 2: IP Service Protocols

---

|                                                                  |      |
|------------------------------------------------------------------|------|
| <b>Chapter 2: ARP Configuration</b> .....                        | 2-1  |
| Overview .....                                                   | 2-1  |
| Configuration Tasks .....                                        | 2-1  |
| Enable ARP .....                                                 | 2-2  |
| Enable Secured ARP (Optional) .....                              | 2-2  |
| Enable Proxy ARP (Optional) .....                                | 2-2  |
| Configure Static Entries in the ARP Table (Optional) .....       | 2-3  |
| Configure the Automatic Deletion of ARP Entries (Optional) ..... | 2-3  |
| Set a Maximum Number of Incomplete ARP Entries (Optional) .....  | 2-3  |
| Configuration Examples .....                                     | 2-4  |
| Command Descriptions .....                                       | 2-4  |
| ip arp .....                                                     | 2-5  |
| ip arp arpa .....                                                | 2-6  |
| ip arp delete-expired .....                                      | 2-7  |
| ip arp maximum incomplete-entries .....                          | 2-8  |
| ip arp proxy-arp .....                                           | 2-9  |
| ip arp secured-arp .....                                         | 2-11 |
| ip arp timeout .....                                             | 2-13 |
| ip subscriber arp .....                                          | 2-15 |
| <b>Chapter 3: ND Configuration</b> .....                         | 3-1  |
| Overview .....                                                   | 3-1  |
| Configuration Tasks .....                                        | 3-2  |
| Configuration Examples .....                                     | 3-4  |
| Command Descriptions .....                                       | 3-4  |
| interface .....                                                  | 3-5  |
| neighbor .....                                                   | 3-7  |
| ns-interval .....                                                | 3-8  |
| preferred-lifetime .....                                         | 3-10 |
| prefix .....                                                     | 3-12 |
| ra .....                                                         | 3-14 |
| reachable-time .....                                             | 3-16 |
| router nd .....                                                  | 3-18 |
| valid-lifetime .....                                             | 3-19 |

---

|                                                       |         |
|-------------------------------------------------------|---------|
| <b>Chapter 4: NTP Configuration</b>                   | 4-1     |
| Overview                                              | 4-1     |
| Configuration Tasks                                   | 4-2     |
| Configure the NTP Server IP Address                   | 4-2     |
| Configure NTP Peer Associations (Optional)            | 4-2     |
| Configure Slowsync (Optional)                         | 4-2     |
| Configuration Examples                                | 4-3     |
| Command Descriptions                                  | 4-3     |
| ntp mode                                              | 4-4     |
| ntp peer                                              | 4-5     |
| ntp server                                            | 4-7     |
| slowsync                                              | 4-9     |
| <br><b>Chapter 5: DHCP Configuration</b>              | <br>5-1 |
| Overview                                              | 5-1     |
| Configuration Tasks                                   | 5-2     |
| Configure an Internal DHCP Server                     | 5-3     |
| Configure an External DHCP Server                     | 5-4     |
| Configure a Context for an External DHCP Server       | 5-5     |
| Configure an Interface for an External DHCP Server    | 5-5     |
| Configure Subscriber Hosts for DHCP Address Functions | 5-6     |
| Configuration Examples                                | 5-6     |
| DHCP Internal Server                                  | 5-6     |
| DHCP Proxy and Maximum Address Support                | 5-7     |
| Subscriber Bindings to DHCP Interfaces                | 5-8     |
| Using Local Authentication                            | 5-8     |
| Using RADIUS Authentication                           | 5-12    |
| DHCP Proxy Through Dynamic Subscriber Bindings        | 5-15    |
| DHCP Proxy Through Static Interface Bindings          | 5-17    |
| DHCP Proxy Through RADIUS                             | 5-18    |
| Loopback Interface as DHCP Source Address             | 5-19    |
| Command Descriptions                                  | 5-20    |
| bootp-filename                                        | 5-21    |
| bootp-siaddr                                          | 5-22    |
| default-lease-time                                    | 5-23    |
| dhcp max-addr                                         | 5-24    |
| dhcp proxy                                            | 5-26    |
| dhcp relay                                            | 5-28    |
| dhcp relay option                                     | 5-30    |
| dhcp relay server                                     | 5-32    |
| dhcp relay server retries                             | 5-34    |
| dhcp relay suppress-nak                               | 5-35    |
| dhcp server                                           | 5-36    |
| dhcp server policy                                    | 5-38    |
| forward-all                                           | 5-39    |
| ip interface                                          | 5-40    |
| mac-address                                           | 5-42    |
| max-hops                                              | 5-43    |
| max-lease-time                                        | 5-44    |
| min-wait                                              | 5-45    |
| offer-lease-time                                      | 5-46    |
| option                                                | 5-47    |
| option-82                                             | 5-53    |
| range                                                 | 5-55    |

|                       |      |
|-----------------------|------|
| server-group .....    | 5-56 |
| standby .....         | 5-57 |
| subnet .....          | 5-58 |
| user-class-id .....   | 5-60 |
| vendor-class .....    | 5-62 |
| vendor-class-id ..... | 5-64 |

---

## Part 3: IP Services

---

|                                                                      |      |
|----------------------------------------------------------------------|------|
| <b>Chapter 6: DNS Configuration</b> .....                            | 6-1  |
| Overview .....                                                       | 6-1  |
| Configuration Tasks .....                                            | 6-2  |
| Configure DNS .....                                                  | 6-2  |
| Enable DNS to Establish Subscriber Sessions (Optional) .....         | 6-2  |
| Configure Static Hostname-to-IP Address Mappings (Optional) .....    | 6-3  |
| Configuration Examples .....                                         | 6-3  |
| Command Descriptions .....                                           | 6-3  |
| dns .....                                                            | 6-4  |
| ip domain-lookup .....                                               | 6-5  |
| ip domain-name .....                                                 | 6-6  |
| ip host .....                                                        | 6-7  |
| ip name-servers .....                                                | 6-8  |
| ipv6 host .....                                                      | 6-9  |
| ipv6 name-servers .....                                              | 6-10 |
| <br><b>Chapter 7: HTTP Redirect Configuration</b> .....              | 7-1  |
| Overview .....                                                       | 7-1  |
| Configuration Tasks .....                                            | 7-2  |
| Configure Subscriber Authentication and Reauthorization .....        | 7-2  |
| Configure an IP ACL and Apply It to Subscribers .....                | 7-2  |
| Configure the HTTP Server on the Active Controller Card .....        | 7-2  |
| Configure and Attach an HTTP Redirect Profile to Subscribers .....   | 7-3  |
| Configure a Policy ACL That Classifies HTTP Packets .....            | 7-4  |
| Configure and Attach a Forward Policy to Redirect HTTP Packets ..... | 7-4  |
| Configuration Examples .....                                         | 7-5  |
| Command Descriptions .....                                           | 7-6  |
| http-redirect profile .....                                          | 7-7  |
| http-redirect server .....                                           | 7-9  |
| port .....                                                           | 7-10 |
| redirect destination local .....                                     | 7-11 |
| url .....                                                            | 7-12 |
| <br><b>Chapter 8: ACL Configuration</b> .....                        | 8-1  |
| Overview .....                                                       | 8-1  |
| IP ACLs .....                                                        | 8-1  |
| IP ACL Applications .....                                            | 8-2  |
| IP ACL Statements .....                                              | 8-2  |
| IP ACL Packet Filtering .....                                        | 8-3  |
| Policy ACLs .....                                                    | 8-3  |
| Policy ACL Applications .....                                        | 8-3  |
| Policy ACL Statements .....                                          | 8-4  |
| Policy ACL Packet Filtering .....                                    | 8-4  |



---

|                                                                    |      |
|--------------------------------------------------------------------|------|
| Configuration Tasks .....                                          | 8-4  |
| Configuration Guidelines .....                                     | 8-5  |
| Configure an IP ACL .....                                          | 8-6  |
| Apply an IP ACL .....                                              | 8-6  |
| Enable ACL Counters or Logging for a Subscriber .....              | 8-7  |
| Modify IP ACL Conditions in Real Time .....                        | 8-7  |
| Configure a Policy ACL .....                                       | 8-7  |
| Apply a Policy ACL .....                                           | 8-8  |
| Modify Policy ACL Conditions in Real Time .....                    | 8-8  |
| Configuration Examples .....                                       | 8-8  |
| Configure an ACL Statement .....                                   | 8-8  |
| Add an ACL Statement .....                                         | 8-9  |
| Resequence ACL Statements .....                                    | 8-9  |
| Configure an Absolute Time Condition Statement .....               | 8-10 |
| Configure a Periodic Time Condition Statement .....                | 8-10 |
| Configure an IP ACL .....                                          | 8-11 |
| Configure a Policy ACL Associated with a QoS Policing Policy ..... | 8-11 |
| Configure a Policy ACL Associated with a Forward Policy .....      | 8-12 |
| Configure a Policy ACL Associated with a NAT Policy .....          | 8-12 |
| Command Descriptions .....                                         | 8-13 |
| absolute .....                                                     | 8-14 |
| access-group .....                                                 | 8-16 |
| access-list .....                                                  | 8-18 |
| admin-access-group .....                                           | 8-19 |
| class .....                                                        | 8-21 |
| condition .....                                                    | 8-23 |
| deny .....                                                         | 8-25 |
| description .....                                                  | 8-34 |
| ip access-group .....                                              | 8-35 |
| ip access-list .....                                               | 8-37 |
| modify ip access-list .....                                        | 8-39 |
| modify policy access-list .....                                    | 8-41 |
| periodic .....                                                     | 8-43 |
| permit .....                                                       | 8-45 |
| policy access-list .....                                           | 8-54 |
| resequence ip access-list .....                                    | 8-56 |
| resequence policy access-list .....                                | 8-57 |

## Part 4: IP Service Policies

---

|                                                                       |      |
|-----------------------------------------------------------------------|------|
| <b>Chapter 9: Forward Policy Configuration</b> .....                  | 9-1  |
| Overview .....                                                        | 9-1  |
| Circuit-Based Forwarding .....                                        | 9-2  |
| Class-Based Forwarding .....                                          | 9-2  |
| Circuit- and Class-Based Forwarding .....                             | 9-2  |
| Configuration Tasks .....                                             | 9-2  |
| Configure a Forward Policy .....                                      | 9-3  |
| Apply a Policy ACL to a Forward Policy .....                          | 9-3  |
| Configuration Examples .....                                          | 9-4  |
| Traffic Mirroring .....                                               | 9-4  |
| Traffic Redirect .....                                                | 9-7  |
| Traffic Drop .....                                                    | 9-9  |
| Combination of Traffic Mirror, Redirect, and Drop in One Policy ..... | 9-11 |

|                                                                  |             |
|------------------------------------------------------------------|-------------|
| Command Descriptions .....                                       | 9-13        |
| drop .....                                                       | 9-14        |
| forward output .....                                             | 9-16        |
| forward policy .....                                             | 9-18        |
| forward policy in .....                                          | 9-19        |
| forward policy out .....                                         | 9-21        |
| mirror destination .....                                         | 9-23        |
| redirect destination circuit .....                               | 9-25        |
| redirect destination next-hop .....                              | 9-26        |
| <b>Chapter 10: NAT Policy Configuration .....</b>                | <b>10-1</b> |
| Overview .....                                                   | 10-1        |
| Static Translation .....                                         | 10-2        |
| Dynamic Translation .....                                        | 10-3        |
| Policy ACLs .....                                                | 10-3        |
| NAT DMZ .....                                                    | 10-3        |
| Summary .....                                                    | 10-4        |
| Configuration Tasks .....                                        | 10-4        |
| Configure a NAT Policy with Static Translations .....            | 10-5        |
| Configure a NAT Policy with a DMZ Host Server .....              | 10-5        |
| Configure a NAT Policy with Dynamic Translations .....           | 10-6        |
| Apply a Policy ACL to a NAT Policy .....                         | 10-7        |
| Configuration Examples .....                                     | 10-7        |
| NAT Policy with Static Translation .....                         | 10-7        |
| NAT Policy with Static NAPT Translation .....                    | 10-8        |
| NAT Policy with Static Translation and a DMZ Host Server .....   | 10-8        |
| NAT Policy with Dynamic Translation and an Ignore Action .....   | 10-9        |
| NAT Policy with Dynamic NAPT Translation and a Drop Action ..... | 10-9        |
| NAT Policy with Static and Dynamic Translations .....            | 10-10       |
| Command Descriptions .....                                       | 10-10       |
| address .....                                                    | 10-11       |
| drop .....                                                       | 10-13       |
| ignore .....                                                     | 10-14       |
| ip dmz .....                                                     | 10-15       |
| ip nat .....                                                     | 10-16       |
| ip nat pool .....                                                | 10-17       |
| ip static in .....                                               | 10-18       |
| ip static out .....                                              | 10-20       |
| nat policy .....                                                 | 10-22       |
| nat policy-name .....                                            | 10-23       |
| pool .....                                                       | 10-24       |
| timeout .....                                                    | 10-25       |
| <b>Chapter 11: Service Policy Configuration .....</b>            | <b>11-1</b> |
| Overview .....                                                   | 11-1        |
| Configuration Tasks .....                                        | 11-2        |
| Configure a Service Policy .....                                 | 11-2        |
| Attach a Service Policy to Subscriber Sessions .....             | 11-2        |
| Configuration Examples .....                                     | 11-3        |
| Command Descriptions .....                                       | 11-4        |
| allow .....                                                      | 11-5        |
| service-policy .....                                             | 11-6        |

---

## Part 5: Quality of Service Policies

---

|                                                               |       |
|---------------------------------------------------------------|-------|
| <b>Chapter 12: QoS Rate- and Class-Limiting Configuration</b> | 12-1  |
| Overview                                                      | 12-1  |
| Priority Groups                                               | 12-2  |
| Policy Access Control Lists                                   | 12-2  |
| QoS Policing and Metering Policies                            | 12-2  |
| Circuit-Based Marking                                         | 12-3  |
| Circuit-Based Rate-Limiting                                   | 12-3  |
| Class-Based Marking                                           | 12-4  |
| Class-Based Rate-Limiting                                     | 12-4  |
| Circuit-Based and Class-Based Rate-Limiting                   | 12-4  |
| Single Rate Three-Color Markers                               | 12-5  |
| Summary                                                       | 12-6  |
| Configuration Tasks                                           | 12-6  |
| Policy Configuration Guidelines                               | 12-6  |
| Configure a Metering Policy                                   | 12-7  |
| Configure a Policing Policy                                   | 12-8  |
| Apply a Policy ACL                                            | 12-9  |
| Configuration Examples                                        | 12-10 |
| Circuit-Based Marking                                         | 12-10 |
| Circuit-Based Rate-Limiting                                   | 12-10 |
| Class-Based and Circuit-Based Rate Limiting                   | 12-10 |
| Command Descriptions                                          | 12-12 |
| conform mark dscp                                             | 12-13 |
| conform mark precedence                                       | 12-16 |
| conform mark priority                                         | 12-18 |
| conform no-action                                             | 12-20 |
| exceed drop                                                   | 12-21 |
| exceed mark dscp                                              | 12-23 |
| exceed mark precedence                                        | 12-25 |
| exceed mark priority                                          | 12-27 |
| exceed no-action                                              | 12-29 |
| mark dscp                                                     | 12-31 |
| mark precedence                                               | 12-33 |
| mark priority                                                 | 12-35 |
| qos policy metering                                           | 12-37 |
| qos policy policing                                           | 12-38 |
| rate                                                          | 12-40 |
| rate percentage                                               | 12-42 |
| violate drop                                                  | 12-44 |
| violate mark dscp                                             | 12-46 |
| violate mark precedence                                       | 12-49 |
| violate mark priority                                         | 12-51 |
| violate no-action                                             | 12-53 |
| <b>Chapter 13: QoS Scheduling Configuration</b>               | 13-1  |
| Overview                                                      | 13-2  |
| Queue Maps                                                    | 13-2  |
| Priority Queuing Policies                                     | 13-3  |
| Enhanced Deficit Round-Robin Policies                         | 13-3  |
| Asynchronous Transfer Mode Weighted Fair Queuing Policies     | 13-4  |
| Priority Weighted Fair Queuing Policies                       | 13-4  |

---

|                                                                      |       |
|----------------------------------------------------------------------|-------|
| Congestion Management and Avoidance .....                            | 13-5  |
| Random Early Detection .....                                         | 13-5  |
| Early Packet Discard .....                                           | 13-6  |
| Multidrop Precedence .....                                           | 13-6  |
| Congestion Avoidance Maps .....                                      | 13-7  |
| Queue Depth .....                                                    | 13-7  |
| Queue Rates .....                                                    | 13-7  |
| Configuration Tasks .....                                            | 13-8  |
| Configure a Queue Map .....                                          | 13-8  |
| Configure a Congestion Avoidance Map .....                           | 13-9  |
| Configure an ATMWFQ Policy .....                                     | 13-9  |
| Configure an EDRR Policy .....                                       | 13-10 |
| Configure a PQ Policy .....                                          | 13-11 |
| Configure a PWFQ Policy .....                                        | 13-11 |
| Configuration Examples .....                                         | 13-12 |
| Queue Maps .....                                                     | 13-12 |
| Congestion Avoidance Map for Multidrop Profiles .....                | 13-13 |
| ATMWFQ Policies .....                                                | 13-13 |
| EDRR Policy .....                                                    | 13-13 |
| PQ Policies .....                                                    | 13-14 |
| RED Parameters .....                                                 | 13-14 |
| Rate-Limiting .....                                                  | 13-14 |
| Backbone Application .....                                           | 13-15 |
| PWFQ Policies .....                                                  | 13-16 |
| Strict Priority .....                                                | 13-16 |
| Normal Priority .....                                                | 13-16 |
| Strict + Normal Priority .....                                       | 13-17 |
| Strict + Normal Priority with Maximum Priority-Group Bandwidth ..... | 13-17 |
| Strict + Normal Priority with Maximum and Minimum Bandwidths .....   | 13-17 |
| Command Descriptions .....                                           | 13-18 |
| congestion-map .....                                                 | 13-19 |
| num-queues .....                                                     | 13-20 |
| qos congestion-avoidance-map .....                                   | 13-22 |
| qos policy atmwfq .....                                              | 13-24 |
| qos policy edrr .....                                                | 13-26 |
| qos policy pq .....                                                  | 13-28 |
| qos policy pwfq .....                                                | 13-30 |
| qos queue-map .....                                                  | 13-31 |
| queue congestion epd .....                                           | 13-33 |
| queue depth .....                                                    | 13-35 |
| queue exponential-weight .....                                       | 13-37 |
| queue-map .....                                                      | 13-39 |
| queue 0 mode .....                                                   | 13-40 |
| queue priority .....                                                 | 13-41 |
| queue priority-group .....                                           | 13-44 |
| queue rate .....                                                     | 13-46 |
| queue red .....                                                      | 13-47 |
| queue weight .....                                                   | 13-52 |
| rate .....                                                           | 13-54 |
| weight .....                                                         | 13-56 |

|                                                                         |       |
|-------------------------------------------------------------------------|-------|
| <b>Chapter 14: QoS Circuit Configuration</b>                            | 14-1  |
| Overview                                                                | 14-2  |
| Circuit Configuration with QoS Policies                                 | 14-2  |
| Hierarchical Configuration for Traffic-Managed Circuits                 | 14-4  |
| Hierarchical Scheduling                                                 | 14-4  |
| Hierarchical Nodes and Node Groups                                      | 14-4  |
| Propagation of QoS Across Layer 3 and Layer 2 Networks                  | 14-5  |
| Propagation of QoS from IP to ATM                                       | 14-6  |
| Propagation of QoS Between IP and Ethernet                              | 14-6  |
| Propagation of QoS Between IP and MPLS                                  | 14-7  |
| Propagation of QoS Between IP and L2TP                                  | 14-8  |
| Configuration Tasks                                                     | 14-9  |
| Configuration Guidelines                                                | 14-10 |
| Configure an ATM PVC for QoS                                            | 14-11 |
| Configure a PVC on a First-Generation ATM OC Traffic Card               | 14-11 |
| Configure a PVC on an ATM DS-3 or Second-Generation ATM OC Traffic Card | 14-11 |
| Configure an Ethernet Circuit for QoS                                   | 14-12 |
| Configure Any Ethernet or Gigabit Ethernet Circuit for QoS              | 14-12 |
| Configure a Traffic-Managed Port for Hierarchical Scheduling            | 14-13 |
| Configure a Traffic-Managed Port for Hierarchical Nodes                 | 14-13 |
| Configure a PDH Circuit for QoS                                         | 14-15 |
| Configure a POS Circuit for QoS                                         | 14-15 |
| Configure Cross-Connected Circuits for QoS                              | 14-16 |
| Configure a Subscriber Circuit for QoS                                  | 14-16 |
| Configure L2TP for QoS                                                  | 14-17 |
| Configure MPLS for QoS                                                  | 14-17 |
| Propagate QoS Using IP DSCP Bits and MPLS EXP Bits                      | 14-17 |
| Propagate QoS Using IP DSCP Bits Only                                   | 14-18 |
| Configuration Examples                                                  | 14-18 |
| Attaching Rate- and Class-Limiting Policies                             | 14-18 |
| PVC Configuration                                                       | 14-18 |
| Cross-Connected Circuit Configuration                                   | 14-18 |
| Subscriber Configuration                                                | 14-19 |
| Attaching Scheduling Policies                                           | 14-19 |
| Port Configuration                                                      | 14-19 |
| PVC Configuration                                                       | 14-19 |
| PWFQ Policy and Hierarchical Shaping                                    | 14-20 |
| PWFQ Policy and Hierarchical Scheduling                                 | 14-20 |
| Propagating QoS                                                         | 14-21 |
| Command Descriptions                                                    | 14-21 |
| clpbit propagate qos to atm                                             | 14-22 |
| egress prefer dscp-qos                                                  | 14-24 |
| propagate qos from ethernet                                             | 14-25 |
| propagate qos from l2tp                                                 | 14-26 |
| propagate qos from-mpls                                                 | 14-27 |
| propagate qos from subscriber                                           | 14-28 |
| propagate qos to ethernet                                               | 14-30 |
| propagate qos to l2tp                                                   | 14-31 |
| propagate qos to-mpls                                                   | 14-33 |
| qos hierarchical mode                                                   | 14-34 |
| qos mode                                                                | 14-36 |
| qos node                                                                | 14-38 |
| qos node-group                                                          | 14-40 |
| qos node-reference                                                      | 14-41 |

|                           |       |
|---------------------------|-------|
| qos policy metering ..... | 14-42 |
| qos policy policing ..... | 14-44 |
| qos policy queuing .....  | 14-46 |
| qos priority .....        | 14-49 |
| qos rate .....            | 14-51 |
| qos weight .....          | 14-53 |

---

## Part 6: Security

---

|                                                          |       |
|----------------------------------------------------------|-------|
| <b>Chapter 15: AAA Configuration</b> .....               | 15-1  |
| Overview .....                                           | 15-1  |
| Authentication .....                                     | 15-1  |
| Administrators .....                                     | 15-2  |
| Subscribers .....                                        | 15-2  |
| Authorization and Reauthorization .....                  | 15-4  |
| CLI Commands Authorization .....                         | 15-4  |
| Dynamic Subscriber Reauthorization .....                 | 15-4  |
| Accounting .....                                         | 15-4  |
| CLI Commands Accounting .....                            | 15-4  |
| Administrator Accounting .....                           | 15-4  |
| Subscriber Accounting .....                              | 15-4  |
| L2TP Accounting .....                                    | 15-5  |
| Configuration Tasks .....                                | 15-5  |
| Configure Global AAA .....                               | 15-6  |
| Limit the Number of Active Administrator Sessions .....  | 15-6  |
| Limit the Number of Active Subscriber Sessions .....     | 15-6  |
| Enable a Direct Connection for Subscriber Circuits ..... | 15-6  |
| Define Structured Username Formats .....                 | 15-7  |
| Configure Authentication .....                           | 15-7  |
| Configure Administrator Authentication .....             | 15-7  |
| Configure Subscriber Authentication .....                | 15-7  |
| Disable Subscriber Authentication .....                  | 15-10 |
| Configure Authorization and Reauthorization .....        | 15-10 |
| Configure CLI Commands Authorization .....               | 15-11 |
| Configure L2TP Peer Authorization .....                  | 15-11 |
| Configure Dynamic Subscriber Reauthorization .....       | 15-11 |
| Configure Accounting .....                               | 15-12 |
| Configure CLI Commands Accounting .....                  | 15-12 |
| Configure Administrator Accounting .....                 | 15-13 |
| Configure Subscriber Accounting .....                    | 15-13 |
| Configure L2TP Accounting .....                          | 15-15 |
| Configuration Examples .....                             | 15-15 |
| Subscriber Authentication .....                          | 15-16 |
| Subscriber Reauthorization .....                         | 15-17 |
| Command Descriptions .....                               | 15-17 |
| aaa accounting administrator .....                       | 15-18 |
| aaa accounting commands .....                            | 15-19 |
| aaa accounting event .....                               | 15-21 |
| aaa accounting l2tp .....                                | 15-23 |
| aaa accounting reauthorization subscriber .....          | 15-25 |
| aaa accounting subscriber .....                          | 15-27 |
| aaa accounting suppress-acct-on-fail .....               | 15-29 |
| aaa authentication administrator .....                   | 15-31 |

|                                                              |             |
|--------------------------------------------------------------|-------------|
| aaa authentication subscriber                                | 15-34       |
| aaa authorization commands                                   | 15-37       |
| aaa authorization tunnel                                     | 15-39       |
| aaa global accounting event                                  | 15-40       |
| aaa global accounting l2tp-session                           | 15-41       |
| aaa global accounting reauthorization subscriber             | 15-42       |
| aaa global accounting subscriber                             | 15-44       |
| aaa global authentication subscriber                         | 15-45       |
| aaa global maximum subscriber                                | 15-46       |
| aaa global update subscriber                                 | 15-48       |
| aaa hint ip-address                                          | 15-50       |
| aaa last-resort                                              | 15-52       |
| aaa maximum subscriber                                       | 15-54       |
| aaa provision binding-order                                  | 15-56       |
| aaa provision route                                          | 15-58       |
| aaa reauthorization bulk                                     | 15-59       |
| aaa update subscriber                                        | 15-61       |
| aaa username-format                                          | 15-63       |
| <b>Chapter 16: RADIUS Configuration</b>                      | <b>16-1</b> |
| Overview                                                     | 16-1        |
| Configuration Tasks                                          | 16-2        |
| Configure the Server IP Address or Hostname                  | 16-2        |
| Configure an IP Source Address (Optional)                    | 16-3        |
| Configure Load Balancing Between RADIUS Servers (Optional)   | 16-3        |
| Modify RADIUS Connection Parameters (Optional)               | 16-3        |
| Send Accounting On and Off Messages                          | 16-3        |
| Modify RADIUS Timeout Parameters                             | 16-4        |
| Strip the Domain Portion of Structured Usernames (Optional)  | 16-5        |
| Change the Server Source Port Value (Optional)               | 16-5        |
| Configure and Assign a RADIUS Policy to a Context (Optional) | 16-5        |
| Configure and Send Attributes in RADIUS Packets (Optional)   | 16-6        |
| Remap Account Termination Codes (Optional)                   | 16-6        |
| Configuration Examples                                       | 16-7        |
| Command Descriptions                                         | 16-8        |
| attribute                                                    | 16-9        |
| radius accounting algorithm                                  | 16-11       |
| radius accounting deadtime                                   | 16-12       |
| radius accounting max-outstanding                            | 16-13       |
| radius accounting max-retries                                | 16-14       |
| radius accounting send-acct-on-off                           | 16-15       |
| radius accounting server                                     | 16-17       |
| radius accounting server-timeout                             | 16-19       |
| radius accounting timeout                                    | 16-20       |
| radius algorithm                                             | 16-21       |
| radius attribute acct-delay-time                             | 16-22       |
| radius attribute acct-session-id                             | 16-23       |
| radius attribute acct-terminate-cause remap                  | 16-24       |
| radius attribute calling-station-id                          | 16-25       |
| radius attribute filter-id                                   | 16-28       |
| radius attribute nas-ip-address                              | 16-30       |
| radius attribute nas-port                                    | 16-31       |
| radius attribute nas-port-id                                 | 16-33       |
| radius attribute nas-port-type                               | 16-36       |

---

|                                                              |       |
|--------------------------------------------------------------|-------|
| radius attribute vendor-specific .....                       | 16-38 |
| radius deadtime .....                                        | 16-39 |
| radius max-outstanding .....                                 | 16-40 |
| radius max-retries .....                                     | 16-41 |
| radius policy .....                                          | 16-42 |
| radius server .....                                          | 16-44 |
| radius server-timeout .....                                  | 16-46 |
| radius source-port .....                                     | 16-47 |
| radius strip-domain .....                                    | 16-48 |
| radius timeout .....                                         | 16-49 |
| rbak-term-ec .....                                           | 16-50 |
| <b>Chapter 17: TACACS+ Configuration</b> .....               | 17-1  |
| Overview .....                                               | 17-1  |
| Configuration Tasks .....                                    | 17-2  |
| Configuration Examples .....                                 | 17-3  |
| Command Descriptions .....                                   | 17-3  |
| tacacs+ deadtime .....                                       | 17-4  |
| tacacs+ max-retries .....                                    | 17-6  |
| tacacs+ server .....                                         | 17-8  |
| tacacs+ strip-domain .....                                   | 17-10 |
| tacacs+ timeout .....                                        | 17-11 |
| <b>Chapter 18: Key Chain Configuration</b> .....             | 18-1  |
| Overview .....                                               | 18-1  |
| Configuration Tasks .....                                    | 18-1  |
| Configure a Key Chain Name and Description (Optional) .....  | 18-2  |
| Configure a Key Chain Name and ID .....                      | 18-2  |
| Configure a Key String .....                                 | 18-2  |
| Limit the Lifespan of a Key .....                            | 18-2  |
| Enable Key Chain Authentication with Routing Protocols ..... | 18-3  |
| Configuration Examples .....                                 | 18-3  |
| Command Descriptions .....                                   | 18-3  |
| accept-lifetime .....                                        | 18-4  |
| key-chain description .....                                  | 18-6  |
| key-chain key-id .....                                       | 18-7  |
| key-string .....                                             | 18-9  |
| send-lifetime .....                                          | 18-10 |
| <b>Chapter 19: Lawful Intercept Configuration</b> .....      | 19-1  |
| Overview .....                                               | 19-1  |
| Configuration Tasks .....                                    | 19-1  |
| Configure an LI Profile .....                                | 19-2  |
| Configure Circuits for LI .....                              | 19-2  |
| Activate an Intercept .....                                  | 19-3  |
| Configuration Examples .....                                 | 19-3  |
| Command Descriptions .....                                   | 19-4  |
| header .....                                                 | 19-5  |
| li-profile .....                                             | 19-6  |
| pending .....                                                | 19-7  |
| transport udp .....                                          | 19-8  |
| type .....                                                   | 19-10 |



---

## Part 7: Appendixes

---

|                                                            |      |
|------------------------------------------------------------|------|
| <b>Appendix A: RADIUS Attributes</b> .....                 | A-1  |
| Overview .....                                             | A-1  |
| RADIUS Packet Format .....                                 | A-2  |
| Packet Types .....                                         | A-2  |
| RADIUS Files .....                                         | A-3  |
| RADIUS Dictionary File .....                               | A-3  |
| RADIUS Clients Files .....                                 | A-4  |
| Subscriber Files .....                                     | A-4  |
| Supported Standard RADIUS Attributes .....                 | A-4  |
| Redback VSAs .....                                         | A-10 |
| <br><b>Appendix B: TACACS+ Attribute-Value Pairs</b> ..... | B-1  |
| TACACS+ Authentication and Authorization AV Pairs .....    | B-1  |
| TACACS+ Administrator Accounting AV Pairs .....            | B-2  |
| TACACS+ Command Accounting AV Pairs .....                  | B-2  |
| <br><b>Index</b> .....                                     | 1    |
| <br><b>Commands</b> .....                                  | 1    |
| <br><b>Modes</b> .....                                     | 1    |

---

# About This Guide

---

This guide describes the tasks and commands used to configure the following SmartEdge® OS IP services and security features: Address Resolution Protocol (ARP), Neighbor Discovery (ND) protocol for IP Version 6 (IPv6) routers, Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), Domain Name System (DNS), HTTP redirect, access control lists (ACLs), forward policies, Network Address Translation (NAT) policies, service policies, quality of service (QoS) policies, authentication, authorization, and accounting (AAA), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), key chains, and lawful intercept (LI).

This preface contains the following sections:

- Related Publications
- Intended Audience
- Organization
- Conventions
- Ordering Documentation

## Related Publications

---

In parallel with this guide, use the *IP Services and Security Operations Guide* for the SmartEdge OS, which describes the tasks and commands used to monitor, administer, and troubleshoot IP services and security features.

Use these guides in conjunction with the following publications:

- *Basic System Configuration Guide* for the SmartEdge OS

Describes the tasks and commands used to configure the following SmartEdge OS features: how to use the SmartEdge command-line interface (CLI), configuration file management, access to the system; basic system parameters; contexts, interfaces, and subscribers; system-wide management features, including bulk statistics, logging facilities, and the Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) functions.

- *Ports, Circuits, and Tunnels Configuration Guide*

Describes the tasks and commands to use the CLI and manage SmartEdge OS releases and configuration files; describes the tasks and commands used to configure the following SmartEdge OS features: traffic cards, their ports, channels, and subchannels, and Automatic Protection Switching (APS); circuits, including clientless IP service selection (CLIPS) circuits and link aggregation; bridging and cross-connections between circuits; Generic Routing Encapsulation (GRE) tunnels (including IP Version 6 [IPv6] over GRE tunnels), Layer 2 Tunneling Protocol (L2TP) tunnels, and overlay tunnels (IPv6 over IP Version 4 [IPv4]); static and dynamic bindings between ports, channels, subchannels, and circuits to interfaces, either directly or indirectly.

- *Routing Protocols Configuration Guide for the SmartEdge OS*

Describes the tasks and commands used to configure the following SmartEdge OS features: static IP routing; dynamically verified static routing (DVSR); Virtual Router Redundancy Protocol (VRRP); Routing Information Protocol (RIP) and RIP next generation (RIPng); Open Shortest Path First (OSPF) and OSPF Version 3 (OSPFv3); Border Gateway Protocol (BGP); BGP/Multiprotocol Label Switching Virtual Private Networks (BGP/MPLS VPNs); Intermediate System-to-Intermediate System (IS-IS); Bidirectional Forwarding Detection (BFD); IP multicast, including Internet Group Management Protocol (IGMP), Multicast Source Discovery Protocol (MSDP), and Protocol Independent Multicast (PIM); routing policies; MPLS; Layer 2 Virtual Private Networks (L2VPNs); Virtual Private LAN Services (VPLS); and Label Distribution Protocol (LDP). BGP, OSPFv3, RIPng, and routing policies include tasks and commands that provide limited support for IPv6 routing.

- *Basic System Operations Guide for the SmartEdge OS*

Describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge OS features described in the *Basic System Configuration Guide*; commands include all **clear**, **debug**, **monitor**, **process**, and **show** commands that monitor and test system-wide functions and features, such as software processes.

- *Ports, Circuits, and Tunnels Operations Guide for the SmartEdge OS*

Describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge OS features described in the *Ports, Circuits, and Tunnels Configuration Guide*; commands include all **clear**, **debug**, **monitor**, and **show** commands, along with other operations-based commands, such as device management and on-demand diagnostics.

- *Routing Protocols Operations Guide for the SmartEdge OS*

Describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge OS features described in the *Routing Protocols Configuration Guide*; commands include all **clear**, **debug**, **monitor**, **process**, and **show** commands, along with other operations-based commands.

- *SmartEdge 800 Router Hardware Guide*

Describes the SmartEdge 800 hardware and provides site preparation information and installation, monitoring, and maintenance procedures for the chassis and cards.

- *SmartEdge 400 Router Hardware Guide*

Describes the SmartEdge 400 hardware and provides site preparation information and installation, monitoring, and maintenance procedures for the chassis and cards.

# Intended Audience

---

This guide is intended for system and network administrators experienced in access and internetwork administration.

## Organization

---

This guide is organized as follows:

- Part 1, “Introduction”  
Describes the SmartEdge OS IP services and security features.
- Part 2, “IP Service Protocols”  
Describes the tasks and commands used to configure ARP, the ND protocol, NTP, and DHCP.
- Part 3, “IP Services”  
Describes the tasks and commands used to configure DNS, HTTP redirect, LI, and IP and policy ACLs.
- Part 4, “IP Service Policies”  
Describes the tasks and commands used to configure forward policies, NAT policies, and service policies.
- Part 5, “Quality of Service Policies”  
Describes the tasks and commands used to configure QoS policies and ports, channels, circuits, and applications for QoS functions.
- Part 6, “Security”  
Describes the tasks and commands used to configure security features, including AAA, RADIUS, TACACS+, and key chains.
- Part 7, “Appendixes”  
Describes attributes used with RADIUS and attribute-value pairs (AVPs) used with TACACS+.

**Note** There are three indexes in this guide: an index of tasks and features, an index of commands, and an index of CLI modes with the commands found within each mode.

## Conventions

---

This guide uses special conventions for the following elements:

- Command Modes and Privilege Levels
- Command Syntax
- Examples

- Task Tables
- Online Navigation Aids

## Command Modes and Privilege Levels

Commands are entered in exec mode or in one of many configuration modes. By default, the majority of commands in exec mode have a privilege level of 3, while commands in any configuration mode have a privilege level of 10. Exceptions are noted in parentheses ( ) in the “Command Mode” section in any command description; for example, “exec (15)”.

For a list of command modes and a figure displaying the command mode hierarchy, see the “Command Mode Hierarchy” section in Chapter 1, “Overview.”

For detailed information about command modes and privilege levels, see the “User Interface” section (in the “Overview” chapter) in the *Basic System Configuration Guide* for the SmartEdge OS.

## Command Syntax

Table 1 lists the descriptions of the elements used in a command syntax statement.

**Table 1 Command Syntax Terminology**

| Syntax Element | Definition                                                                                                                                                                                                                                         | Example Fragment                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Argument       | An item for which you must supply a value.                                                                                                                                                                                                         | <i>slot</i>                                                                                                                                                         |
| Construct      | A combination of: <ul style="list-style-type: none"> <li>• A keyword and its argument.</li> <li>• Two or more keywords that cannot be specified independently.</li> <li>• Two or more arguments that cannot be specified independently.</li> </ul> | <ul style="list-style-type: none"> <li>• <b>min-wait</b> <i>seconds</i></li> <li>• <b>line</b> <i>fdl ansi</i></li> <li>• <i>src</i> <i>src-wildcard</i></li> </ul> |
| Keyword        | An optional or required item that must be entered exactly as shown.                                                                                                                                                                                | <b>all</b>                                                                                                                                                          |

Table 2 describes separator characters used in a command syntax statement.

**Table 2 Separator Characters in Command Syntax**

| Character | Use                                                                                          | Example Fragment                                                                                   |
|-----------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| @         | Separates the prefix name from the suffix name.                                              | <i>sub-name@ctx-name</i>                                                                           |
| /         | Separates slot from port, IP address from prefix length, and separates fields in URLs.       | <i>slot[/port]</i><br><i>{ip-addr   lprefix-length}</i><br><i>ldevice[/directory]lfilename.ext</i> |
| :         | Separates a port from a channel and a channel from a subchannel.                             | <i>port[:chan-num]</i><br><i>ds3-chan-num[:ds1-chan-num]</i>                                       |
| -         | Separates starting value from ending value.                                                  | <i>start-end</i>                                                                                   |
|           | Separates output modifiers from keywords and arguments in <b>show</b> commands. <sup>1</sup> | <b>show configuration   include port</b>                                                           |

1. For more information about the use of the pipe ( | ) character, see the “Using the CLI” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

The following guidelines apply to the characters in Table 2:

- The separator character between the prefix name and the suffix name in a structured username is configurable; the @ character is the default and is used in command syntax throughout this guide.
- Separator characters act as one-character keywords; therefore, they are always shown in bold.

Table 3 lists the characters and formats used in command syntax statements.

**Table 3 Text Formats and Characters in Command Syntax**

| Convention                                                                                                                                              | Example                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Commands and keywords are indicated in <b>bold</b> .                                                                                                    | <b>no ip unnumbered</b>                                                                                                                                                                             |
| Arguments for which you must supply the value are indicated in <i>italics</i> .                                                                         | <b>banner login</b> <i>delimited-text</i>                                                                                                                                                           |
| Square brackets ([ ]) indicate optional arguments, keywords, and constructs within scripts or commands.                                                 | <b>show clock</b> [ <b>universal</b> ]<br><b>enable</b> [ <i>level</i> ]                                                                                                                            |
| Alternative arguments and keywords within commands are separated by the pipe character (   ).                                                           | <b>public-key</b> { <b>DSA</b>   <b>RSA</b> } [ <b>after-key</b> <i>existing-key</i>  <br><b>position</b> <i>key-position</i> ] { <i>new-key</i>   <b>ftp</b> <i>url</i> }                          |
| Alternative, but required arguments and keywords, are shown within grouped braces ({ }), and are separated by the pipe character (   ).                 | <b>debug ssh</b> { <b>all</b>   <b>ssh-general</b>   <b>sshd-detail</b>   <b>sshd-general</b> }<br><b>ip address</b> <i>ip-addr</i> { <i>netmask</i>   <i>lprefix-length</i> } [ <b>secondary</b> ] |
| Optional and required arguments, keywords, and constructs can be nested with grouped braces and square brackets, where the syntax requires such format. | <b>enable authentication</b> { <b>none</b>   <i>method</i> [ <i>method</i> [ <i>method</i> ]]}                                                                                                      |

## Examples

Examples use the following conventions:

- System prompts are of the form [context]hostname(mode)#, [context]hostname#, or [context]hostname>.

In this case, *context* indicates the current context, *hostname* represents the configured name of the SmartEdge system, and *mode* indicates the string for the current configuration mode, if applicable.

Whether the prompt includes the # or the > symbol depends on the privilege level. For further information on privilege levels, see the “Overview” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

For example, the prompt in the *local* context on the Redback system in *context* configuration mode is:

```
[local]Redback(config-ctx)#
```

- Information displayed by the system is in **Courier** font.
- Information that you enter is in **Courier bold** font.

## Task Tables

Tasks to configure features are described in task tables under the “Configuration Tasks” section in each chapter. The command syntax displays only the root command, which is hyperlinked to the location where the complete command syntax is described in the “Command Descriptions” section of each chapter.

Table 4 shows an example of a configuration task table.

**Table 4** Configuration Task Table Example

| Task                                                   | Root Command               | Notes                                                                                                                 |
|--------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Assign a priority group.                               | <b>qos priority</b>        | The QoS bit setting for packets traveling across the ingress circuit is not changed by the priority group assignment. |
| Attach a policing policy.                              | <b>qos policy policing</b> |                                                                                                                       |
| Attach a metering policy.                              | <b>qos policy metering</b> |                                                                                                                       |
| Attach a scheduling policy.                            | <b>qos policy queuing</b>  | Policy types include EDRR and PQ.                                                                                     |
| Optional. Modify the mode of an EDRR policy algorithm. | <b>qos mode</b>            | By default, the mode is normal. Only one mode type is supported on a single port.                                     |

## Online Navigation Aids

To aid in accessing information in the online format for this guide, the following types of cross-references are hyperlinks:

- Cross-references to chapters, sections, tables, and figures in the text
- Lists of section headings within a chapter or appendix
- Commands listed in the “Related Commands” section at the end of each command description
- Entries in the table of contents
- Entries in indexes

**Note** Hyperlinks in PDF files appear the same as regular text; however, your cursor changes from an open hand icon to a pointing finger icon when you move your cursor over a hyperlink.

## Ordering Documentation

---

Redback® documentation is available on CD-ROM, which ships with Redback products. The appropriate CD-ROMS are included with your products as follows:

- SMS™ product
- SmartEdge router product
- NetOp™ product (includes NetOp Element Manager System [EMS] and NetOp Policy Manager [PM])



To order additional copies of the appropriate CD-ROM or printed, bound books, perform the following steps:

1. Log on to the Redback Networks Support web site at <http://www.redback.com> and enter a username and password.

If you do not have a logon username and password, contact your Redback Networks support representative, or send an e-mail to [supportlogin@redback.com](mailto:supportlogin@redback.com) with a copy of the **show hardware** command output, your contact name, company name, address, and telephone number.

2. On the Redback Networks Support web site, select one of the Redback Networks product line tabs at the bottom of the web page, click **Documentation** on the navigation bar, and then click **To Order Books** on the navigation bar.

To electronically provide feedback on our documentation, perform the following steps:

1. On the Documentation web page, click **Feedback** on the navigation bar.
2. Complete and submit the documentation feedback form.

We appreciate your comments.



# Introduction

---

This part describes SmartEdge<sup>®</sup> OS IP services and security features and consists of Chapter 1, “Overview.”



# Overview

This chapter provides an overview of SmartEdge® OS IP services and security features, and lists the relevant command-line interface (CLI) modes as described in the following sections:

- SmartEdge OS Architecture
- IP Protocols
- IP Services
- IP Service Policies
- Quality of Service
- Security
- Command Mode Hierarchy

**Note** In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

## SmartEdge OS Architecture

The SmartEdge OS is based on a general-purpose operating system that works in conjunction with the ASIC-based SmartEdge hardware products to provide a scalable and robust multiservice platform. The SmartEdge OS performs the route processing and other control functions, and runs on the controller card. The packet forwarding function is performed by Packet Processing ASICs (PPAs) on the individual traffic cards. Each major system component (see Table 1-1) runs as a separate process in the system.

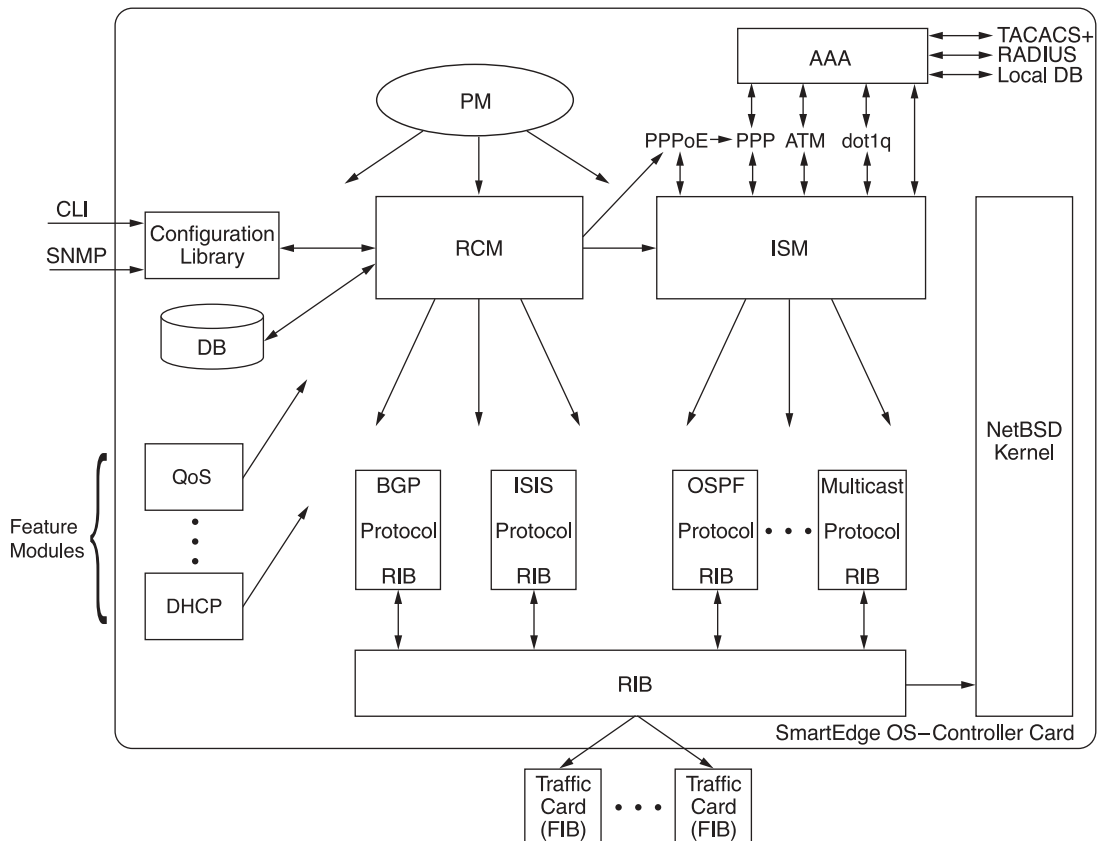
**Table 1-1 SmartEdge OS Components**

| System Component                                    | Function                                                                                                                                  |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication, authorization, and accounting (AAA) | Forces all authentication requests and accounting updates to a single set of Remote Authentication Dial-In User Service (RADIUS) servers. |
| NetBSD kernel                                       | Provides a lean and stable base for the SmartEdge OS.                                                                                     |
| Process Manager (PM)                                | Monitors and controls the operation of the other processes in the system.                                                                 |
| Router Configuration Manager (RCM)                  | Controls all system configurations using a transaction-oriented database.                                                                 |

**Table 1-1 SmartEdge OS Components (continued)**

| System Component                          | Function                                                                                                                                                          |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface and Circuit State Manager (ISM) | Monitors and disseminates the state of all interfaces, ports, and circuits in the system.                                                                         |
| Routing protocols                         | Run as an independent processes, maintaining independent Routing Information Bases (RIBs). The routing processes send the routing information to the central RIB. |
| RIB                                       | Downloads forwarding tables to the traffic cards.                                                                                                                 |
| Feature modules                           | Run as independent processes, each in its own protected address space.                                                                                            |
| Traffic card                              | Includes the PPA ASICs, which contain the Forwarding Information Base (FIB) and forwarding code.                                                                  |

Figure 1-1 illustrates the SmartEdge OS architecture.

**Figure 1-1 SmartEdge OS Architecture**

0565

# IP Protocols

---

The SmartEdge OS provides the IP protocols described in the following sections:

- Address Resolution Protocol
- Neighbor Discovery Protocol
- Dynamic Host Configuration Protocol
- Network Time Protocol

## Address Resolution Protocol

The SmartEdge OS implementation of the Address Resolution Protocol (ARP) is consistent with RFC 826, *An Ethernet Address Resolution Protocol*, also called *Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. In addition, the SmartEdge OS provides a configurable ARP entry-age timer and the option to automatically delete expired dynamic ARP entries.

## Neighbor Discovery Protocol

SmartEdge routers use the Neighbor Discovery (ND) protocol for IP Version 6 (IPv6) to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. The IPv6 ND protocol corresponds to a combination of the IPv4 ARP and Internet Control Management Protocol (ICMP) Router Discovery. The ND protocol is described in RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*.

IPv6 is a new version of the Internet Protocol, designed as the successor to IP Version 4 (IPv4). IPv6 is fully described in RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*. The changes from IPv4 to IPv6 include:

- Increase in address size from 32 bits to 128 bits
- Simplified header
- Extensible header with optional extension headers
- Designed to co-exist with IPv4
- Uses multicast addresses instead of broadcast addresses

For a description of IPv6 addressing and the types of IPv6 addresses, see RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*.

**Note** When IPv6 addresses are not referenced or explicitly specified, the term, IP address, can refer generally to IPv4 addresses, IPv6 addresses, or IP addressing. In instances where IPv6 addresses are referenced or explicitly specified, the term, IP address, refers only to IPv4 addresses.

## Dynamic Host Configuration Protocol

The SmartEdge router provides three types of Dynamic Host Configuration Protocol (DHCP) support:

- External DHCP relay server

In relay mode, the SmartEdge router acts as an intermediary between the DHCP server and the subscriber. The router forwards requests from the subscriber's PC to the DHCP server and relays the server's responses back to the subscriber's PC.

- External DHCP proxy server

In proxy mode, the SmartEdge router provides responses directly to the subscriber requests. Each subscriber sees the router as the DHCP server, and as such, sends all DHCP negotiations, including IP address release and renewal, to the router, which then relays the information to the DHCP server.

Essentially, the proxy feature enables the router to track IP address lease times and other DHCP information more closely. With Remote Authentication Dial-In User Service (RADIUS) authentication, an accounting record is sent from the SmartEdge router to RADIUS every time an IP address is assigned or released.

- Internal DHCP server

The SmartEdge router provides the functions of the DHCP server; no communications are sent to an external DHCP server.

**Note** Before using an external DHCP server, the SmartEdge OS must first be configured with the IP address or hostname of one or multiple external DHCP servers. DHCP servers are configured on a per-context basis, with a limit of one server per context.

## Network Time Protocol

The SmartEdge OS supports versions 1, 2, and 3 of the Network Time Protocol (NTP). On the SmartEdge router, NTP operates in client mode only, meaning that the router can be synchronized by a remote NTP server, but the remote server cannot be synchronized by the router.

**Note** Before using NTP, the SmartEdge router must first be configured with the IP address of one or multiple NTP servers.

## IP Services ---

The SmartEdge OS provides the IP services described in the following sections:

- Domain Name System
- HTTP Redirect
- Access Control Lists



## Domain Name System

The Domain Name System (DNS) enables subscribers to access devices using hostnames, instead of IP addresses. When a command refers to a hostname, the SmartEdge OS consults the local host table for mappings. If the information is not in the table, the router generates a DNS query to resolve the hostname. DNS is enabled on a per-context basis, with one domain name allowed per context.

## HTTP Redirect

HTTP redirect enables service providers to interrupt subscriber HTTP sessions and to redirect them to a preconfigured URL. Applications include the ability to require customer registration, to direct customers to web sites for downloading virus protection software, and to advertise new services or software updates. An HTTP redirect profile containing a redirect URL is attached to subscriber records, and a forward policy redirects HTTP traffic to the lightweight HTTP server on the controller card attached to the subscriber circuit. The forward policy that performs the redirection is removed through a subscriber reauthorization mechanism.

## Lawful Intercept

Lawful intercept (LI) enables service providers to mirror subscriber packets and send them to a mediation system, which can be anywhere in the network. The SmartEdge OS can mirror packets from any circuit in the system, at the ingress or egress point, and send the mirrored packets to the mediation system using a User Datagram Protocol (UDP)/IP session.

## Access Control Lists

The SmartEdge OS supports IP access control lists (ACLs) and policy ACLs as described in the following sections:

- IP ACLs
- Policy ACLs
- Conditional ACLs

### IP ACLs

IP ACLs are lists of packet filters. Based on the criteria specified in the IP ACLs associated with the packet, the SmartEdge OS decides whether the packet should be forwarded or dropped. IP ACLs filter packets through the use of **deny** and **permit**, or **seq deny** and **seq permit** statements. IP ACLs are applied interfaces and contexts and affect packets on all circuits bound to the interface or all administrative packets on a context.

### Policy ACLs

Policy ACLs are lists of packet filters, packet classifications, or both. Based on criteria specified in the policy ACLs associated with the packet, the SmartEdge OS decides whether the packet should be forwarded, dropped, or assigned a class name. Policy ACLs filter packets, classify packets, or perform both actions, through the use of **permit** and **seq permit** statements. Policy ACLs can be applied to forward policies, to NAT policies, and to quality of service (QoS) metering and policing policies.

### Conditional ACLs

You can configured both IP ACLs and policy ACLs with time-based conditions that filter or classify packets for a specified time period. In addition, you can modify time-based conditions in real-time, without requiring you to modify the configuration file for the SmartEdge OS.

## IP Service Policies

---

The SmartEdge OS provides the IP service policies described in the following sections:

- Forward Policies
- Network Address Translation Policies
- Service Policies

### Forward Policies

Forward policies support IP traffic mirroring, redirect, and drop. IP traffic mirroring copies packets traveling across a circuit and forwards the duplicated packets to a designated outgoing port. IP traffic redirect forwards IP packets to IP addresses that are different than their original destination. IP traffic drop determines which particular packets should be dropped, rather than forwarded.

### Network Address Translation Policies

Through Network Address Translation (NAT) policies, hosts using unregistered IP addresses on private networks can connect to hosts on the Internet, and vice versa. NAT translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network.

### Service Policies

Service policies determine the context, or contexts that Point-to-Point Protocol (PPP)- and PPP over Ethernet (PPPoE) subscribers can access by verifying the domain or context name associated with subscriber records.

A service policy can be attached to any PPP- or PPPoE-encapsulated subscriber circuit, including PPP-encapsulated Layer 2 Tunneling Protocol (L2TP) tunnels.

## Quality of Service

---

The SmartEdge OS provides the QoS features described in the following sections:

- Classification, Marking, and Rate-Limiting
- Scheduling

## Classification, Marking, and Rate-Limiting

The SmartEdge OS classifies, marks, and rate-limits incoming packets as described in these sections:

- Priority Groups
- Policy Access Control Lists
- QoS Policing and Metering Policies

### Priority Groups

A priority group number assignment enables you to classify all traffic, including non-IP traffic, on an ingress circuit. A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not changed by this command. The actual queue depends upon the number of queues configured on the circuit.

### Policy Access Control Lists

A classification filter is configured through a policy ACL. Each policy ACL supports up to eight unique classes. Packets can be classified according to IP precedence value, protocol number, IP source and destination address, Internet Control Management Protocol (ICMP) attributes, Internet Group Management Protocol (IGMP) attributes, Transmission Control Protocol (TCP) attributes, and User Datagram Protocol (UDP) attributes.

A policy ACL can be applied to incoming or outgoing packets on a port, circuit, or for a subscriber profile. A policy ACL is applied to incoming packets through a QoS policing policy and to outgoing packets through a QoS metering policy.

### QoS Policing and Metering Policies

A QoS policing policy marks, rate-limits, or performs both actions on incoming packets, while a QoS metering policy does the same for outgoing packets. Both types of policies can be applied at one of two levels or at both levels simultaneously. One level of application applies to all packets on a particular circuit. Another level of application applies to only a particular class of packets traveling across the circuit. The class is configured through a policy ACL.

## Scheduling

After classification, marking, and rate-limiting occurs on an incoming packet, the packet is placed into an output queue for servicing by an egress traffic card's scheduler. The SmartEdge OS supports up to eight queues per circuit. Queues are serviced according to a queue map scheme, a QoS scheduling policy, or both, as described in the following sections:

- Queue Maps
- Priority Queuing
- Enhanced Deficit Round Robin
- Asynchronous Transfer Mode Weighted-Fair Queuing
- Priority Weighted-Fair Queuing

- Hierarchical Scheduling
- Hierarchical Nodes and Node Groups
- Congestion Management and Avoidance

### Queue Maps

The SmartEdge OS assigns factory preset, or default, mapping of a priority group to a particular egress queue, according to the number of queues configured on a circuit. You can configure queue maps to override the default mapping of packets into egress queues. You can apply queue maps along with any of the four QoS scheduling policies.

### Priority Queuing

With a priority queuing (PQ) scheduling policy, the output queues on a circuit are serviced in strict priority order; that is, packets waiting in the highest-priority queue (queue 0) are serviced until that queue is empty, then packets waiting in the second-highest priority queue are serviced (queue 1), and so on. Under congestion, PQ allows the highest priority traffic to get through, at the expense of lower-priority traffic.

### Enhanced Deficit Round Robin

The enhanced deficit round-robin (EDRR) scheduling policy can operate in one of three modes: normal, strict, or alternate. In normal mode, queue 0 is treated like all other queues on a circuit. Each queue receives its share of the circuit's bandwidth according to the weight assigned to the queue. In strict mode, queue 0 always has priority over all other queues configured on a circuit. In alternate mode, in every other round, either queue 0 or one of the other queues on the circuit is served, in alternating fashion.

### Asynchronous Transfer Mode Weighted-Fair Queuing

The Asynchronous Transfer Mode weighted-fair queuing (ATMWFQ) scheduling policy can operate in one of two modes: alternate or strict. In either mode, a modified deficit round-robin (MDRR) algorithm is used to implement class-based WFQ.

In alternate mode, the servicing of queues alternates between queue 0 and the remaining queues. Queue 0 is served, then the next queue is served. Queue 0 is served again, and the next queue in turn is served, and so on. For example, if there are four queues configured, the order of servicing will be q0, q1, q0, q2, q0, q3, q0, q1, and so on. In strict mode, high-priority queue 0 is serviced immediately and then the other queues are serviced in a round-robin fashion.

### Priority Weighted-Fair Queuing

Priority weighted-fair queuing (PWFQ) policies use a priority- and a weight-based algorithm to implement hierarchical QoS-aware scheduling. Each queue in the policy includes both a priority and a relative weight, which control how each queue is serviced. Inside the PWFQ policy, priority takes precedence, and for queues placed at the same priority, the individual configured weight defines how the queue is used in the scheduling decision.

With PWFQ policies, you can configure different congestion behaviors that depend on the DSCP values of the packets in a queue; this feature is referred to as multidrop precedence. Multidrop precedence supports up to three profiles for each queue, and each profile defines a different congestion behavior for one or more DSCP values.

**Note** PWFQ policies are supported only for Gigabit Ethernet (GE1020) and Gigabit Ethernet 3 (GE3) traffic cards.

## Hierarchical Scheduling

Hierarchical scheduling provides the means to perform QoS scheduling at the port, 802.1Q tunnel, and 802.1Q permanent virtual circuits (PVC) levels, using PWFQ policies. Hierarchical scheduling operates on PWFQ queues in either of two modes: strict or WRR. In strict mode, each queue is serviced according to the priority you assigned to the queue. In WRR mode, each queue is serviced in round-robin order according to its priority and its traffic share, as determined by the relative weight.

## Hierarchical Nodes and Node Groups

A hierarchical node functions as an individual circuit, such as an 802.1Q PVC; you can assign a traffic rate and attach a PWFQ policy to it. In addition, you can specify the scheduling mode for the queues defined by the PWFQ policy, either strict or WRR.

Each node is a member of a node group. You can assign a traffic rate and a scheduling mode (which might not be the same traffic rate or scheduling mode assigned to any of the nodes within the group) to a node group. When a subscriber record is assigned to a hierarchical node, all sessions for that subscriber are governed by the QoS shaping configured for the node and for the node group.

**Note** Hierarchical nodes and node groups are supported only for GE3 and GE1020 traffic cards.

## Congestion Management and Avoidance

The SmartEdge OS employs the following congestion avoidance features with scheduling policies:

- Random Early Detection
- Queue Depth
- Queue Rates

### Random Early Detection

With PQ, EDRR, and ATMWFQ policies, you can configure random early detection (RED) parameters to manage buffer utilization under congestion by signaling to sources of traffic that the network is on the verge of entering a congested state, rather than waiting until the network is actually congested.

### Queue Depth

With EDRR and PQ policies, you can modify the number of packets that are allowed in each queue configured on a circuit.

### Queue Rates

With PQ and EDRR policies, you can configure a rate limit, which specifies a long-term, nominal average bit rate for the queuing policy and uses a burst tolerance to specify the number of bytes allowed above the configured rate. In PQ policies, the rate is controlled per individual queue, while in EDRR policies, the rate is a combined traffic rate for all queues in the policy. A reasonable guideline for burst tolerance is 10 times the link maximum transmission unit (MTU).

# Security

---

The SmartEdge OS provides the security features described in the following sections:

- Authentication, Authorization, and Accounting
- Remote Authentication Dial-In User Service
- Terminal Access Controller Access Control System Plus
- Key Chains

## Authentication, Authorization, and Accounting

The SmartEdge OS uses authentication, authorization, and accounting (AAA) to authenticate subscribers through database records kept in one of these locations:

- Locally in the SmartEdge OS through subscriber commands
- On a RADIUS server or set of servers

The first location is the local database, which is a set of subscriber configuration mode commands entered through the SmartEdge OS CLI. The local database provides what is known as local authentication. The second location is the RADIUS server's database, which contains the subscriber records. The SmartEdge OS, configured with the IP address or hostname of the RADIUS server, relies on the database records of the server to authenticate subscribers.

Each SmartEdge OS context can use the IP address or hostname of a RADIUS configured within its context for authentication—this is known as context-specific RADIUS authentication. Alternatively, a context can be configured to use the IP address or hostname of the RADIUS server in the local context—this is known as global authentication. With global authentication, the RADIUS server is expected to return the Context-Name vendor-specific attribute (VSA) that indicates the particular context to which the subscriber is to be bound. You can also configure the SmartEdge router to try authentication through the RADIUS server configured in the current context first, with a fallback to the global RADIUS server or to the local database, in case the RADIUS server in the current context becomes unreachable.

The SmartEdge OS supports subscriber session reauthorization, so that a subscriber's attributes can be updated dynamically, without requiring renegotiation for a current subscriber session and without dropping the session. The updates to the subscriber record are made immediately without interruption.

Subscriber accounting tracks RADIUS-based messages for subscriber sessions. The data can be sent to a set of RADIUS servers in the local context, a set of RADIUS servers in another context, or both. This last case is called two-stage accounting, where, for example, a wholesaler can send a copy of accounting data to his own RADIUS server and to an upstream service provider's RADIUS server, allowing end-of-period accounting data to be reconciled and validated by both parties.

## Remote Authentication Dial-In User Service

RADIUS is based on a client/server architecture. The SmartEdge OS can be configured to act as a RADIUS client. The use of RADIUS replaces the need for local configuration of user records, although we recommend a local configuration in case the remote server is unreachable.

**Note** RADIUS servers are context specific, with a limit of five servers for each context.

If your network topology requires separate RADIUS accounting servers for billing or load-balancing purposes, you can also configure one or more RADIUS accounting servers, which then take over the accounting functions from the RADIUS servers. The SmartEdge OS can send RADIUS accounting data to a global set of RADIUS servers, a context-specific set of RADIUS servers, or both. This last case is referred to as two-stage accounting.

## Terminal Access Controller Access Control System Plus

The Terminal Access Controller Access Control System Plus (TACACS+) protocol secures remote access to networks and network services and is based on a client/server architecture. The SmartEdge router can be configured to act as a TACACS+ client. The use of TACACS+ replaces the need for local configuration of user records, although we recommend a local configuration in case the remote server is unreachable. The SmartEdge OS supports the TACACS+ features of OPIE, S/Key, and secureID.

**Note** Before using TACACS+, the SmartEdge router must first be configured with the IP address or hostname of one or multiple TACACS+ servers. TACACS+ servers are configured on a per-context basis, with a limit of six servers per context.

## Key Chains

Key chains allow you to control authentication keys used by various routing protocols in the system. Currently, the SmartEdge OS supports the use of key chains with the Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) routing protocols. In the configuration process, you establish a name for each key chain, and an identification for each key within the key chain.

## Command Mode Hierarchy

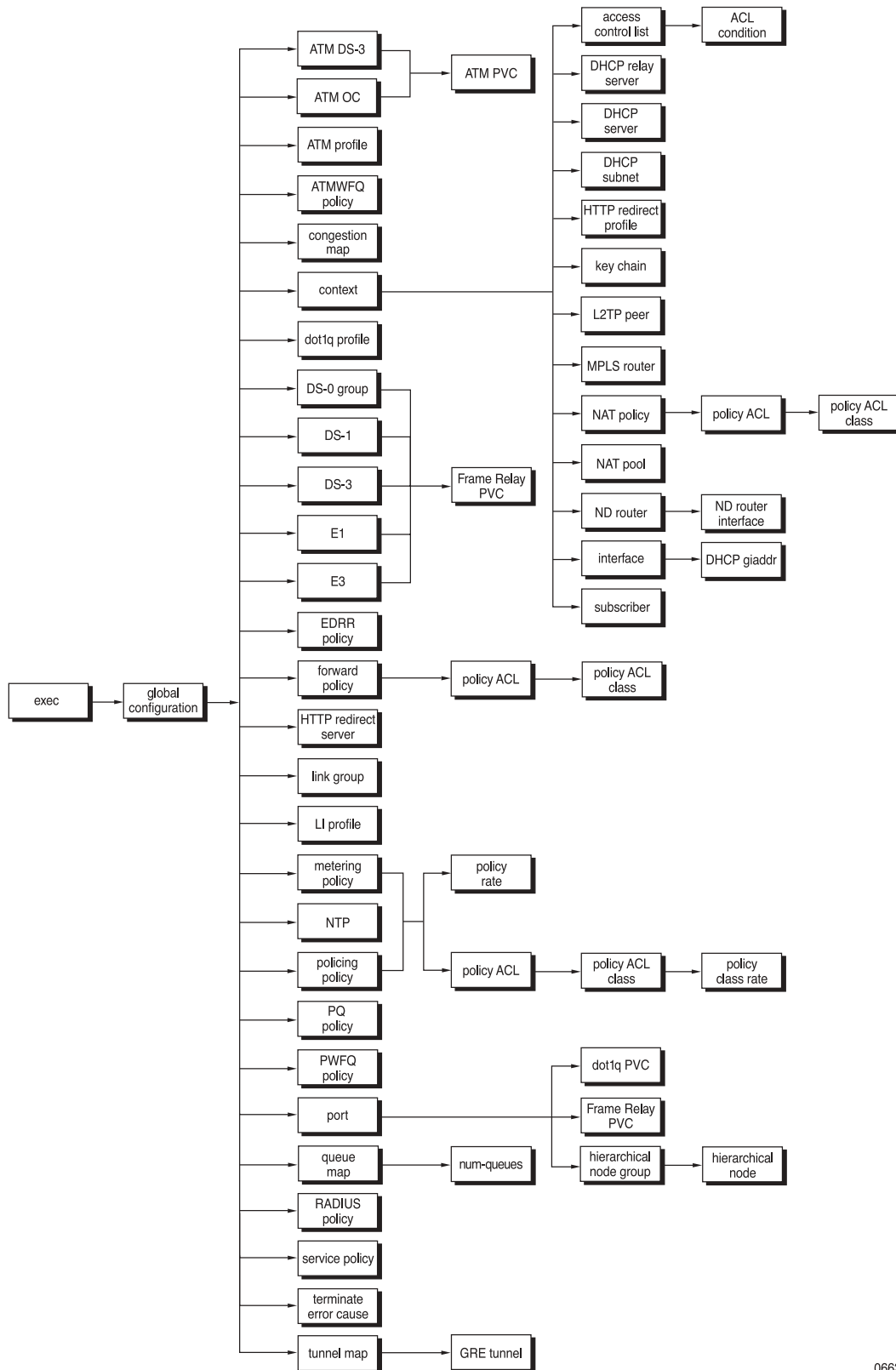
---

Command modes exist in a hierarchy; that is, you must access the higher-level command mode before you can access a lower-level command mode in the same chain.

**Note** For modes relevant to basic system features, see the “Overview” chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For modes relevant to configuring ports, circuits, and tunnels, see the “Overview” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS. For modes relevant to routing protocol features, see the “Overview” chapter in the *Routing Protocols Configuration Guide* for the SmartEdge OS.

Figure 1-2 shows the hierarchy of the command modes that are used to configure IP services and security features.

Figure 1-2 Command Modes Related to IP Services and Security Features



0663



Table 1-2 lists the command modes (in alphabetical order) that are relevant to IP services and security features. It includes the commands to access each mode and the command-line prompt for each mode.

**Table 1-2 Command Modes and Prompts**

| Mode Name                      | Commands Used to Access                                                                          | Command-Line Prompt      |
|--------------------------------|--------------------------------------------------------------------------------------------------|--------------------------|
| exec                           | (user logon)                                                                                     | # or >                   |
| access control list            | <b>ip access-list</b> and <b>policy access-list</b> commands from context configuration mode     | (config-access-list)#    |
| ACL condition                  | <b>condition time-range</b> command from access control list configuration mode                  | (config-acl-condition)#  |
| ATM DS-3                       | <b>port atm</b> command from global configuration mode                                           | (config-atm-ds3)#        |
| ATM OC                         | <b>port atm</b> command from global configuration mode                                           | (config-atm-oc)#         |
| ATM profile                    | <b>atm profile</b> command from global configuration mode                                        | (config-atm-profile)#    |
| ATM PVC                        | <b>atm pvc</b> command from ATM OC and ATM DS-3 configuration modes                              | (config-atm-pvc)#        |
| ATMWFQ policy                  | <b>qos policy atmwfq</b> command from global configuration mode                                  | (config-policy-atmwfq)#  |
| CLIPS PVC                      | <b>clips pvc</b> command from ATM PVC, dot1q PVC, and port configuration modes                   | (config-clips-pvc)#      |
| congestion map                 | <b>qos congestion-avoidance-map</b> command from global configuration mode                       | (config-congestion-map)# |
| context                        | <b>context</b> command from global configuration mode                                            | (config-ctx)#            |
| DHCP giaddr                    | <b>dhcp relay or dhcp proxy</b> command from interface configuration mode                        | (config-dhcp-giaddr)#    |
| DHCP relay server              | <b>dhcp relay server</b> command from context configuration mode                                 | (config-dhcp-relay)#     |
| DHCP server                    | <b>dhcp server</b> command from context configuration mode                                       | (config-dhcp-server)#    |
| DHCP subnet                    | <b>subnet</b> command from context configuration mode                                            | (config-dhcp-subnet)#    |
| dot1q profile                  | <b>dot1q profile</b> command from global configuration mode                                      | (config-dot1q-profile)#  |
| dot1q PVC                      | <b>dot1q pvc</b> command from port configuration mode                                            | (config-dot1q-pvc)#      |
| DS-0 group                     | <b>port ds0s</b> command from global configuration mode                                          | (config-ds0-group)#      |
| DS-1                           | <b>port ds1</b> command from global configuration mode                                           | (config-ds1)#            |
| DS-3                           | <b>port channelized-ds3</b> and <b>port ds3</b> commands from global configuration mode          | (config-ds3)#            |
| E1                             | <b>port e1</b> command from global configuration mode                                            | (config-e1)#             |
| E3                             | <b>port e3</b> command from global configuration mode                                            | (config-e3)#             |
| EDRR policy                    | <b>qos policy edrr</b> command from global configuration mode                                    | (config-policy-edrr)#    |
| forward policy                 | <b>forward policy</b> command from global configuration mode                                     | (config-policy-frwd)#    |
| Frame Relay PVC                | <b>frame-relay pvc</b> command from DS-0 group, DS-1, DS-3, E1, E3, and port configuration modes | (config-fr-pvc)#         |
| global                         | <b>configure</b> command from exec mode                                                          | (config)#                |
| GRE tunnel                     | <b>gre-tunnel</b> command from tunnel map configuration mode                                     | (config-gre-tunnel)#     |
| hierarchical node group        | <b>hierarchical node-group</b> command from port configuration mode                              | (config-h-node)#         |
| hierarchical node <sup>1</sup> | <b>hierarchical qos node</b> command from hierarchical node group configuration mode             | (config-h-node)#         |
| HTTP redirect profile          | <b>http-redirect profile</b> command from context configuration mode                             | (config-hr-profile)#     |

**Table 1-2 Command Modes and Prompts** (*continued*)

| Mode Name             | Commands Used to Access                                                                                               | Command-Line Prompt         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------|
| HTTP redirect server  | <b>http-redirect server</b> command from global configuration mode                                                    | (config-hr-server)#         |
| interface             | <b>interface</b> command from context configuration mode                                                              | (config-if)#                |
| key chain             | <b>key-chain</b> command from context configuration mode                                                              | (config-key-chain)#         |
| L2TP peer             | <b>l2tp-peer</b> command from context configuration mode                                                              | (config-l2tp)#              |
| link group            | <b>link-group</b> command from global configuration mode                                                              | (config-link-group)#        |
| LI profile            | <b>li-profile</b> command from global configuration mode                                                              | (config-liprofile)#         |
| metering policy       | <b>qos policy metering</b> command from global configuration mode                                                     | (config-policy-metering)#   |
| MPLS router           | <b>router mpls</b> command from context configuration mode                                                            | (config-mpls)#              |
| NAT policy            | <b>nat policy</b> command from context configuration mode                                                             | (config-policy-nat)#        |
| NAT pool              | <b>ip nat pool</b> command from context configuration mode                                                            | (config-nat-pool)#          |
| ND router             | <b>router nd</b> command from context configuration mode                                                              | (config-nd)#                |
| ND router interface   | <b>interface</b> command from ND router configuration mode                                                            | (config-nd-if)#             |
| NTP                   | <b>ntp mode</b> command from global configuration mode                                                                | (config-ntp)#               |
| num-queues            | <b>num-queue</b> command from queue map configuration mode                                                            | (config-num-queues)#        |
| policing policy       | <b>qos policy policing</b> command from global configuration mode                                                     | (config-policy-policing)#   |
| policy ACL            | <b>access-group</b> command from forward policy, NAT policy, metering policy, and policing policy configuration modes | (config-policy-acl)#        |
| policy ACL class      | <b>class</b> command from policy ACL configuration mode                                                               | (config-policy-acl-class)#  |
| policy class rate     | <b>rate</b> command from policy ACL class configuration mode                                                          | (config-policy-class-rate)# |
| policy rate           | <b>rate</b> command from metering policy and policing policy configuration modes                                      | (config-policy-rate)#       |
| port                  | <b>port channelized-OC12</b> , <b>port ethernet</b> , and <b>port pos</b> commands from global configuration mode     | (config-port)#              |
| PQ policy             | <b>qos policy pq</b> command from global configuration mode                                                           | (config-policy-pq)#         |
| PWFQ policy           | <b>qos policy pwfq</b> command from global configuration mode                                                         | (config-policy-pwfq)#       |
| queue map             | <b>qos queue-map</b> command from global configuration mode                                                           | (config-queue-map)#         |
| RADIUS policy         | <b>radius policy</b> command from global configuration mode                                                           | (config-rad-policy)#        |
| service policy        | <b>service-policy</b> command from global configuration mode                                                          | (config-policy-svc)#        |
| subscriber            | <b>subscriber</b> command from context configuration mode                                                             | (config-sub)#               |
| terminate error cause | <b>radius attribute acct-terminate-cause remap</b> command in global configuration mode                               | (config-term-ec)#           |
| tunnel map            | <b>tunnel map</b> command from global configuration mode                                                              | (config-tunnel-map)#        |

1. The prompt for this configuration mode is identical to the prompt for the hierarchical node group configuration mode.

# IP Service Protocols

---

This part describes the tasks and commands used to configure Address Resolution Protocol (ARP), the Neighbor Discovery (ND) protocol, Dynamic Host Configuration Protocol (DHCP), and Network Time Protocol (NTP). It consists of the following chapters:

- Chapter 2, “ARP Configuration”
- Chapter 3, “ND Configuration”
- Chapter 5, “DHCP Configuration”
- Chapter 4, “NTP Configuration”



# ARP Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS Address Resolution Protocol (ARP) features.

For information about the tasks and commands used to monitor, troubleshoot, and administer ARP features, see the “ARP Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

The SmartEdge OS supports RFC 826, *An Ethernet Address Resolution Protocol*, also called, *Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. In addition, the SmartEdge OS supports a configurable ARP entry age timer and the option to enable automatic deletion of dynamic ARP entries (as opposed to automatic refresh of the ARP table).

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure ARP, perform the tasks described in the following sections:

- Enable ARP
- Enable Secured ARP (Optional)
- Enable Proxy ARP (Optional)

- Configure Static Entries in the ARP Table (Optional)
- Configure the Automatic Deletion of ARP Entries (Optional)
- Set a Maximum Number of Incomplete ARP Entries (Optional)

## Enable ARP

To enable ARP, perform the task described in Table 2-1.

**Table 2-1 Enable ARP**

| Task        | Root Command       | Notes                                                                                                                                             |
|-------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable ARP. | <b>ip arp arpa</b> | Enter this command in interface configuration mode.<br>By default, ARP is already enabled. Use the <b>no</b> form of this command to disable ARP. |

## Enable Secured ARP (Optional)

To enable secured ARP, perform the task described in Table 2-2. You can enable either secured ARP or proxy ARP on an interface.

**Table 2-2 Enable Secured ARP (Optional)**

| Task                | Root Command              | Notes                                                                                                         |
|---------------------|---------------------------|---------------------------------------------------------------------------------------------------------------|
| Enable secured ARP. | <b>ip arp secured-arp</b> | Enter this command in interface configuration mode.<br>ARP must be enabled before you can enable secured ARP. |

## Enable Proxy ARP (Optional)

To enable proxy ARP, perform the task described in Table 2-3. You can enable either secured ARP or proxy ARP on an interface.

**Table 2-3 Enable Proxy ARP (Optional)**

| Task              | Root Command            | Notes                                                                                                       |
|-------------------|-------------------------|-------------------------------------------------------------------------------------------------------------|
| Enable proxy ARP. | <b>ip arp proxy-arp</b> | Enter this command in interface configuration mode.<br>ARP must be enabled before you can enable proxy ARP. |

## Configure Static Entries in the ARP Table (Optional)

To configure static entries in the ARP table, perform the appropriate task described in Table 2-4. If you use both commands to specify the same IP address and medium access control (MAC) address, the most recently updated command takes precedence.

**Table 2-4** Configure Static Entries in the ARP Table (Optional)

| Task                                                                                                                      | Root Command             | Notes                                                |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------------------------------|
| Configure an entry in the ARP table for a subscriber whose host cannot (or is not configured to) respond to ARP requests. | <b>ip subscriber arp</b> | Enter this command in subscriber configuration mode. |
| Configure an entry in the ARP table.                                                                                      | <b>ip arp</b>            | Enter this command in context configuration mode.    |

## Configure the Automatic Deletion of ARP Entries (Optional)

To configure the automatic deletion of ARP table entries, perform the tasks described in Table 2-5; enter all commands in interface configuration mode.

**Table 2-5** Configure the Automatic Deletion of ARP Entries

| Task                                                                                          | Root Command                 | Notes                                                                                                                |
|-----------------------------------------------------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Configure the automatic deletion of ARP entries.                                              | <b>ip arp delete-expired</b> |                                                                                                                      |
| Modify the length of time entries remain in the ARP table before being automatically deleted. | <b>ip arp timeout</b>        | Optional. When you enable the <b>ip arp delete-expired</b> command, entries are deleted after 60 minutes by default. |

## Set a Maximum Number of Incomplete ARP Entries (Optional)

When requesting the MAC address that corresponds to a particular IP address for a subscriber circuit, the SmartEdge OS creates an incomplete entry in the ARP table and sends an ARP request packet. On reply, the entry is updated and completed. By default, the maximum number of incomplete entries that are allowed in the ARP table is 4,294,967,295.

To set a maximum allowable number of incomplete entries, perform the task described in Table 2-6.

**Table 2-6** Set a Maximum Number of Incomplete ARP Entries (Optional)

| Task                                                      | Root Command                             | Notes                                             |
|-----------------------------------------------------------|------------------------------------------|---------------------------------------------------|
| Set a maximum allowable number of incomplete ARP entries. | <b>ip arp maximum incomplete-entries</b> | Enter this command in context configuration mode. |

## Configuration Examples

---

The following example enables secured ARP on the interface, `intf-1`:

```
[local]Redback(config-ctx)#interface intf-1  
[local]Redback(config-if)#ip arp secured-arp
```

The following example creates a static entry in the ARP table for IP address, `31.22.213.124`, and associates the IP address with the MAC address, `43:32:23:32:12:82`. After 4 minutes (240 seconds), any ARP entry associated with the `intf-2` interface is deleted from the ARP table.

```
[local]Redback(config-ctx)#ip arp 31.22.213.124 43:32:23:32:12:82  
[local]Redback(config-ctx)#interface intf-2  
[local]Redback(config-if)#ip arp delete-expired  
[local]Redback(config-if)#ip arp timeout 240
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure ARP features. The commands are presented in alphabetical order.

|                                          |                           |
|------------------------------------------|---------------------------|
| <b>ip arp</b>                            | <b>ip arp proxy-arp</b>   |
| <b>ip arp arpa</b>                       | <b>ip arp secured-arp</b> |
| <b>ip arp delete-expired</b>             | <b>ip arp timeout</b>     |
| <b>ip arp maximum incomplete-entries</b> | <b>ip subscriber arp</b>  |



## ip arp

**ip arp** *ip-addr mac-addr* [**alias**]

**no ip arp** *ip-addr mac-addr* [**alias**]

### Purpose

Associates an IP address with a medium access control (MAC) address and creates a corresponding entry in the Address Resolution Protocol (ARP) table.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                                |
|-----------------|--------------------------------------------------------------------------------|
| <i>ip-addr</i>  | Host IP address in the form <i>A.B.C.D</i> .                                   |
| <i>mac-addr</i> | MAC address of the host in the form <i>hh:hh:hh:hh:hh:hh</i> .                 |
| <b>alias</b>    | Optional. Configures the system to respond to ARP requests for the IP address. |

### Default

No entry is created in the ARP table.

### Usage Guidelines

Use the **ip arp** command to associate an IP address with a MAC address and create a corresponding entry in the ARP table.

**Note** If you enter both this command and the **ip subscriber arp** command (in subscriber configuration mode) and specify the same IP address and MAC address, the most recently updated command takes precedence. Only the circuit and interface are updated in the ARP table.

Use the **no** form of this command to remove an entry from the configuration and from the ARP table.

### Examples

The following example associates IP address, 31.22.213.124, with the MAC address, 00:30:23:32:12:82, and creates a corresponding entry in the ARP table:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#ip arp 31.22.213.124 00:30:23:32:12:82
```

### Related Commands

**ip subscriber arp**

## ip arp arpa

**ip arp arpa**  
**no ip arp arpa**  
**default ip arp arpa**

### Purpose

Enables the standard Address Resolution Protocol (ARP) on this interface.

### Command Mode

interface configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Standard ARP is enabled.

### Usage Guidelines

Use the **ip arp arpa** command to enable standard ARP on this interface.

Use the **no** form of this command to disable standard ARP on this interface.

Use the **default** form of this command to enable standard ARP on this interface.

### Examples

The following example disables standard ARP on the toToronto interface at IP address, 10.20.1.1:

```
[local]Redback(config-ctx)#interface toToronto  
[local]Redback(config-if)#ip address 10.20.1.1 255.255.255.0  
[local]Redback(config-if)#no ip arp arpa
```

### Related Commands

**ip arp**

# ip arp delete-expired

**ip arp delete-expired**

**{no | default} ip arp delete-expired**

## Purpose

Enables the automatic deletion of expired dynamic Address Resolution Protocol (ARP) entries associated with this interface from the ARP table.

## Command Mode

interface configuration

## Syntax Description

This command has no keywords or arguments.

## Default

Automatic deletion is disabled.

## Usage Guidelines

Use the **ip arp delete-expired** command to enable the automatic deletion of expired dynamic ARP entries associated with this interface from the ARP table. Entries are deleted after they have been in the ARP table for the amount of time specified by the **ip arp timeout** command (in interface configuration mode). If the **ip arp timeout** command is not configured, the default value of 3,600 seconds (60 minutes) is used.

If you do not enable automatic deletion of expired dynamic ARP entries, expired entries are treated differently depending on the value of the *seconds* argument in the **ip arp timeout** command. If the value of the *seconds* argument is greater than 70, an ARP entry is refreshed unless no ARP reply is received in response to the refresh request packet. In that case, the entry is removed from the cache. If the value of the *seconds* argument is less than 70, expired entries are removed from the cache.

Use the **no** or **default** form of this command to disable the automatic deletion of expired entries.

## Examples

The following example configures the system to automatically delete expired dynamic ARP entries on the toBoston interface at IP address, 10.30.2.1:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface toBoston
[local]Redback(config-if)#ip address 10.30.2.1 255.255.255.0
[local]Redback(config-if)#ip arp delete-expired
```

## Related Commands

**ip arp maximum incomplete-entries**

**ip arp timeout**

## ip arp maximum incomplete-entries

**ip arp maximum incomplete-entries** *num-entries*

{**no** | **default**} **ip arp maximum incomplete-entries**

### Purpose

Sets a maximum allowable number of incomplete entries for subscriber circuits that can exist in the Address Resolution Protocol (ARP) table for the context.

### Command Mode

context configuration

### Syntax Description

|                    |                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <i>num-entries</i> | Maximum number of incomplete entries in the ARP table. The range of values is 1 to 4,294,967,295; the default value is 4,294,967,295. |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|

### Default

The maximum number of incomplete entries for subscriber circuits in the ARP table is 4,294,967,295.

### Usage Guidelines

Use the **ip arp maximum incomplete-entries** command to set a maximum allowable number of incomplete entries for subscriber circuits that can exist in the ARP table for the context.

When requesting the medium access control (MAC) address that corresponds to a particular IP address, the SmartEdge OS creates an incomplete entry in the ARP table and sends an ARP request packet. On reply, the entry is updated and complete.

Use the **no** or **default** form of this command to return to the default setting of a maximum of 4,294,967,295 incomplete entries for subscriber circuits in the ARP table.

### Examples

The following example limits the number of incomplete entries in the ARP table to 250 for the `local` context:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#ip arp maximum 250
```

### Related Commands

**ip arp delete-expired**

**ip arp timeout**

## ip arp proxy-arp

**ip arp proxy-arp [always]**  
**{no | default} ip arp proxy-arp**

### Purpose

Enables the proxy Address Resolution Protocol (ARP) on this interface.

### Command Mode

interface configuration

### Syntax Description

|               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>always</b> | Optional. Indicates that proxy ARP must be functional for multiple hosts on the same circuit. |
|---------------|-----------------------------------------------------------------------------------------------|

### Default

Proxy ARP is disabled.

### Usage Guidelines

Use the **ip arp proxy-arp** command to enable proxy ARP on this interface. When enabled, the SmartEdge router acts as an ARP proxy for hosts that are not on the same interface as the ARP request sender.

**Note** You must enable standard ARP on this interface before you can enable proxy ARP; by default, standard ARP is enabled.

Proxy ARP and secured ARP are mutually exclusive services for an interface; enabling either service for an interface automatically disables the other service for that interface.

Use the **always** keyword to enable proxy ARP for multiple hosts that reside on the same circuit; if not specified, this capability is limited to hosts on individual circuits.

Use the **no** or **default** form of this command to disable proxy ARP on this interface.

**Note** To disable only the support for multiple hosts on the same circuit, you must first disable proxy ARP, and then enable it without the **always** keyword.

### Examples

The following example enables proxy ARP on the `fromBoston` interface at IP address, `10.2.3.4`, for all hosts on the circuit:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface fromBoston
[local]Redback(config-if)#ip address 10.2.3.4 255.255.255.0
[local]Redback(config-if)#ip arp proxy-arp always
```

## Related Commands

`ip arp arpa`

## ip arp secured-arp

**ip arp secured-arp** [**always**]  
**{no | default} ip arp secured-arp**

### Purpose

Enables the secured Address Resolution Protocol (ARP) on a specified interface.

### Command Mode

interface configuration

### Syntax Description

|               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>always</b> | Optional. Indicates that proxy ARP must be functional for multiple hosts on the same circuit. |
|---------------|-----------------------------------------------------------------------------------------------|

### Default

Secured ARP is disabled.

### Usage Guidelines

Use the **ip arp secured-arp** command to enable secured ARP on a specified interface.

**Note** You must enable standard ARP on this interface before you can enable secured ARP; by default, standard ARP is enabled.

Secured ARP and proxy ARP are mutually exclusive services for an interface; enabling either service for an interface automatically disables the other service for the same interface.

Use the **always** keyword to enable secured ARP for multiple hosts that reside on the same circuit; if not specified, this capability is limited to hosts on individual circuits.

When secured ARP is enabled, ARP requests received on an interface are not answered unless the request comes from the circuit known to contain the requesting host. ARP requests are sent by the interface only on the circuit known to contain the target host, and are not flooded to all circuits bound to an interface.

Use the **no** or **default** form of this command to disable secured ARP on this interface.

**Note** To disable only the support for multiple hosts on the same circuit, you must first disable secured ARP, and then enable it without the **always** keyword.

### Examples

The following example enables secured ARP on the interface, **sec-arp**, at IP address, **10.1.1.1**, for all hosts on the circuit:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface sec-arp
[local]Redback(config-if)#ip address 10.1.1.1 255.255.255.0
[local]Redback(config-if)#ip arp secured-arp always
```

## Related Commands

`ip arp arpa`



## ip arp timeout

**ip arp timeout** *seconds*

**{no | default} ip arp timeout**

### Purpose

Configures how long Address Resolution Protocol (ARP) entries remain in the ARP table before automatic deletion (if configured).

### Command Mode

interface configuration

### Syntax Description

|                |                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <i>seconds</i> | Number of seconds after which an ARP entry is deleted from the ARP table. The range of values is 0 to 4,294,967; the default value is 3,600. |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|

### Default

ARP entries remain in the table for 3,600 seconds (one hour).

### Usage Guidelines

Use the **ip arp timeout** command to specify how long ARP entries remain in the ARP table.

If you do not use the **ip arp delete-expired** command (in interface configuration mode) to enable the automatic deletion of expired dynamic ARP entries, expired entries are treated differently depending on the value of the *seconds* argument in the **ip arp timeout** command. If the value of the *seconds* argument is greater than 70, an ARP entry is refreshed unless no ARP reply is received in response to the refresh request packet. In that case, the entry is removed from the cache. If the value of the *seconds* argument is less than 70, expired entries are removed from the cache.

Use the **no** or **default** form of this command to restore the timeout setting to its default value of 3,600 seconds.

### Examples

The following example sets the ARP timeout value for the toToronto interface at IP address, 10.30.2.1, to two hours (7200 seconds):

```
[local]Redback(config-ctx)#interface toToronto
[local]Redback(config-if)#ip address 10.30.2.1 255.255.255.0
[local]Redback(config-if)#ip arp timeout 7200
```

## Related Commands

`ip arp arpa`  
`ip arp delete-expired`  
`ip arp proxy-arp`

## ip subscriber arp

**ip subscriber arp** *ip-addr mac-addr*

**no ip subscriber arp** *ip-addr*

### Purpose

Creates an entry in the Address Resolution Protocol (ARP) cache for a subscriber whose host cannot (or is not configured to) respond to ARP requests.

### Command Mode

subscriber configuration

### Syntax Description

|                 |                                                               |
|-----------------|---------------------------------------------------------------|
| <i>ip-addr</i>  | IP address of the subscriber's host.                          |
| <i>mac-addr</i> | Medium access control (MAC) address of the subscriber's host. |

### Default

None

### Usage Guidelines

Use the **ip subscriber arp** command to create an entry in the ARP cache for a subscriber whose host cannot (or is not configured to) respond to ARP requests.

**Note** This command is available only if you are configuring a named subscriber record and is only relevant for circuits with RFC 1483 bridged-encapsulation.

**Note** If you enter both the **ip subscriber arp** and the **ip arp** commands (in subscriber and context configuration modes, respectively), and specify the same IP address and MAC address, the most recently updated command takes precedence. Only the circuit and interface are updated in the ARP table.

Use the **no** form of this command to remove the specified entry.

### Examples

The following example configures an ARP cache entry for a host with IP address, 10.1.1.1, and hardware address, d3:9f:23:46:77:13, for the NoGrokARPs subscriber. The entry is installed into the ARP cache of the appropriate interface when the circuit is brought up.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#subscriber name NoGrokARPs
[local]Redback(config-sub)#ip address 10.1.1.1
[local]Redback(config-sub)#ip subscriber arp 10.1.1.1 d3:9f:23:46:77:13
```

## Related Commands

`ip arp`

# ND Configuration

---

The SmartEdge® routers use the Neighbor Discovery (ND) protocol for IP Version 6 (IPv6) to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. This chapter describes the tasks and commands used to configure the ND protocol through the SmartEdge OS.

For information about the tasks and commands used to monitor, troubleshoot, and administer the ND protocol, see the “ND Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

**Note** When IPv6 addresses are not referenced or explicitly specified, the term, IP address, can refer generally to IP Version 4 (IPv4) addresses, IPv6 addresses, or IP addressing. In instances where IPv6 addresses are referenced or explicitly specified, the term, IP address, refers only to IPv4 addresses. For a description of IPv6 addressing and the types of IPv6 addresses, see RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

The IPv6 ND protocol for the SmartEdge OS corresponds to a combination of the IPv4 Address Resolution Protocol (ARP) and Internet Control Management Protocol (ICMP) Router Discovery. The ND protocol is described in RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*.

The ND protocol provides many improvements over the IPv4 set of protocols, some of which are included here:

- Router advertisement messages carry link-layer addresses; no additional packet exchange is needed to resolve the router's link-layer address.
- Router advertisement messages carry prefixes for a link; there is no need to have a separate mechanism to configure the netmask.

- Router advertisement messages enable address autoconfiguration.
- Routers can advertise an maximum transmission unit (MTU) for use on the link, ensuring that all nodes use the same MTU value on links that lack a well-defined MTU.
- Address resolution multicasts are spread over 4 billion ( $2^{32}$ ) multicast addresses, greatly reducing address resolution related interrupts on nodes other than the target node. Moreover, non-IPv6 routers should not be interrupted at all.
- Multiple prefixes can be associated with the same link. Routers can be configured to omit some or all prefixes from Router Advertisement messages. In such cases, hosts assume that destinations are off-link and send traffic to routers.
- Neighbor Unreachability Detection is part of the base protocol, significantly improving the robustness of packet delivery in the presence of failing routers, partially failing or partitioned links, and nodes that change their link-layer addresses.
- Unlike ARP, ND detects half-link failures (using Neighbor Unreachability Detection) and avoids sending traffic to neighbors with which two-way connectivity is absent.
- Unlike in IPv4 Router Discovery, the Router Advertisement messages do not contain a preference field. The preference field is not needed to handle routers of different stability; the Neighbor Unreachability Detection detects a dead router and switches to a working one.
- Requiring the hop limit to be equal to 255 makes ND immune to off-link senders that accidentally or intentionally send ND messages. In IPv4, off-link senders can send Router Advertisement messages.
- Placing address resolution at the ICMP layer makes the ND protocol more media-independent than ARP and makes it possible to use standard IP authentication and security mechanisms as appropriate.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure an ND router, perform the tasks described in Table 3-1; enter all commands in ND router configuration mode, unless otherwise noted. For more information about the **context**, **interface**, and **ipv6 address** commands (in global, context, and interface configuration modes, respectively), see the “Context Configuration” and “Interface Configuration” chapters in the *Basic System Configuration Guide* for the SmartEdge OS.

**Table 3-1** Configure an ND Router

| #  | Task                                            | Root Command        | Notes                                               |
|----|-------------------------------------------------|---------------------|-----------------------------------------------------|
| 1. | Create or select the context for the ND router. | <b>context</b>      | Enter this command in global configuration mode.    |
| 2. | Create the interface for the ND router.         | <b>interface</b>    | Enter this command in context configuration mode.   |
| 3. | Specify an IPv6 IP address for the interface.   | <b>ipv6 address</b> | Enter this command in interface configuration mode. |

**Table 3-1** Configure an ND Router (*continued*)

| #  | Task                                                                                                          | Root Command              | Notes                                                                        |
|----|---------------------------------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------|
| 4. | Create the ND router and access ND router configuration mode.                                                 | <b>router nd</b>          | Enter this command in context configuration mode.                            |
| 5. | Optional. Configure global settings for the ND router using one or more of the following tasks, in any order: |                           | Each of the commands is prefaced with the <b>global</b> keyword.             |
|    | Specify the value for the Retrans Timer field.                                                                | <b>ns-interval</b>        |                                                                              |
|    | Specify the value for the Preferred Lifetime field.                                                           | <b>preferred-lifetime</b> |                                                                              |
|    | Configure RA messages.                                                                                        | <b>ra</b>                 | You can enter this command multiple times to configure different parameters. |
|    | Specify the value for the Reachable Time field.                                                               | <b>reachable-time</b>     |                                                                              |
|    | Specify the value for the Valid Lifetime field.                                                               | <b>valid-lifetime</b>     |                                                                              |

To configure an interface for an ND router, perform the tasks described in Table 3-2; enter all commands in ND router interface configuration mode, unless otherwise noted.

**Table 3-2** Configure an ND Router Interface

| #  | Task                                                                                                       | Root Command              | Notes                                                                        |
|----|------------------------------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------|
| 1. | Select the context for the ND router.                                                                      | <b>context</b>            | Enter this command in global configuration mode.                             |
| 2. | Select the ND router and access ND router configuration mode.                                              | <b>router nd</b>          | Enter this command in context configuration mode.                            |
| 3. | Select an existing interface and access ND router interface configuration mode.                            | <b>interface</b>          | Enter this command in ND router configuration mode.                          |
| 4. | Optional Configure the settings for this interface using one or more of the following tasks, in any order: |                           | Unspecified settings default to the ND router global settings.               |
|    | Specify the value for the Retrans Timer field.                                                             | <b>ns-interval</b>        |                                                                              |
|    | Specify the value for the Preferred Lifetime field.                                                        | <b>preferred-lifetime</b> |                                                                              |
|    | Configure RA messages.                                                                                     | <b>ra</b>                 | You can enter this command multiple times to configure different parameters. |
|    | Specify the value for the Reachable Time field.                                                            | <b>reachable-time</b>     |                                                                              |
|    | Specify the value for the Valid Lifetime field.                                                            | <b>valid-lifetime</b>     |                                                                              |
| 5. | Specify a static neighbor for this interface.                                                              | <b>neighbor</b>           | You can enter this command multiple times.                                   |
| 6. | Configure a prefix to be advertised for this interface.                                                    | <b>prefix</b>             | You can enter this command multiple times.                                   |

## Configuration Examples

---

The following example configures an ND router in the `local` context and the `int1` interface for the ND router:

```
! Create or select the context
[local]Redback(config)#context local
! Create the interface with an IPv6 IP address
[local]Redback(config-ctx)#interface int1
[local]Redback(config-if)#ipv6 address 2005::1/64
[local]Redback(config-if)#exit
! Create the ND router; specify global parameters for all ND interfaces in this context
! The global settings override the default settings
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#global ns-interval 100
[local]Redback(config-nd-if)#global preferred-lifetime 43200
[local]Redback(config-nd)#global ra interval 60
[local]Redback(config-nd)#global ra lifetime 360
[local]Redback(config-nd-if)#global reachable-time 1800
[local]Redback(config-nd-if)#global valid-lifetime 43200
! Select an interface
[local]Redback(config-nd)#interface int1
! Specify interface-specific parameters; the interface settings override the global
settings
[local]Redback(config-nd-if)#ns-interval 20
[local]Redback(config-nd-if)#preferred-lifetime 2880
[local]Redback(config-nd-if)#ra suppress
[local]Redback(config-nd-if)#valid-lifetime 2880
! Specify one or more static neighbors for this interface
[local]Redback(config-nd-if)#neighbor 2006::1/64 00:30:88:00:0a:30
! Specify one or more prefixes and their parameters; the prefix settings override the
interface settings
[local]Redback(config-nd-if)#prefix 2006::1/64 no-autoconfig no-onlink
preferred-lifetime 360 valid-lifetime 360
[local]Redback(config-nd-if)#prefix 2007::/112
[local]Redback(config-ctx)#
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure the ND protocol. The commands are presented in alphabetical order.

|                           |                       |
|---------------------------|-----------------------|
| <b>interface</b>          | <b>ra</b>             |
| <b>neighbor</b>           | <b>reachable-time</b> |
| <b>ns-interval</b>        | <b>router nd</b>      |
| <b>preferred-lifetime</b> | <b>valid-lifetime</b> |
| <b>prefix</b>             |                       |



# interface

**interface** *if-name*

**no interface** *if-name*

## Purpose

Selects the interface to be configured for the Neighbor Discovery (ND) protocol and accesses ND router interface configuration mode.

## Command Mode

ND router configuration

## Syntax Description

*if-name*      Name of the ND router interface.

## Default

None

## Usage Guidelines

Use the **interface** command to select the interface to be configured for the ND router protocol and access ND router interface configuration mode.

You must have already created the interface with the **interface** command (in context configuration mode). You must also have assigned an IPv6 IP address to it with the **ipv6 address** command (in interface configuration mode). Both commands are described in the “Interface Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

The interface inherits the default ND parameters and any global ND parameters that you have configured for the ND router. To configure an ND parameter specific to this interface, enter the appropriate command in ND router interface configuration mode.

Use the **no** form of this command to delete the ND router configuration for the specified interface.

## Examples

The following example selects the `int1` ND router interface:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#router nd  
[local]Redback(config-nd)#interface int1  
[local]Redback(config-nd-if)#
```

Related Commands

|                           |                       |
|---------------------------|-----------------------|
| <b>neighbor</b>           | <b>ra</b>             |
| <b>ns-interval</b>        | <b>reachable-time</b> |
| <b>preferred-lifetime</b> | <b>router nd</b>      |
| <b>prefix</b>             | <b>valid-lifetime</b> |

# neighbor

**neighbor** *ipv6-addr mac-addr*  
**no neighbor** *ipv6-addr mac-addr*

## Purpose

Specifies a static neighbor for this Neighbor Discovery (ND) router interface.

## Command Mode

ND router interface configuration

## Syntax Description

|                  |                                                                       |
|------------------|-----------------------------------------------------------------------|
| <i>ipv6-addr</i> | IPv6 address for this neighbor in the format <i>A:B:C:D:E:F:G:H</i> . |
| <i>mac-addr</i>  | Medium access control (MAC) address for this neighbor.                |

## Default

No static neighbors are specified for any interface.

## Usage Guidelines

Use the **neighbor** command to specify a static neighbor for this ND router interface. Enter this command multiple times to configure more than one neighbor.

Use the **no** form of this command to delete the neighbor from the configuration for this ND router interface.

## Examples

The following example specifies a neighbor with IPv6 address, `2006::1/112`, and MAC address, `00:30:88:00:0a:30`, for the `int1` ND router interface:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#router nd  
[local]Redback(config-nd)#interface int1  
[local]Redback(config-nd-if)#neighbor 2006::1/112 00:30:88:00:0a:30
```

## Related Commands

**prefix**  
**ra**  
**reachable-time**

## ns-interval

In ND router configuration mode, the syntax is:

```
global ns-interval retrans-timer
{no | default} global ns-interval
```

In ND router interface configuration mode, the syntax is:

```
ns-interval retrans-timer
{no | default} ns-interval
```

### Purpose

Specifies the value for the Retrans Timer field.

### Command Mode

ND router configuration  
ND router interface configuration

### Syntax Description

|                      |                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>global</b>        | Specifies the global value for all interfaces. This keyword is available only in ND router configuration mode.          |
| <i>retrans-timer</i> | Value for the Retrans Timer field (in milliseconds). The range of values is 0 to 4,294,967,295; the default value is 0. |

### Default

The Retrans Timer field is 0 (unspecified).

### Usage Guidelines

Use the **ns-interval** command to specify the value for the Retrans Timer field. In ND router configuration mode, this command specifies the global value for all interfaces; in ND router interface mode, it specifies the value for this Neighbor Discovery (ND) router interface. If specified, the setting for the interface overrides the global setting.

Use the **no** or **default** form of this command to specify the default value for the Retrans Timer field.

### Examples

The following example specifies 100 milliseconds for the Retrans Timer field for the ND router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#global ns-interval 100
```

The following example specifies 20 milliseconds for the Retrans Timer field for the ND router interface, `int1`, which overrides the global setting:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#router nd  
[local]Redback(config-nd)#interface int1  
[local]Redback(config-nd-if)#ns-interval 20
```

## Related Commands

None

## preferred-lifetime

In ND router configuration mode, the syntax is:

```
global preferred-lifetime preferred-lifetime
{no | default} global preferred-lifetime
```

In ND router interface configuration mode, the syntax is:

```
preferred-lifetime preferred-lifetime
{no | default} preferred-lifetime
```

### Purpose

Specifies the value for the Preferred Lifetime field.

### Command Mode

ND router configuration  
ND router interface configuration

### Syntax Description

|                           |                                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>global</b>             | Specifies the global value for all interfaces. This keyword is available only in ND router configuration mode.                                 |
| <i>preferred-lifetime</i> | Value for the Preferred Lifetime field (in seconds). The range of values is 0 to 4,294,967,295; the default value is 604,800 seconds (7 days). |

### Default

The preferred lifetime is seven days.

### Usage Guidelines

Use the **preferred-lifetime** command to specify the value for the Preferred Lifetime field. In ND router configuration mode, this command specifies the global value for all interfaces; in ND router interface mode, it specifies the value for this Neighbor Discovery (ND) router interface. If specified, the setting for the interface overrides the global setting.

Use the **no** or **default** form of this command to specify the default value.

### Examples

The following example specifies a preferred lifetime of 43200 seconds (12 hours) for all interfaces for this ND router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#global preferred-lifetime 43200
```

The following example specifies a preferred lifetime of 2880 seconds (48 minutes) for the `int1` ND router interface, which overrides the global setting:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#router nd  
[local]Redback(config-nd)#interface int1  
[local]Redback(config-nd-if)#preferred-lifetime 2880
```

## Related Commands

`prefix`  
`valid-lifetime`

# prefix

```
prefix ipv6-prefix/length [no-autoconfig] [no-onlink] [preferred-lifetime preferred-lifetime]
[valid-lifetime valid-lifetime]

{no | default} prefix ipv6-prefix/length
```

## Purpose

Configures a prefix to be advertised for this Neighbor Discovery (ND) router interface.

## Command Mode

ND router interface configuration

## Syntax Description

|                                                     |                                                                                                                                                      |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ipv6-prefix</i>                                  | Prefix for the IPv6 address for this ND router interface in the format <i>A:B:C:D:E:F:G:H</i> .                                                      |
| <i>length</i>                                       | Number of prefix bits. The range of values is 0 to 128.                                                                                              |
| <b>no-autoconfig</b>                                | Optional. Sets the autonomous address configuration flag to not use this prefix for automatic configuration; this is the default.                    |
| <b>no-onlink</b>                                    | Optional. Sets the on-link flag to not use this prefix for on-link determination; this is the default.                                               |
| <b>preferred-lifetime</b> <i>preferred-lifetime</i> | Optional. Preferred lifetime for this prefix (in seconds). The range of values is 0 to 4,294,967,295; the default value is 604,800 seconds (7 days). |
| <b>valid-lifetime</b> <i>valid-lifetime</i>         | Optional. Valid lifetime for this prefix (in seconds). The range of values is 0 to 4,294,967,295; the default value is 2,592,000 seconds (30 days).  |

## Default

No prefix is configured for any ND router interface.

## Usage Guidelines

Use the **prefix** command to configure a prefix to be advertised for this ND router interface. Enter this command multiple times to configure more than one prefix.

Use the optional keywords and constructs to define the fields in the Prefix Information option for this prefix:

- **no-autoconfig**—Sets the autonomous address configuration flag in the Prefix Information option to FALSE.
- **no-onlink**—Sets the on-link flag to FALSE.



- **preferred-lifetime**—Specifies the value for the Preferred Lifetime field.
- **valid-lifetime**—Specifies the value for the Valid Lifetime field.

The values for the **preferred-lifetime** *preferred-lifetime* and **valid-lifetime** *valid-lifetime* constructs override the values for the interface that you specified with the **preferred-lifetime** and **valid-lifetime** commands (in ND router interface configuration mode).

Use the **no** or **default** form of this command to delete the specified prefix from this interface configuration.

## Examples

The following example configures the 5555:bbbb::22/64 prefix for the int1 ND router interface:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd)#interface int1
[local]Redback(config-nd-if)#prefix 5555:bbbb::22/64 no-autoconfig no-onlink
preferred-lifetime 360 valid-lifetime 360
```

## Related Commands

**preferred-lifetime**  
**ra**  
**valid-lifetime**

## ra

In ND router configuration mode, the syntax is:

```
global ra [interval ra-interval | lifetime ra-lifetime | managed-config | other-config | suppress]
{no | default} global ra [interval ra-interval | lifetime ra-lifetime | managed-config | other-config |
suppress]
```

In ND router interface configuration mode, the syntax is:

```
ra {enable | [interval ra-interval | lifetime ra-lifetime | managed-config | other-config | suppress]}
```

```
{no | default} ra {enable | [interval ra-interval | lifetime ra-lifetime | managed-config | other-config |
suppress]}
```

## Purpose

Configures options and settings for Router Advertisement (RA) messages.

## Command Mode

ND router configuration  
ND router interface configuration

## Syntax Description

|                                    |                                                                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>global</b>                      | Specifies global values for all interfaces. This keyword is available only in ND router configuration mode.                     |
| <b>enable</b>                      | Enables the sending of RA messages for this ND router interface. This keyword is not available in ND router configuration mode. |
| <b>interval</b> <i>ra-interval</i> | Optional. RA interval between transmissions (in seconds). The range of values is 5 to 600; the default value is 200 seconds.    |
| <b>lifetime</b> <i>ra-lifetime</i> | Optional. RA lifetime (in seconds). The range of values is 30 to 36,000; the default value is 1,800 seconds.                    |
| <b>managed-config</b>              | Optional. Sets the managed-address configuration flag in RA messages to TRUE; the default value is not set (FALSE).             |
| <b>other-config</b>                | Optional. Sets the other-stateful configuration flag in RA messages to TRUE; the default value is not set (FALSE).              |
| <b>suppress</b>                    | Optional. Specifies that RA messages be suppressed; the default value is not suppressed.                                        |

## Default

RA messages are not configured for any ND router or ND router interface.

## Usage Guidelines

Use the **ra** command to configure options and settings for RA messages. In ND router configuration mode, this command configures RA for all interfaces; in ND router interface mode, it configures RA for this ND router interface. If specified, the interface parameters override the global parameters. Enter this command multiple times to configure more than one parameter.

Use the **no** or **default** form of this command to remove RA messages from the configuration for this ND router or ND router interface.

## Examples

The following example configures RA for this ND router with a retransmission interval of 60 seconds and a lifetime of six minutes (360 seconds):

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd)#global ra interval 60
[local]Redback(config-nd)#global ra lifetime 360
```

The following example suppresses RA for the `int1` ND router interface:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd)#interface int1
[local]Redback(config-nd-if)#ra suppress
```

## Related Commands

**prefix**  
**reachable-time**

## reachable-time

In ND router configuration mode, the syntax is:

**global reachable-time** *duration*

{**no** | **default**} **global reachable-time**

In ND router interface configuration mode, the syntax is:

**reachable-time** *duration*

{**no** | **default**} **reachable-time**

### Purpose

Specifies the value for the Reachable Time field in Router Advertisement (RA) messages.

### Command Mode

ND router configuration

ND router interface configuration

### Syntax Description

|                 |                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>global</b>   | Specifies the global value for all interfaces. This keyword is available only in ND router configuration mode.                     |
| <i>duration</i> | Value for the Reachable Time field (in milliseconds). The range of values is 0 to 3,600,000; the default value is 0 (unspecified). |

### Default

The duration is unspecified in any RA messages.

### Usage Guidelines

Use the **reachable-time** command to specify the value for the Reachable Time field in RA messages. This value is the time this Neighbor Discovery (ND) router or ND router interface assumes that a neighbor is reachable. In ND router configuration mode, this command specifies the global value for all interfaces; in ND router interface mode, specifies the value for this ND router interface. If specified, the parameters for an interface override the global parameters.

Use the **no** or **default** form of this command to specify the default duration.

### Examples

The following example specifies a reachable time of 1800 milliseconds for all interfaces for the ND router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#global reachable-time 1800
```

The following example specifies a reachable time of 3600 milliseconds for the `int1` ND router interface:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#router nd  
[local]Redback(config-nd)#interface int1  
[local]Redback(config-nd-if)#reachable-time 3600
```

## Related Commands

**neighbor**  
**ra**

## router nd

**router nd**

**no router nd**

### Purpose

Creates or selects a Neighbor Discovery (ND) router and accesses ND router configuration mode.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

No ND router is created.

### Usage Guidelines

Use the **router nd** command to create or select an ND router and access ND router configuration mode. You can create a single ND router in each context.

Use the **no** form of this command to remove the ND router from the configuration; the **no** form also removes the ND-specific configuration from any interfaces in this context.

### Examples

The following example creates an ND router in the `local` context:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#router nd
```

### Related Commands

**interface**

## valid-lifetime

In ND router configuration mode, the syntax is:

**global valid-lifetime** *lifetime*

**{no | default} global valid-lifetime**

In ND router interface configuration mode, the syntax is:

**valid-lifetime** *lifetime*

**{no | default} valid-lifetime**

### Purpose

Specifies the value for the Valid Lifetime field in the Prefix Information option.

### Command Mode

ND router configuration

ND router interface configuration

### Syntax Description

|                 |                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>global</b>   | Specifies the global value for all interfaces. This keyword is available only in ND router configuration mode.                                |
| <i>lifetime</i> | Value for the Valid Lifetime field (in seconds). The range of values is 0 to 4,294,967,295; the default value is 2,592,000 seconds (30 days). |

### Default

The valid lifetime is 30 days.

### Usage Guidelines

Use the **valid-lifetime** command to specify the value for the Valid Lifetime field in the Prefix Information option. In ND router configuration mode, this command specifies the global value for all interfaces; in ND router interface mode, specifies the value for this ND router interface. If specified, the setting for the interface overrides the global setting.

Use the **no** or **default** form of this command to specify the default condition.

### Examples

The following example specifies a valid lifetime of 43200 seconds (12 hours) for all interfaces for this ND router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#global valid-lifetime 43200
```

## Command Descriptions

---

The following example specifies a valid lifetime of 2880 seconds (48 minutes) for the `int1` ND router interface, which overrides the global setting:

```
[ local]Redback(config)#context local
[ local]Redback(config-ctx)#router nd
[ local]Redback(config-nd)#interface int1
[ local]Redback(config-nd-if)#valid-lifetime 2880
```

## Related Commands

**preferred-lifetime**  
**prefix**



# NTP Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS Network Time Protocol (NTP) features.

For information about the task and commands used to monitor, troubleshoot, and administer NTP features, see the “NTP Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

NTP exchanges timekeeping information between servers and clients via the Internet to synchronize clocks. NTP makes estimates based on several variables, including network delay, dispersion of packet exchanges, and clock offset. Extremely reliable sources, such as radio clocks and Global Positioning System (GPS) satellite timing receivers, act as primary servers. Company or campus servers can act as secondary time servers. To reduce overhead, secondary servers distribute time to attached local hosts.

The SmartEdge OS supports NTP as described in RFC 1305, *Network Time Protocol*. Although the default version is Version 3, the SmartEdge OS also supports versions 1 and 2. On a SmartEdge router, NTP operates in client mode only. The SmartEdge router can be synchronized by a remote NTP server, but the remote server cannot be synchronized by the SmartEdge router.

# Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure NTP, perform the tasks described in the following sections:

- Configure the NTP Server IP Address
- Configure NTP Peer Associations (Optional)
- Configure Slowsync (Optional)

## Configure the NTP Server IP Address

To configure the NTP server IP address, perform the task described in Table 4-1.

**Table 4-1** Configure the NTP Server IP Address

| Task                                                                  | Root Command      | Notes                                            |
|-----------------------------------------------------------------------|-------------------|--------------------------------------------------|
| Configure the SmartEdge router to synchronize to a remote NTP server. | <b>ntp server</b> | Enter this command in global configuration mode. |

## Configure NTP Peer Associations (Optional)

To configure NTP peer associations, perform the task described in Table 4-2.

**Table 4-2** Configure NTP Peer Associations

| Task                                                                                                                | Root Command    | Notes                                            |
|---------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------------------|
| Configure the peer association for symmetric synchronization of the SmartEdge router time and remote NTP peer time. | <b>ntp peer</b> | Enter this command in global configuration mode. |

## Configure Slowsync (Optional)

To configure the SmartEdge router to slowly adjust its local clock rate to compensate for differences with a remote NTP clock source, perform the tasks described in Table 4-3.

**Table 4-3** Configure Slowsync

| #  | Task                           | Root Command    | Notes                                            |
|----|--------------------------------|-----------------|--------------------------------------------------|
| 1. | Access NTP configuration mode. | <b>ntp mode</b> | Enter this command in global configuration mode. |
| 2. | Configure slowsync.            | <b>slowsync</b> | Enter this command in NTP configuration mode.    |

## Configuration Examples

---

The following example configures the NTP client on the SmartEdge router to synchronize with a remote NTP server at IP address 10.1.1.1:

```
[local]Redback(config)#ntp server 10.1.1.1
```

The following commands configure the NTP client on the SmartEdge router to use multiple remote NTP servers as synchronization sources. In this case, the preferred server is at IP address, 20.1.1.1. Symmetric synchronization is also enabled, using the NTP peer with IP address, 155.53.32.75.

```
[local]Redback#config
[local]Redback(config)#ntp server 10.1.1.1
[local]Redback(config)#ntp server 20.1.1.1 prefer
[local]Redback(config)#ntp peer 155.53.32.75
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure NTP. The commands are presented in alphabetical order.

**ntp mode**  
**ntp peer**

**ntp server**  
**slowsync**

## ntp mode

**ntp mode**

### Purpose

Enters NTP configuration mode.

### Command Mode

global configuration

### Syntax Description

This command has no keywords or arguments.

### Default

None

### Usage Guidelines

Use the **ntp mode** command to enter NTP configuration mode.

### Examples

The following example changes the mode from global configuration to NTP configuration:

```
[local]Redback(config)#ntp mode  
[local]Redback(config-ntp)#
```

### Related Commands

**slowsync**

## ntp peer

**ntp peer** *ip-addr* [**context** *ctx-name*] [**prefer**] [**source** *if-name*] [**version** *ver-num*]

**no ntp peer** [*ip-addr*]

### Purpose

Configures peer association for symmetric synchronization of the SmartEdge router time and remote Network Time Protocol (NTP) peer time.

### Command Mode

global configuration

### Syntax Description

|                                |                                                                                                                                                               |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>                 | IP address of the remote NTP peer. Optional when used with the <b>no</b> form of this command.                                                                |
| <b>context</b> <i>ctx-name</i> | Optional. Context in which the destination address is reachable. This construct is used when the NTP peer must be reached through a context other than local. |
| <b>prefer</b>                  | Optional. Marks the NTP peer as the preferred peer when multiple NTP peers are configured.                                                                    |
| <b>source</b> <i>if-name</i>   | Optional. SmartEdge interface that is to be used for NTP traffic.                                                                                             |
| <b>version</b> <i>ver-num</i>  | Optional. NTP version. Version options are 1, 2, and 3; the default value is 3.                                                                               |

### Default

The context for the NTP peer is the local context. The NTP version is Version 3.

### Usage Guidelines

Use the **ntp peer** command to configure a peer association for symmetric synchronization of the SmartEdge router time and remote NTP peer time.

Use the **no** form of this command to disable NTP services on the device.



**Caution** Risk of data loss. If you use the **no** form without specifying the IP address of a specific peer, all existing NTP peer associations are removed. To reduce the risk, of losing NTP peer associations, always specify the IP address when using the **no** form.

### Examples

The following example configures the SmartEdge router to symmetrically synchronize with the remote NTP peer at IP address, 155.53.32.75. The peer is also marked as the preferred peer.

```
[local]Redback(config)#ntp peer 155.53.32.75 prefer
```

## Related Commands

`ntp server`  
`slowsync`

## ntp server

**ntp server** *ip-addr* [**context** *ctx-name*] [**prefer**] [**source** *if-name*] [**version** *ver-num*]

**no ntp server** [*ip-addr*]

### Purpose

Configures the SmartEdge router to synchronize to a remote Network Time Protocol (NTP) server.

### Command Mode

global configuration

### Syntax Description

|                                |                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>                 | IP address of the remote NTP server. Optional when used with the <b>no</b> form of this command.                                                                |
| <b>context</b> <i>ctx-name</i> | Optional. Context in which the destination address is reachable. This construct is used when the NTP server must be reached through a context other than local. |
| <b>prefer</b>                  | Optional. Marks the NTP server as the preferred server when multiple NTP servers are configured.                                                                |
| <b>source</b> <i>if-name</i>   | Optional. SmartEdge interface that is to be used for NTP traffic.                                                                                               |
| <b>version</b> <i>ver-num</i>  | Optional. NTP version. Version options are 1, 2, and 3; the default value is 3.                                                                                 |

### Default

NTP is disabled.

### Usage Guidelines

Use the **ntp server** command to start the NTP daemon and configure the SmartEdge router to synchronize to a remote NTP server.

**Note** A remote NTP client cannot synchronize with the SmartEdge router.

Use the **no** form of this command to disable NTP services on the device. If you use the **no** form without specifying the IP address of a specific server, all existing NTP server associations are removed.

### Examples

The following example configures the NTP client to synchronize with an NTP remote server at IP address, 155.53.12.12, and makes it the preferred server:

```
[local]Redback(config)#ntp server 155.53.12.12 prefer
```

**Related Commands**

ntp peer  
slowsync



# slowsync

**slowsync**

{ **no** | **default** } **slowsync**

## Purpose

Configures the SmartEdge router to slowly adjust its local clock rate to compensate for differences with a remote Network Time Protocol (NTP) clock source.

## Command Mode

NTP configuration

## Syntax

This command has no keywords or arguments.

## Default

Gradual adjustment of the local clock rate is disabled.

## Usage Guidelines

Use the **slowsync** command to configure the SmartEdge router to slowly adjust its local clock rate to compensate for differences with a remote NTP clock source.

This command changes the rate of the SmartEdge OS clock so that it gradually converges with the NTP server clock—provided the initial difference in time between the two clocks is less than 16 minutes. If the time difference is more than 16 minutes, synchronization does not occur.

The NTP daemon adjusts the SmartEdge router clock within a few minutes if the difference between the SmartEdge router clock and the remote NTP server is greater than 5 seconds (and less than 16 minutes). This adjustment occurs within the first five minutes after the NTP daemon is started.

Use the **no** or **default** form of this command to disable gradual adjustment of the local clock rate.

## Examples

The following example enables the gradual adjustment of the local clock rate:

```
[local]Redback(config-ntp)#slowsync
```

## Related Commands

**ntp peer**

**ntp server**



---

# DHCP Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS Dynamic Host Configuration Protocol (DHCP) features.

For information about the commands used to monitor, troubleshoot, and administer DHCP features, see the “DHCP Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

DHCP dynamically configures IP address information for subscriber hosts. The SmartEdge OS provides three types of DHCP support:

- DHCP relay server

The SmartEdge router acts as an intermediary between an external DHCP server and the subscriber (client). The router forwards requests from the subscriber to the DHCP server and relays the server’s responses back to the subscriber.

- DHCP proxy server

The SmartEdge router provides responses directly to subscriber requests. Each subscriber sees the router as the DHCP server, and as such, sends all DHCP negotiations, including IP address release and renewal, to the router, which then relays the information to the external DHCP server. The proxy feature enables the router to maintain IP address lease timers.

- DHCP internal

The SmartEdge router provides the functions of the DHCP server; no communications are sent to an external DHCP server.

For every valid DHCP response received from or transmitted to a subscriber, an entry is created in the Address Resolution Protocol (ARP) table. The entry includes the IP address that is assigned to the requesting medium access control (MAC) address and the incoming circuit on which the DHCP request is received. All entries are secured ARP entries. Because entries are cached in the ARP table, the SmartEdge router can route downstream packets to the correct outgoing interface. For more information about ARP, see Chapter 2, “ARP Configuration.”

Clientless IP service selection (CLIPS) exclusion allows you to configure DHCP sessions on ports and PVCs that you have also configured for dynamic CLIPS sessions. With CLIPS exclusion, you can specify which sessions are DHCP hosts; all other sessions are dynamic CLIPS sessions. CLIPS exclusion applies only the DHCP proxy and internal servers. For more information about configuring CLIPS exclusion, see the “CLIPS Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

When Remote Authentication Dial-In User Service (RADIUS) authentication is enabled, the SmartEdge router sends an accounting record to a RADIUS server each time an IP address is assigned or released.

If the Smartedge router is acting as a DHCP proxy or internal server for CLIPS subscribers, the vendor class identifier that is received in the DHCP Discover packet for the CLIPS session is sent in the RADIUS Access-Request and Accounting-Request packets to the RADIUS server, using Redback® vendor-specific attribute (VSA) 125.

For more information about RADIUS, see Chapter 16, “RADIUS Configuration.” For information about Redback VSAs, see Appendix A, “RADIUS Attributes.”

**Note** DHCP, in all modes, maintains host entries only for multibind interfaces.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure DHCP features, perform the tasks described in the following sections:

- Configure an Internal DHCP Server
- Configure an External DHCP Server
- Configure a Context for an External DHCP Server
- Configure an Interface for an External DHCP Server
- Configure Subscriber Hosts for DHCP Address Functions

## Configure an Internal DHCP Server

To configure the SmartEdge OS to act as an internal DHCP server, perform the tasks described in Table 5-1.

**Table 5-1 Configure an Internal DHCP Server**

| #  | Task                                                                                                       | Root Command              | Notes                                                                                                                                                                                                                            |
|----|------------------------------------------------------------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select the context for the DHCP internal server and access context configuration mode.           | <b>context</b>            | Enter this command in global configuration mode. This command is documented in the “Context Configuration” chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS.                                          |
| 2. | Create or select the interface for the DHCP internal server and access interface configuration mode.       | <b>interface</b>          | Enter this command in context configuration mode. Specify the <b>multibind</b> keyword. This command is documented in the “Interface Configuration” chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS. |
| 3. | Assign one or more IP addresses to this interface.                                                         | <b>ip address</b>         | Enter this command in interface configuration mode. This command is documented in the “Interface Configuration” chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS.                                     |
| 4. | Enable this interface for internal DHCP server support and assign an IP address for its support.           | <b>dhcp server</b>        | Enter this command in interface configuration mode.                                                                                                                                                                              |
| 5. | Enable internal DHCP server functions in this context and access DHCP server configuration mode.           | <b>dhcp server policy</b> | Enter this command in context configuration mode.                                                                                                                                                                                |
| 6. | Specify global settings for the DHCP server and all its subnets, using one or more of the following tasks: |                           | Enter these commands in DHCP server configuration mode.                                                                                                                                                                          |
|    | Specify the default lease time.                                                                            | <b>default-lease-time</b> |                                                                                                                                                                                                                                  |
|    | Specify the maximum lease time.                                                                            | <b>max-lease-time</b>     |                                                                                                                                                                                                                                  |
|    | Specify the offer lease time.                                                                              | <b>offer-lease-time</b>   |                                                                                                                                                                                                                                  |
|    | Specify one or more DHCP options.                                                                          | <b>option</b>             | Enter this command multiple times to specify as many options as you require.                                                                                                                                                     |
|    | Specify the filename of the boot loader image file.                                                        | <b>bootp-filename</b>     |                                                                                                                                                                                                                                  |
|    | Specify the IP address that the boot loader client uses to download the boot loader image file.            | <b>bootp-siaddr</b>       |                                                                                                                                                                                                                                  |
|    | Create a static mapping between a subnet and the specified vendor class ID.                                | <b>vendor-class</b>       |                                                                                                                                                                                                                                  |
| 7. | Create a subnet for the DHCP server and access DHCP subnet configuration mode.                             | <b>subnet</b>             | Enter this command in DHCP server configuration mode.                                                                                                                                                                            |

**Table 5-1** Configure an Internal DHCP Server (*continued*)

| #  | Task                                                                                                                                    | Root Command              | Notes                                                                        |
|----|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------|
| 8. | Optional. Configure this subnet, using one or more of the following tasks:                                                              |                           | Enter all commands in DHCP subnet configuration mode.                        |
|    | Assign a range of IP addresses to this subnet.                                                                                          | <b>range</b>              |                                                                              |
|    | Create a static mapping between a MAC address and an IP address in this subnet.                                                         | <b>mac-address</b>        |                                                                              |
|    | Create a static mapping between the agent circuit id subfield or the agent remote id subfield in the option 82 field and an IP address. | <b>option-82</b>          |                                                                              |
|    | Specify the maximum number of IP addresses allowed for an agent circuit id.                                                             | <b>option-82</b>          |                                                                              |
|    | Specify the default lease time for this subnet.                                                                                         | <b>default-lease-time</b> | These settings override the global settings for this subnet.                 |
|    | Specify the maximum lease time for this subnet.                                                                                         | <b>max-lease-time</b>     |                                                                              |
|    | Specify the offer lease time for this subnet.                                                                                           | <b>offer-lease-time</b>   |                                                                              |
|    | Specify one or more DHCP options for this subnet.                                                                                       | <b>option</b>             | Enter this command multiple times to specify as many options as you require. |

## Configure an External DHCP Server

To configure an external DHCP relay or proxy server, perform the tasks described in Table 5-2; enter all commands in DHCP relay server configuration mode, unless otherwise noted.

**Table 5-2** Configure an External DHCP Server

| #  | Task                                                                                       | Root Command             | Notes                                                                                                                    |
|----|--------------------------------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 1. | Configure an external DHCP server, and enter DHCP relay server configuration mode.         | <b>dhcp relay server</b> | Enter this command in context configuration mode. You can configure only one DHCP server IP address in a single context. |
| 2. | Configure the maximum hop count allowed for DHCP requests.                                 | <b>max-hops</b>          |                                                                                                                          |
| 3. | Configure the interval, in seconds, to wait before forwarding requests to the DHCP server. | <b>min-wait</b>          |                                                                                                                          |
| 4. | Assign the DHCP server to a DHCP server group.                                             | <b>server-group</b>      |                                                                                                                          |
| 5. | Specify forwarding for DHCP messages, using one of the following tasks:                    |                          |                                                                                                                          |
|    | • Forward packets to all other DHCP servers in the DHCP server group.                      | <b>forward-all</b>       |                                                                                                                          |
|    | • Forward packets to a standby DHCP server.                                                | <b>standby</b>           |                                                                                                                          |

## Configure a Context for an External DHCP Server

To configure a context for an external DHCP relay or proxy server, perform the tasks described in Table 5-3; enter all commands in context configuration mode.

**Table 5-3 Configure a Context for an External DHCP Server**

| Task                                                                                                                                                   | Root Command                     | Notes                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------|
| Specify the number of attempts and the interval to wait for each attempt when trying to reach an external DHCP server before it is marked unreachable. | <b>dhcp relay server retries</b> |                                                                                                          |
| Disable the sending of a DHCPNAK message if the SmartEdge OS receives a DHCPREQUEST message for which it does not have an entry.                       | <b>dhcp relay suppress-nak</b>   |                                                                                                          |
| Optional. Add the DHCP relay information option to packets.                                                                                            | <b>dhcp relay option</b>         | The DHCP relay information option is described in RFC 3046, <i>DHCP Relay Agent Information Option</i> . |

## Configure an Interface for an External DHCP Server

To configure an interface for an external DHCP relay or proxy server, perform the tasks described in Table 5-4; enter all commands in interface configuration mode, unless otherwise noted.

**Table 5-4 Configure an Interface for an External DHCP Server**

| Task                                                                                                                                                                                                                                                                                                                                                                                                        | Root Command                               | Notes                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enable the interface for an external DHCP server, using one of the following tasks: <ul style="list-style-type: none"> <li>• Enable the interface to relay DHCP messages to an external DHCP server, and access DHCP giaddr configuration mode.</li> <li>• Enable the interface to act as a proxy between subscribers and an external DHCP server, and access DHCP giaddr configuration mode.</li> </ul> | <b>dhcp relay</b><br><br><b>dhcp proxy</b> | These commands are mutually exclusive. If you are configuring CLIPS, you must use the <b>dhcp proxy</b> command.<br><br>The value for the <i>max-dhcp-addrs</i> argument used with these commands works in conjunction with the <i>max-sub-addrs</i> value specified in the <b>dhcp max-addr</b> command (in subscriber configuration mode); see the "Configure Subscriber Hosts for DHCP Address Functions" section. |
| 2. Optional. Configure an IP source address.                                                                                                                                                                                                                                                                                                                                                                | <b>ip source-address</b>                   | The interface address that you specify with this command must be reachable by the external DHCP server. You must specify the <b>dhcp-server</b> keyword.<br><br>For more information about this command, see the "Interface Configuration" chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS.                                                                                               |
| 3. Specify an IP address for the giaddr field for DHCP packets that match the specified vendor-class-id.                                                                                                                                                                                                                                                                                                    | <b>vendor-class-id</b>                     | Enter this command in DHCP giaddr configuration mode. You can enter either of these commands multiple times to specify multiple vendor-class IDs.                                                                                                                                                                                                                                                                     |

**Note** By default, the IP address of the interface on which DHCP messages are transmitted is sent in DHCP packets. To not publish this IP address, configure an interface (typically loopback) to appear to be the source address for DHCP packets.

## Configure Subscriber Hosts for DHCP Address Functions

To configure subscriber hosts for DHCP address functions, perform the tasks described in Table 5-5; enter all commands in subscriber configuration mode.

**Table 5-5 Configure Subscriber Hosts for DHCP Address Functions**

| Task                                                                                                                                                                                                          | Root Command         | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Optional. Configure hosts to use DHCP to dynamically acquire address information for a subscriber circuit and set a maximum number of IP addresses that can be assigned to hosts associated with the circuit. | <b>dhcp max-addr</b> | You can also configure this information in the subscriber record through the RADIUS database instead of through this command. Use Redback vendor-specific attribute (VSA) 3, DHCP-Max-Leases, for the maximum number of IP addresses; see Appendix A, "RADIUS Attributes."                                                                                                                                                                                             |
| Optional. Configure hosts to use a specific DHCP interface to acquire address information for a subscriber circuit.                                                                                           | <b>ip interface</b>  | <p>You must configure the subscriber record or profile with the <b>dhcp max-addr</b> command.</p> <p>You must enable the specified interface for DHCP proxy or DHCP relay; see the "Configure an Interface for an External DHCP Server" section.</p> <p>You can also configure this information in the subscriber record through the RADIUS database instead of through this command. Use Redback VSA 104, IP-Interface-Name; see Appendix A, "RADIUS Attributes."</p> |

---

## Configuration Examples

---

The following sections provide DHCP configuration examples:

- DHCP Internal Server
- DHCP Proxy and Maximum Address Support
- Subscriber Bindings to DHCP Interfaces
- DHCP Proxy Through Dynamic Subscriber Bindings
- DHCP Proxy Through Static Interface Bindings
- DHCP Proxy Through RADIUS
- Loopback Interface as DHCP Source Address

### DHCP Internal Server

The following example configures an internal DHCP server and two subnets:

```
! Create the context and the interface.
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#interface dhcp-if multibind

! Assign two subnets to the interface
[local]Redback(config-if)#ip address 12.1.1.0/24
[local]Redback(config-if)#ip address 13.1.1.0/24 secondary

! Enable the interface for internal DHCP functions and assign an IP address to it.
[local]Redback(config-if)#dhcp server 12.1.1.1
```



```
[local]Redback(config-if)#exit

! Enable the context for internal DHCP server functions.
[local]Redback(config-ctx)#dhcp server policy

! Specify global settings for the internal DHCP server and all its subnets.
[local]Redback(config-dhcp-server)#default-lease-time 14400
[local]Redback(config-dhcp-server)#maximum-lease-time 172800
[local]Redback(config-dhcp-server)#offer-lease-time 300
[local]Redback(config-dhcp-server)#option domain-name redback.com

! Specify the boot loader image file and the server IP address where it can be found
[local]Redback(config-dhcp-server)#bootp-filename of1267.bin
[local]Redback(config-dhcp-server)#bootp-siaddr 200.1.1.0

! Create an unnamed subnet and configure it.
[local]Redback(config-dhcp-server)#subnet 13.1.1.1/24
[local]Redback(config-dhcp-subnet)#range 13.1.1.50 13.1.1.99

! Override the global settings for these options.
[local]Redback(config-dhcp-subnet)#default-lease-time 3600
[local]Redback(config-dhcp-subnet)#maximum-lease-time 14400
[local]Redback(config-dhcp-subnet)#option domain-name cool.com
[local]Redback(config-dhcp-subnet)#option domain-name-servers 12.1.1.254
[local]Redback(config-dhcp-subnet)#exit

! Create a named subnet and configure it.
[local]Redback(config-dhcp-server)#subnet 13.1.1.100/24 name sub2
[local]Redback(config-dhcp-subnet)#range 13.1.1.150 13.1.1.199

!Create static mappings for this named subnet
[local]Redback(config-dhcp-subnet)#mac-address 02:12:34:56:78:90 ip-address 13.1.1.2
[local]Redback(config-dhcp-subnet)#option-82 circuit-id "4:1 vlan 102" offset 3
ip-address 13.1.1.3
[local]Redback(config-dhcp-subnet)#option-82 circuit-id "4:1 vlan 102" offset 3
max-addresses 10

! Override the global setting for this option.
[local]Redback(config-dhcp-subnet)#option domain-name hot.com
[local]Redback(config-dhcp-subnet)#exit

!Create a static mapping for this named subnet
[local]Redback(config-dhcp-server)#vendor-class "abc-client" offset 5 subnet sub2
```

## DHCP Proxy and Maximum Address Support

The following example illustrates how the value for the *max-sub-addr* argument for the **dhcp max-addr** command (in subscriber configuration mode) works in conjunction with the value for the *max-dhcp-addr* argument for the **dhcp proxy** command (in interface configuration mode). In this example, the number of DHCP clients that can be supported on the DHCP proxy multibind interface at IP address, 120.1.1.1, is restricted to 10, with the **dhcp proxy** command. The first four subscribers, each with a value of 1 for

*max-sub-addr*s, can be authenticated and a circuit can be brought up for each of them. However, subscriber sub5 cannot be authenticated because its *max-sub-addr* value is 10, which exceeds the remaining number of addresses available on the interface, which is now 6.

```
[local]Redback(config-ctx)#interface subscriber multibind
[local]Redback(config-if)#ip address 120.1.1.1/16
[local]Redback(config-if)#dhcp proxy 10
[local]Redback(config-if)#ip arp timeout 120
[local]Redback(config-if)#ip arp delete-expired
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface to-dhcp-server
[local]Redback(config-if)#ip address 100.1.1.1/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#subscriber name sub1
[local]Redback(config-sub)#dhcp max-addr 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub2
[local]Redback(config-sub)#dhcp max-addr 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub3
[local]Redback(config-sub)#dhcp max-addr 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub4
[local]Redback(config-sub)#dhcp max-addr 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub5
[local]Redback(config-sub)#dhcp max-addr 10
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#dhcp relay server 100.1.1.156
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
```

## Subscriber Bindings to DHCP Interfaces

Two examples of binding subscribers to DHCP interfaces are described in the following sections:

- Using Local Authentication
- Using RADIUS Authentication

### Using Local Authentication

The following example binds subscribers to DHCP interfaces using the **ip interface** command (in subscriber configuration mode) with local authentication:

```
[local]Redback(config)#context atm_subs
[local]Redback(config-ctx)#interface bronze multibind
[local]Redback(config-if)#ip address 120.1.3.1/24
[local]Redback(config-if)#dhcp proxy 65535
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface gold multibind
[local]Redback(config-if)#ip address 120.1.1.1/24
[local]Redback(config-if)#dhcp proxy 100
```

```

[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface silver multibind
[local]Redback(config-if)#ip address 120.1.2.1/24
[local]Redback(config-if)#dhcp proxy 10
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#subscriber profile gold
[local]Redback(config-sub)#ip interface name gold
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber profile silver
[local]Redback(config-sub)#ip interface name silver
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber profile bronze
[local]Redback(config-sub)#ip interface name bronze
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub1
[local]Redback(config-sub)#profile gold
[local]Redback(config-sub)#dhcp max-addrs 10
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub2
[local]Redback(config-sub)#profile silver
[local]Redback(config-sub)#dhcp max-addrs 10
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub3
[local]Redback(config-sub)#profile bronze
[local]Redback(config-sub)#dhcp max-addrs 10
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 1/4
[local]Redback(config-atm-oc)#no shutdown
[local]Redback(config-atm-oc)#atm pvc 0 101 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub1@atm_subs
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#atm pvc 0 102 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub2@atm_subs
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#atm pvc 0 103 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub3@atm_subs

```

The following example displays information about these subscriber circuits:

```

[atm_subs]Redback>show subscribers active

sub1@atm_subs
  Circuit    1/4:1 vpi-vci 0 101
  Internal Circuit  1/4:1:63/1/2/24579
  Current port-limit unlimited
  profile gold (applied)
  dhcp max-addrs 10 (applied)
  ip interface gold (applied)
sub2@atm_subs
  Circuit    1/4:1 vpi-vci 0 102
  Internal Circuit  1/4:1:63/1/2/24580

```

```

Current port-limit unlimited
profile silver (applied)
dhcp max-addrs 10 (applied)
ip interface silver (applied)
sub3@atm_subs
Circuit 1/4:1 vpi-vci 0 103
Internal Circuit 1/4:1:63/1/2/24581
Current port-limit unlimited
profile bronze (applied)
dhcp max-addrs 10 (applied)
ip interface bronze (applied)

```

The following example displays information about the DHCP hosts after they have been established on the active subscriber circuits:

```
[atm_subs]Redback>show subscribers active
```

```

sub1@atm_subs
Circuit 1/4:1 vpi-vci 0 101
Internal Circuit 1/4:1:63/1/2/24579
Current port-limit unlimited
profile gold (applied)
dhcp max-addrs 10 (applied)
ip interface gold (applied)
    IP host entries installed by DHCP: (max_addr 10 cur_enties 10)

    120.1.1.199    00:dd:00:00:00:0a
    120.1.1.191    00:dd:00:00:00:09
    120.1.1.192    00:dd:00:00:00:08
    120.1.1.200    00:dd:00:00:00:07
    120.1.1.194    00:dd:00:00:00:05
    120.1.1.193    00:dd:00:00:00:06
    120.1.1.196    00:dd:00:00:00:03
    120.1.1.195    00:dd:00:00:00:04
    120.1.1.197    00:dd:00:00:00:02
    120.1.1.198    00:dd:00:00:00:01

```

```

sub2@atm_subs
Circuit 1/4:1 vpi-vci 0 102
Internal Circuit 1/4:1:63/1/2/24580
Current port-limit unlimited
profile silver (applied)
dhcp max-addrs 10 (applied)
ip interface silver (applied)
    IP host entries installed by DHCP: (max_addr 10 cur_enties 10)

    120.1.2.191    00:dd:00:00:00:14
    120.1.2.192    00:dd:00:00:00:13
    120.1.2.193    00:dd:00:00:00:12
    120.1.2.194    00:dd:00:00:00:11
    120.1.2.195    00:dd:00:00:00:10
    120.1.2.196    00:dd:00:00:00:0f

```

```

120.1.2.197    00:dd:00:00:00:0e
120.1.2.198    00:dd:00:00:00:0d
120.1.2.199    00:dd:00:00:00:0c
120.1.2.200    00:dd:00:00:00:0b
sub3@atm_subs
Circuit 1/4:1 vpi-vci 0 103
Internal Circuit 1/4:1:63/1/2/24581
Current port-limit unlimited
profile bronze (applied)
dhcp max-addr 10 (applied)
ip interface bronze (applied)
IP host entries installed by DHCP: (max_addr 10 cur_entries 10)
120.1.3.191    00:dd:00:00:00:1e
120.1.3.192    00:dd:00:00:00:1d
120.1.3.193    00:dd:00:00:00:1c
120.1.3.194    00:dd:00:00:00:1b
120.1.3.195    00:dd:00:00:00:1a
120.1.3.196    00:dd:00:00:00:19
120.1.3.197    00:dd:00:00:00:18
120.1.3.198    00:dd:00:00:00:17
120.1.3.199    00:dd:00:00:00:16
120.1.3.200    00:dd:00:00:00:15

```

The following example displays DHCP relay host information for this configuration:

```
[atm_subs]Redback>show dhcp relay hosts
```

| Circuit             | Lease | Ttl  | Timestamp               | Host        | Relay/Proxy | Hardware address  | Context  |
|---------------------|-------|------|-------------------------|-------------|-------------|-------------------|----------|
| 1/4:1 vpi-vci 0 101 | 1800  | 1709 | Thu Nov 8 09:16:21 2005 | 120.1.1.198 | Proxy       | 00:dd:00:00:00:01 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1710 | Thu Nov 8 09:16:22 2005 | 120.1.1.197 | Proxy       | 00:dd:00:00:00:02 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1713 | Thu Nov 8 09:16:24 2005 | 120.1.1.195 | Proxy       | 00:dd:00:00:00:04 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1713 | Thu Nov 8 09:16:24 2005 | 120.1.1.196 | Proxy       | 00:dd:00:00:00:03 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1711 | Thu Nov 8 09:16:22 2005 | 120.1.1.193 | Proxy       | 00:dd:00:00:00:06 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1712 | Thu Nov 8 09:16:23 2005 | 120.1.1.194 | Proxy       | 00:dd:00:00:00:05 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1712 | Thu Nov 8 09:16:23 2005 | 120.1.1.200 | Proxy       | 00:dd:00:00:00:07 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1711 | Thu Nov 8 09:16:22 2005 | 120.1.1.192 | Proxy       | 00:dd:00:00:00:08 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1711 | Thu Nov 8 09:16:22 2005 | 120.1.1.191 | Proxy       | 00:dd:00:00:00:09 | atm_subs |
| 1/4:1 vpi-vci 0 101 | 1800  | 1711 | Thu Nov 8 09:16:23 2005 | 120.1.1.199 | Proxy       | 00:dd:00:00:00:0a | atm_subs |
| 1/4:1 vpi-vci 0 102 | 1800  | 1717 | Thu Nov 8 09:16:28 2005 | 120.1.2.197 | Proxy       | 00:dd:00:00:00:0e | atm_subs |
| 1/4:1 vpi-vci 0 102 |       |      |                         | 120.1.2.200 |             | 00:dd:00:00:00:0b |          |

```

1800      1713      Thu Nov  8 09:16:25 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.199      00:dd:00:00:00:0c
1800      1716      Thu Nov  8 09:16:28 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.198      00:dd:00:00:00:0d
1800      1716      Thu Nov  8 09:16:27 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.196      00:dd:00:00:00:0f
1800      1716      Thu Nov  8 09:16:27 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.195      00:dd:00:00:00:10
1800      1715      Thu Nov  8 09:16:27 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.194      00:dd:00:00:00:11
1800      1717      Thu Nov  8 09:16:28 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.193      00:dd:00:00:00:12
1800      1718      Thu Nov  8 09:16:29 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.192      00:dd:00:00:00:13
1800      1717      Thu Nov  8 09:16:29 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 102      120.1.2.191      00:dd:00:00:00:14
1800      1719      Thu Nov  8 09:16:30 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.200      00:dd:00:00:00:15
1800      1718      Thu Nov  8 09:16:30 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.199      00:dd:00:00:00:16
1800      1720      Thu Nov  8 09:16:32 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.198      00:dd:00:00:00:17
1800      1721      Thu Nov  8 09:16:32 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.197      00:dd:00:00:00:18
1800      1721      Thu Nov  8 09:16:32 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.196      00:dd:00:00:00:19
1800      1722      Thu Nov  8 09:16:33 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.195      00:dd:00:00:00:1a
1800      1723      Thu Nov  8 09:16:34 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.194      00:dd:00:00:00:1b
1800      1721      Thu Nov  8 09:16:33 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.193      00:dd:00:00:00:1c
1800      1722      Thu Nov  8 09:16:33 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.192      00:dd:00:00:00:1d
1800      1722      Thu Nov  8 09:16:33 2005 Proxy      atm_subs
1/4:1 vpi-vci 0 103      120.1.3.191      00:dd:00:00:00:1e
1800      1723      Thu Nov  8 09:16:34 2005 Proxy      atm_subs

```

## Using RADIUS Authentication

The following example binds subscribers to DHCP interfaces, using the **ip interface** command (in subscriber configuration mode) with RADIUS authentication:

```

[local]Redback(config)#context atm_subs
[local]atm_subs(config-ctx)#interface bronze multibind
[local]atm_subs(config-if)#ip address 120.1.3.1/24
[local]atm_subs(config-if)#dhcp proxy 100
[local]atm_subs(config-if)#exit
[local]atm_subs(config-ctx)#interface gold multibind
[local]atm_subs(config-if)#ip address 120.1.1.1/24
[local]atm_subs(config-if)#dhcp proxy 100
[local]atm_subs(config-if)#exit

```

```

[local]atm_subs(config-ctx)#interface silver multibind
[local]atm_subs(config-if)#ip address 120.1.2.1/24
[local]atm_subs(config-if)#dhcp proxy 100
[local]atm_subs(config-if)#exit
[local]atm_subs(config-ctx)#interface to-linux-server
[local]atm_subs(config-if)#ip address 108.1.1.1/24
[local]atm_subs(config-if)#exit
[local]atm_subs(config-ctx)#interface to-sms-server
[local]atm_subs(config-if)#ip address 100.1.1.1/24
[local]atm_subs(config-if)#exit
[local]atm_subs(config-ctx)#radius server 108.1.1.157 key mpls4
[local]atm_subs(config-ctx)#radius max-retries 5
[local]atm_subs(config-ctx)#radius timeout 5
[local]atm_subs(config-ctx)#radius algorithm round-robin
[local]atm_subs(config-ctx)#radius accounting algorithm round-robin
[local]atm_subs(config-ctx)#aaa authentication subscriber radius
[local]atm_subs(config-ctx)#aaa accounting subscriber radius
[local]atm_subs(config-ctx)#aaa accounting event dhcp
[local]atm_subs(config-ctx)#radius accounting server 108.1.1.157 key mpls4
[local]atm_subs(config-ctx)#subscriber profile gold
[local]atm_subs(config-sub)#ip interface name gold
[local]atm_subs(config-sub)#exit
[local]atm_subs(config-ctx)#subscriber profile silver
[local]atm_subs(config-sub)#ip interface name silver
[local]atm_subs(config-sub)#exit
[local]atm_subs(config-ctx)#subscriber profile bronze
[local]atm_subs(config-sub)#ip interface name bronze
[local]atm_subs(config-sub)#exit
[local]atm_subs(config-ctx)#dhcp relay server 108.1.1.157
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
[local]atm_subs(config-ctx)#exit
[local]atm_subs(config)#card atm-oc3-4-port 1
[local]atm_subs(config)#port atm 1/4
[local]atm_subs(config-atm-oc)#no shutdown
[local]atm_subs(config-atm-oc)#atm pvc 0 101 profile a1 encapsulation bridge1483
[local]atm_subs(config-atm-pvc)#bind subscriber sub1@atm_subs password test
[local]atm_subs(config-atm-pvc)#exit
[local]atm_subs(config-atm-oc)#atm pvc 0 102 profile a1 encapsulation bridge1483
[local]atm_subs(config-atm-pvc)#bind subscriber sub2@atm_subs password test
[local]atm_subs(config-atm-pvc)#exit
[local]atm_subs(config-atm-oc)#atm pvc 0 103 profile a1 encapsulation bridge1483
[local]atm_subs(config-atm-pvc)#bind subscriber sub3@atm_subs password test

```

The following example displays the RADIUS subscriber files:

```

sub1@atm_subs    Password = "test"
                 Service-Type = Framed-User,
                 RB-IP-Interface-Name = gold,
                 RB-DHCP-Max-Leases = 10,
                 RB-Context-Name = atm_subs

```

```
sub2@atm_subs Password = "test"
Service-Type = Framed-User,
RB-IP-Interface-Name = silver,
RB-DHCP-Max-Leases = 10,
RB-Context-Name = atm_subs
```

```
sub3@atm_subs Password = "test"
Service-Type = Framed-User,
RB-IP-Interface-Name = bronze,
RB-DHCP-Max-Leases = 10,
RB-Context-Name = atm_subs
```

In the RADIUS dictionary, the relevant attribute is:

|            |      |                      |     |        |
|------------|------|----------------------|-----|--------|
| VENDORATTR | 2352 | RB-IP-Interface-Name | 104 | string |
|------------|------|----------------------|-----|--------|

One of the sample Accounting-Alive packets with the RADIUS IP interface attribute is:

```
Code: Accounting-Request
Identifier: 38
Authentic: 'l<199>[<151><142><192>@<0><15><175>KC0}<163>'
Attributes:
  User-Name = "sub3@atm_subs"
  Acct-Status-Type = Alive
  Acct-Session-Id = "0003003F3000601C-40757C65"
  Service-Type = Framed-User
  NAS-Identifier = "mpls4"
  NAS-Port = 17039424
  NAS-Port-Type = Sync
  NAS-Port-Id = "1/4 vpi-vci 0 103"
  Connect-Info = "a1"
  RB-Platform-ID = SmartEdge
  Acct-Authentic = RADIUS
  RB-IP-Interface-Name = "bronze"
  RB-DHCP-Max-Leases = 10
  Acct-Session-Time = 105
  Acct-Input-Packets = 32
  Acct-Output-Packets = 26
  Acct-Input-Octets = 7733
  Acct-Output-Octets = 5388
  Acct-Input-Gigawords = 0
  Acct-Output-Gigawords = 0
  RB-Acct-Input-Packets-64 = 0x20
  RB-Acct-Output-Packets-64 = 0x1a
  RB-Acct-Input-Octets-64 = 0x1e35
```



## DHCP Proxy Through Dynamic Subscriber Bindings

The following example configures DHCP proxy through dynamic subscriber bindings:

```
[local]Redback(config)#context dyn-sub-bindings
[local]Redback(config-ctx)#interface dyn-sub-if multibind
[local]Redback(config-if)#ip address 100.1.1.1/24
[local]Redback(config-if)#dhcp proxy 251
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface to-dhcp-server
[local]Redback(config-if)#ip address 108.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#subscriber name sub21
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub22
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub23
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub24
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub25
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub101
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub102
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub103
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub104
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name sub105
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#dhcp max-addrs 1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#dhcp relay server 108.1.1.156
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
[local]Redback(config-ctx)#exit
```

```
[local]Redback(config)#atm profile a1
[local]Redback(config-atm-profile)#shaping ubr
[local]Redback(config-atm-profile)#exit
[local]Redback(config)#card atm-oc3-4-port 5
[local]Redback(config-card)#exit
[local]Redback(config)#port atm 5/2
[local]Redback(config-atm-oc)#no shutdown
[local]Redback(config-atm-oc)#atm pvc 0 101 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub101@subscriber password test
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#atm pvc 0 102 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub102@subscriber password test
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#atm pvc 0 103 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub103@subscriber password test
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#atm pvc 0 104 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub104@subscriber password test
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#atm pvc 0 105 profile a1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber sub105@subscriber password test
[local]Redback(config-atm-pvc)#exit
[local]Redback(config-atm-oc)#exit
[local]Redback(config)#port ethernet 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface to-dhcp-server subscriber
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 21
[local]Redback(config-dot1q-pvc)#bind subscriber sub21@subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 22
[local]Redback(config-dot1q-pvc)#bind subscriber sub22@subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 23
[local]Redback(config-dot1q-pvc)#bind subscriber sub23@subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 24
[local]Redback(config-dot1q-pvc)#bind subscriber sub24@subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 25
[local]Redback(config-dot1q-pvc)#bind subscriber sub25@subscriber
```

## DHCP Proxy Through Static Interface Bindings

The following example configures DHCP proxy through static interface bindings:

```
[local]Redback(config)#context non-subscriber
[local]Redback(config-ctx)#interface non-subscriber multibind
[local]Redback(config-if)#ip address 100.1.1.1/16
[local]Redback(config-if)#dhcp proxy 1000
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface to-dhcp-server
[local]Redback(config-if)#ip address 108.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface vlan.1 multibind
[local]Redback(config-if)#ip address 121.1.1.1/24
[local]Redback(config-if)#dhcp proxy 250
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface vlan.10 multibind
[local]Redback(config-if)#ip address 130.1.1.1/24
[local]Redback(config-if)#dhcp proxy 250
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#dhcp relay server 108.1.1.156
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
[local]Redback(config-ctx)#exit
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 1
[local]Redback(config-dot1q-pvc)#bind interface vlan.1 non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 10
[local]Redback(config-dot1q-pvc)#bind interface vlan.10 non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 11 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 12 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 13 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 14 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 15 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 16 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
```

```
[local]Redback(config-port)#dot1q pvc 17 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 18 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 19 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 20 encaps multi
[local]Redback(config-dot1q-pvc)#bind interface non-subscriber non-subscriber
```

## **DHCP Proxy Through RADIUS**

The following example configures DHCP proxy through RADIUS:

```
[local]Redback(config)#no service multiple-contexts
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface loop1 loopback
[local]Redback(config-if)#ip address 11.200.1.1/32
[local]Redback(config-if)#ip source-address dhcp-server
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface subscriber multibind
[local]Redback(config-if)#ip address 100.1.0.1/16
[local]Redback(config-if)#dhcp proxy 50
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface to-cisco-dhcp-server
[local]Redback(config-if)#ip address 108.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#radius server 108.1.1.157 key dhcp
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#dhcp relay server 108.1.1.156
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
[local]Redback(config-ctx)#exit
[local]Redback(config)#card ether-12-port 9
[local]Redback(config-card)#exit
[local]Redback(config)#port ethernet 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface to-cisco-dhcp-server local
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 1
[local]Redback(config-dot1q-pvc)#bind subscriber sub1@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 2
[local]Redback(config-dot1q-pvc)#bind subscriber sub2@local password test
[local]Redback(config-dot1q-pvc)#exit
```

```
[local]Redback(config-port)#dot1q pvc 3
[local]Redback(config-dot1q-pvc)#bind subscriber sub3@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 4
[local]Redback(config-dot1q-pvc)#bind subscriber sub4@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 5
[local]Redback(config-dot1q-pvc)#bind subscriber sub5@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 6
[local]Redback(config-dot1q-pvc)#bind subscriber sub6@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 7
[local]Redback(config-dot1q-pvc)#bind subscriber sub7@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 8
[local]Redback(config-dot1q-pvc)#bind subscriber sub8@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 9
[local]Redback(config-dot1q-pvc)#bind subscriber sub9@local password test
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 10
[local]Redback(config-dot1q-pvc)#bind subscriber sub10@local password test
```

The following output displays sample content from the RADIUS server file used in this example:

```
sub1@local      Password = "test"
                Service-Type = Framed-User,
                DHCP_Max_Leases = 1
sub2@local      Password = "test"
                Service-Type = Framed-User,
                DHCP_Max_Leases = 1
sub3@local      Password = "test"
                Service-Type = Framed-User,
                DHCP_Max_Leases = 1
sub4@local      Password = "test"
                Service-Type = Framed-User,
                DHCP_Max_Leases = 1
```

## Loopback Interface as DHCP Source Address

The following example shows that the IP address of the interface connected to the external DHCP server is 108.1.1.1; however, a loopback interface is configured with another IP address, which is sent to the DHCP server as the source IP address for DHCP packets:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to-dhcp-server
[local]Redback(config-if)#ip address 108.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface loop1 loopback
[local]Redback(config-if)#ip address 11.200.1.1/32
[local]Redback(config-if)#ip source-address dhcp-server
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure DHCP features. The commands are presented in alphabetical order.

|                                  |                         |
|----------------------------------|-------------------------|
| <b>bootp-filename</b>            | <b>mac-address</b>      |
| <b>bootp-siaddr</b>              | <b>max-hops</b>         |
| <b>default-lease-time</b>        | <b>max-lease-time</b>   |
| <b>dhcp max-addrs</b>            | <b>min-wait</b>         |
| <b>dhcp proxy</b>                | <b>offer-lease-time</b> |
| <b>dhcp relay</b>                | <b>option</b>           |
| <b>dhcp relay option</b>         | <b>option-82</b>        |
| <b>dhcp relay server</b>         | <b>range</b>            |
| <b>dhcp relay server retries</b> | <b>server-group</b>     |
| <b>dhcp relay suppress-nak</b>   | <b>standby</b>          |
| <b>dhcp server</b>               | <b>subnet</b>           |
| <b>dhcp server policy</b>        | <b>user-class-id</b>    |
| <b>forward-all</b>               | <b>vendor-class</b>     |
| <b>ip interface</b>              | <b>vendor-class-id</b>  |

## bootp-filename

**bootp-filename** *bootfile-name*  
**no bootp-filename** *bootfile-name*

### Purpose

Specifies the filename of the boot loader image file.

### Command Mode

DHCP server configuration

### Syntax Description

*bootfile-name*                      Name of the boot loader image file.

### Default

No boot loader image is specified.

### Usage Guidelines

Use the **bootp-filename** command to specify the filename of the boot loader image file. The boot loader image file is run when the system is reloaded or powered on.

Use the **no** form of this command to specify the default condition.

### Examples

The following example specifies the boot loader image file for the SmartEdge router:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#dhcp server policy  
[local]Redback(config-dhcp-server)#bootp-filename of1267.bin
```

### Related Commands

**bootp-siaddr**

## bootp-siaddr

**bootp-siaddr** *ip-addr*  
**no bootp-siaddr** *ip-addr*

### Purpose

Specifies the IP address that the boot loader client uses to download the boot loader image file.

### Command Mode

DHCP server configuration

### Syntax Description

*ip-addr* IP address the boot loader client uses.

### Default

No IP address is specified.

### Usage Guidelines

Use the **bootp-siaddr** command to specify the IP address that the boot loader client uses to download the boot loader image file.

Use the **no** form of this command to specify the default condition.

### Examples

The following example specifies the IP address for the SmartEdge router with the boot loader image file:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#bootp-siaddr 200.1.1.0
```

### Related Commands

**bootp-filename**



## default-lease-time

**default-lease-time** *seconds*

**no default-lease-time**

### Purpose

Specifies the default lease time for this Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

### Command Mode

DHCP server configuration

DHCP subnet configuration

### Syntax Description

|                |                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------|
| <i>seconds</i> | Length of time for the default lease. The range of values is 900 (15 minutes) to 31,536,000 (one year). |
|----------------|---------------------------------------------------------------------------------------------------------|

### Default

The default length of time is two hours.

### Usage Guidelines

Use the **default-lease-time** command to specify the default lease time for the DHCP server or one of its subnets. In DHCP server configuration mode, this command specifies the default lease time for all subnets; in DHCP subnet configuration mode, it specifies the default lease time for that subnet. The value you specify for a subnet overrides the global value for the server.

Use the **no** form of this command to specify the default value.

### Examples

The following example specifies a default lease time of 4 hours (14400) for the DHCP server and all its subnets:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#default-lease-time 14400
```

### Related Commands

**max-lease-time**

**offer-lease-time**

**subnet**

## dhcp max-addr

**dhcp max-addr** *max-sub-addr*

**no dhcp max-addr**

### Purpose

Indicates that associated hosts are to use Dynamic Host Configuration Protocol (DHCP) to dynamically acquire address information for the subscriber's circuit, and sets a maximum number of IP addresses that the SmartEdge OS expects the external DHCP server to assign to hosts associated with the circuit.

### Command Mode

subscriber configuration

### Syntax Description

*max-sub-addr* Maximum number of unique IP addresses the SmartEdge OS expects the external DHCP server to assign to hosts associated with a given subscriber circuit. The range of values is 1 to 100.

For dynamic clientless IP service selection (CLIPS) subscribers, the value for the *max-sub-addr* argument must be 1.

### Default

None

### Usage Guidelines

Use the **dhcp max-addr** command to indicate that associated hosts are to use DHCP to dynamically acquire address information for the subscriber's circuit, and to set a maximum number of IP addresses that the SmartEdge OS expects the external DHCP server to assign to hosts associated with the circuit.

For non-CLIPS subscribers, the SmartEdge OS deducts the value of the *max-sub-addr* argument from the value for the *max-dhcp-addr* argument that you configured for a DHCP proxy or DHCP relay interface, using the **dhcp proxy** or **dhcp relay** commands (in interface configuration mode), available at the time a subscriber is bound to a circuit. When the value for the *max-dhcp-addr* argument for a DHCP proxy or DHCP relay interface reaches 0, that interface is no longer available for subscriber bindings.

For dynamic CLIPS subscribers, you must configure the subscriber record or profile with no IP address and specify 1 as the value for the *max-sub-addr* argument; for information about CLIPS, see the "CLIPS Configuration" chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

Use the **no** form of this command to disable the use of DHCP for the subscriber's circuit.

**Note** If you configure a subscriber record with a **dhcp max-addr**s command and with one or more static IP host addresses, using the **ip address** command (in interface configuration mode), the static IP addresses always take precedence; the associated circuit is bound to an interface on the basis of the static IP addresses. If you configure the record with a **dhcp max-addr**s command, and you do not configure any static addresses for it, the associated circuit is bound to the first available interface with capacity for this subscriber.

## Examples

The following example configures the subscriber, `dhcp-test`, to expect a total of 8 IP addresses that can be assigned at any time:

```
[local]Redback(config-ctx)#subscriber name dhcp-test  
[local]Redback(config-sub)#dhcp max-addrs 8
```

## Related Commands

- dhcp proxy**
- dhcp relay**
- dhcp relay server**

## dhcp proxy

**dhcp proxy** *max-dhcp-addr*s [**server-group** *name*]

**no dhcp proxy**

### Purpose

Enables this interface to act as proxy between subscribers and an external Dynamic Host Configuration Protocol (DHCP) server, and access DHCP giaddr configuration mode.

### Command Mode

interface configuration

### Syntax Description

|                                 |                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <i>max-dhcp-addr</i> s          | Maximum number of IP addresses available on the interface. The range of values is 1 to 65,535.                                       |
| <b>server-group</b> <i>name</i> | Optional. DHCP server group. Forwards all DHCP requests received on the interface to all DHCP servers in the specified server group. |

### Default

DHCP proxy is disabled.

### Usage Guidelines

Use the **dhcp proxy** command to enable this interface to act as a proxy between subscribers and an external DHCP server, and access DHCP giaddr configuration mode.

When you enable DHCP proxy, the interface relays all DHCP packets, including the release and renewal of IP addresses for subscriber sessions, between the DHCP server and the subscriber. To the subscriber, the SmartEdge router appears to be the DHCP server.

The SmartEdge OS uses the value for the *max-dhcp-addr*s argument to load balance between IP addresses from multiple pools. When you configure the SmartEdge OS for subscriber DHCP proxy, the value of the *max-dhcp-addr*s argument indicates the total number of subscriber requests that will be forwarded on the interface.

The SmartEdge OS deducts the *max-sub-addr*s value for the **dhcp max-addr**s command (in subscriber configuration mode) from the current value for *max-dhcp-addr*s argument for the DHCP proxy interface at the time a subscriber is bound to a circuit using that interface. When the value of *max-dhcp-addr*s for a DHCP proxy interface reaches 0, that interface is no longer available for subscriber bindings.

Use the **no** form of this command to disable DHCP proxy on the interface.

**Note** You can configure an interface to act as either a DHCP relay or a DHCP proxy; the **dhcp relay** and **dhcp proxy** commands are mutually exclusive.

**Note** For the **dhcp proxy** command to take effect, you must configure an external DHCP server, using the **dhcp relay server** command in the context in which the interface is configured.

## Examples

The following example enables the proxy1 interface to act as a DHCP proxy for the DHCP server at IP address, 10.30.40.50:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50  
[local]Redback(config-dhcp-relay)#exit  
[local]Redback(config-ctx)#interface proxy1  
[local]Redback(config-if)#ip address 10.1.2.3 255.255.255.0  
[local]Redback(config-if)#dhcp proxy 253
```

## Related Commands

- dhcp max-addr**
- dhcp relay**
- dhcp relay server**

## dhcp relay

**dhcp relay** *max-dhcp-addrs* [**server-group** *group-name*]

**no dhcp relay**

### Purpose

Enables this interface to relay Dynamic Host Configuration Protocol (DHCP) messages to an external DHCP server, and access DHCP giaddr configuration mode.

### Command Mode

interface configuration

### Syntax Description

|                                       |                                                                                                                                      |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <i>max-dhcp-addrs</i>                 | Maximum number of IP addresses available on the interface. The range of values is 0 to 65,535.                                       |
| <b>server-group</b> <i>group-name</i> | Optional. DHCP server group. Forwards all DHCP requests received on the interface to all DHCP servers in the specified server group. |

### Default

DHCP relay is disabled.

### Usage Guidelines

Use the **dhcp relay** command to enable this interface to relay DHCP messages to an external DHCP server, and access DHCP giaddr configuration mode.

The SmartEdge OS uses the value for the *max-dhcp-addrs* argument to load balance between IP addresses from multiple pools. When you configure the SmartEdge OS for subscriber DHCP relay, the value of the *max-dhcp-addrs* argument indicates the total number of subscriber requests that can be forwarded on the interface.

The value of the *max-sub-addrs* argument for the **dhcp max-addrs** command (in subscriber configuration mode) is deducted from the *max-dhcp-addrs* value configured for a DHCP relay interface available at the time a subscriber is bound to a circuit on that interface. When the value of *max-dhcp-addrs* for a DHCP relay interface reaches 0, that interface is no longer available for subscriber bindings.

**Note** You can configure an interface to act as either a DHCP relay or a DHCP proxy; the **dhcp relay** and **dhcp proxy** commands are mutually exclusive.

**Note** For the **dhcp relay** command to take effect, you must configure an external DHCP server, using the **dhcp relay server** command in the context in which the interface is configured.

Use the **no** form of this command to disable DHCP relay on the interface.

## Examples

The following example enables DHCP relay on interface `eth1`, which is configured with a total of 253 IP addresses that can be allocated by the DHCP server at any time from the `10.1.1.0` subnet:

```
[local]Redback(config-ctx)#interface eth1  
[local]Redback(config-if)#ip address 10.1.1.0 255.255.255.0  
[local]Redback(config-if)#dhcp relay 253  
[local]Redback(config-dhcp-giaddr)#
```

## Related Commands

- `dhcp max-addr`
- `dhcp proxy`
- `dhcp relay server`

## dhcp relay option

**dhcp relay option** [hostname [separator character]]

**no dhcp relay option** [hostname [separator character]]

### Purpose

Enables the sending of Dynamic Host Configuration Protocol (DHCP) options in DHCP packets relayed by the interfaces in the specified context.

### Command Mode

context configuration

### Syntax Description

|                            |                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hostname</b>            | Optional. Prepends the SmartEdge router hostname to the agent circuit id field of DHCP option 82. The SmartEdge OS uses the hostname that you have configured using the <b>system hostname</b> command (in context configuration mode). If you have not configured the hostname, the SmartEdge OS uses the default hostname of “Redback.” |
| <b>separator character</b> | Optional. Character that separates the elements of the attribute string. Changes the character that separates the hostname from the circuit id field of DHCP option 82. The default separator character is the colon (:).                                                                                                                 |

### Default

DHCP options are not sent.

### Usage Guidelines

Use the **dhcp relay option** command to enable the sending of DHCP options in all DHCP packets that are relayed by the interfaces in the specified context.

On some networks, DHCP is used to dynamically configure IP address information for subscriber hosts. The SmartEdge router can act as a relay or as a proxy for DHCP servers. DHCP is typically used with RFC 1483 bridge-encapsulated circuits, as opposed to Point-to-Point Protocol (PPP) circuits.

The SmartEdge OS can use DHCP relay options to help track DHCP requests. Some options can also enhance the DHCP server’s function. The DHCP relay options are described in RFC 3046, *DHCP Relay Agent Information Option*.

In order for relay options to take effect, you must enable DHCP relay for the context, using the **dhcp relay server** command (in context configuration mode), and for an interface, using the **dhcp relay** or **dhcp proxy** command (in interface configuration mode). You must also configure subscriber records, using the **dhcp max-addrs** command (in subscriber configuration mode) to indicate that associated hosts are to use DHCP relay to dynamically acquire address information.

Use the **no** form of this command to disable the sending of DHCP options.



## Examples

The following example enables the sending of DHCP relay options:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
```

The following example prepends the system hostname, SE800, to the agent circuit id field of DHCP option 82 and, by default, uses the colon (:) to separate the hostname from the circuit id field:

```
[local]Redback(config)#server hostname SE800
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp relay server 108.1.1.157
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option hostname
```

The DHCP server's lease log for this configuration would be similar to the following example:

```
lease 120.1.3.191 {
  starts 2 2005/11/08 10:05:21;
  ends 2 2005/11/08 10:35:21;
  binding state active
  netx binding state free
  hardware ethernet 00:dd:00:00:00:1e;
  uid "\001\006\000\335\000\000\000\036";
  option agent.circuit-id "SE800:1/4 vpi-vci 0 103";
}
```

## Related Commands

- dhcp proxy**
- dhcp relay**
- dhcp relay server**

## dhcp relay server

**dhcp relay server** {*ip-addr* | *hostname*} [**max-hops** *count*] [**min-wait** *interval*]

**no dhcp relay server** {*ip-addr* | *hostname*} [**max-hops** *count*] [**min-wait** *interval*]

### Purpose

Configures an external Dynamic Host Configuration Protocol (DHCP) server and enters DHCP relay server configuration mode.

### Command Mode

context configuration

### Syntax Description

|                                 |                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>                  | IP address of the DHCP server.                                                                                                                              |
| <i>hostname</i>                 | Hostname of the DHCP server.                                                                                                                                |
| <b>max-hops</b> <i>count</i>    | Optional. Maximum number of hops allowed for requests. The range of values for the <i>count</i> argument is 1 to 16.                                        |
| <b>min-wait</b> <i>interval</i> | Optional. Minimum time, in seconds, to wait before forwarding requests to the DHCP server. The range of values for the <i>interval</i> argument is 0 to 60. |

### Default

Disabled

### Usage Guidelines

Use the **dhcp relay server** command to configure an external DHCP server and enter DHCP relay server configuration mode. You can configure up to five external DHCP servers in each context.

If you have configured Remote Authentication Dial-In User Service (RADIUS) authentication, the SmartEdge OS sends an accounting record to RADIUS every time DHCP assigns or releases an IP address.

**Note** For the **dhcp relay server** command to take effect, you must also enable DHCP relay or DHCP proxy on an interface in the same context, using the **dhcp proxy** or **dhcp relay** command (in interface configuration mode).

To indicate that associated hosts are to use DHCP relay to dynamically acquire address information, you must configure the subscriber default profile, a named profile, or subscriber records with the **dhcp max-addrs** command (in subscriber configuration mode).

Use the **no** form of this command to disable the DHCP server.

## Examples

The following example configures an external DHCP server at IP address, 10.30.40.50, and enters DHCP relay server configuration mode:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50  
[local]Redback(config-dhcp-relay)#
```

## Related Commands

- dhcp max-addr**
- dhcp proxy**
- dhcp relay**
- dhcp relay server retries**
- max-hops**
- min-wait**
- server-group**
- standby**

## dhcp relay server retries

**dhcp relay server retries** *count* **timeout** *interval*

**no dhcp relay server retries** *count* **timeout** *interval*

### Purpose

Specifies the number of attempts and the interval to wait for each attempt when trying to reach an external Dynamic Host Configuration Protocol (DHCP) server before it is marked unreachable.

### Command Mode

context configuration

### Syntax Description

|                                |                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <i>count</i>                   | Maximum consecutive number of times to attempt reaching the DHCP server; the default value is 3.                                         |
| <b>timeout</b> <i>interval</i> | Interval, in seconds, to wait for a reply after a DHCP request packet is sent. The default value for the <i>interval</i> argument is 30. |

### Default

Up to three attempts are made to reach a DHCP server, with a wait interval of 30 seconds for each attempt.

### Usage Guidelines

Use the **dhcp relay server retries** command to specify the number of attempts and the interval to wait for each attempt when trying to reach an external DHCP server before it is marked unreachable.

If the interval expires without receiving a reply from the DHCP server, another DHCP request is sent to the DHCP server until the maximum consecutive number of attempts has been reached. If the interval expires after the last attempt without reaching the DHCP server, then the DHCP server is marked unreachable.

Use the **no** form of this command to specify the default conditions.

### Examples

The following example configures the SmartEdge router to make up to 5 attempts to reach a DHCP server, with a wait interval of 15 seconds for each attempt:

```
[local]Redback(config-ctx)#dhcp relay server retries 5 timeout 15
[local]Redback(config-ctx)#
```

### Related Commands

**dhcp relay server**

# dhcp relay suppress-nak

**dhcp relay suppress-nak**

**no dhcp relay suppress-nak**

## Purpose

Disables the sending of a DHCPNAK message when the SmartEdge OS receives a DHCPREQUEST message for which it does not have an entry.

## Command Mode

context configuration

## Syntax Description

This command has no keywords or arguments.

## Default

A DHCPNAK message is always sent.

## Usage Guidelines

Use the **dhcp relay suppress-nak** command to disable the sending of a DHCPNAK message when the SmartEdge OS receives a DHCPREQUEST message for which it does not have an entry. In this case, the request is dropped.

Use the **no** form of this command to enable the default condition.

## Examples

The following example disables the sending of a DHCPNAK message:

```
[local]Redback(config-ctx)#dhcp relay suppress-nak
```

## Related Commands

None

## dhcp server

**dhcp server** {**interface** | *ip-addr*}  
**no dhcp server** {**interface** | *ip-addr*}

### Purpose

Enables this interface for internal Dynamic Host Configuration Protocol (DHCP) server support and assigns the IP address to be used for this support.

### Command Mode

interface configuration

### Syntax Description

|                  |                                                                     |
|------------------|---------------------------------------------------------------------|
| <b>interface</b> | Assigns the primary IP address of the interface to the DHCP server. |
| <i>ip-addr</i>   | One of the secondary IP addresses assigned to the interface.        |

### Default

No internal DHCP servers are created.

### Usage Guidelines

Use the **dhcp server** command to enable this interface for internal DHCP server support and assign the IP address to be used for this support.

For information about the **context** command (in global configuration mode), the **interface** command (in context configuration mode), and the **ip address** command (in interface configuration mode), see the “Context Configuration” and “Interface Configuration” chapters, respectively, in the *Basic System Configuration Guide* for the SmartEdge OS.

**Note** The actual choice of an IP address for the internal DHCP server is made by authentication, authorization, and accounting (AAA), subject to any static mappings, subnets, and ranges that you have configured for the server.

Use the **no** form of this command to delete the internal DHCP server.

### Examples

The following example creates an internal DHCP server using the secondary IP address for the dhcp-if interface in the dhcp context:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#interface dhcp-if multibind
[local]Redback(config-if)#ip address 12.1.1.1/24
[local]Redback(config-if)#ip address 13.1.1.1/24 secondary
[local]Redback(config-if)#dhcp server 13.1.1.1
```

## Related Commands

`dhcp server policy`

## dhcp server policy

**dhcp server policy**

**no dhcp server policy**

### Purpose

Enables internal Dynamic Host Configuration Protocol (DHCP) server functions in this context and accesses DHCP server configuration mode.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Internal DHCP server functions are disabled for this context.

### Usage Guidelines

Use the **dhcp server policy** command to enable internal DHCP server functions in this context and access DHCP server configuration mode.

Use the **no** form of this command to disable internal DHCP server functions.

### Examples

The following example enables DHCP server functions in the dhcp context:

```
[local]Redback(config)#context dhcp  
[local]Redback(config-ctx)#dhcp server policy  
[local]Redback(config-dhcp-server)#
```

### Related Commands

**dhcp server**



## forward-all

**forward-all**

**no forward-all**

### Purpose

Forwards packets to all other external Dynamic Host Configuration Protocol (DHCP) servers in a DHCP server group.

### Command Mode

DHCP relay server configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Packets are not forwarded to the other DHCP servers in the DHCP server group.

### Usage Guidelines

When a DHCP server is unreachable, DHCP request packets can be forwarded to all other DHCP servers in its DHCP server group. Use the **forward-all** command to forward packets to all other DHCP servers in a server group.

**Note** When the DHCP server is unreachable, you can either forward packets to all other DHCP servers in its DHCP server group or forward packets to its standby DHCP server, but not both; the **forward-all** and **standby** commands are mutually exclusive.

Use the **no** form of this command to disable the forward all option.

### Examples

The following example forwards packets to all other DHCP servers in DHCP server group, `int-grp`, when the DHCP server, `10.30.40.50`, is unreachable:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50  
[local]Redback(config-dhcp-relay)#server-group int-grp  
[local]Redback(config-dhcp-relay)#forward-all
```

### Related Commands

**dhcp relay server**  
**server-group**  
**standby**

## ip interface

**ip interface name** *if-name*

**no ip interface name** *if-name*

### Purpose

Configure hosts to use a specific Dynamic Host Configuration Protocol (DHCP) interface to acquire address information for a subscriber's circuit.

### Command Mode

subscriber configuration

### Syntax Description

**name** *if-name*                      DHCP interface name.

### Default

The subscriber is bound to the first available DHCP interface.

### Usage Guidelines

Use the **ip interface** command to configure hosts to use a specific DHCP interface to acquire address information for a subscriber's circuit.

You must enable the specified interface for DHCP proxy or DHCP relay using the **dhcp proxy** or **dhcp relay** command (in interface configuration mode), respectively.

You must use the **dhcp max-addr** command (in subscriber configuration mode) to enable hosts to acquire address information for the subscriber's circuit.

Use the **no** form of this command to restore the default condition where the subscriber is bound to the first available DHCP interface.

### Examples

The following example creates an interface and specifies that hosts use the DHCP `if-dhcp` interface to acquire address information for the circuit used by the `sub-dhcp` subscriber:

```
[local]Redback(config-ctx)#interface name if-dhcp
[local]Redback(config-if)#ip address 10.1.1.1 255.255.255.0
[local]Redback(config-if)#dhcp relay
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#subscriber name sub-dhcp
[local]Redback(config-sub)#dhcp max-addr 3
[local]Redback(config-sub)#ip interface name if-dhcp
```

**Related Commands**

None

## mac-address

**mac-address** *mac-addr* **ip-address** *ip-addr*

**no mac-address** *mac-addr* **ip-address** *ip-addr*

### Purpose

Creates a static mapping between a medium access control (MAC) address and an IP address in this subnet.

### Command Mode

DHCP subnet configuration

### Syntax Description

|                                  |                                                      |
|----------------------------------|------------------------------------------------------|
| <i>mac-addr</i>                  | MAC address for the subnet.                          |
| <b>ip-address</b> <i>ip-addr</i> | IP address to which the MAC address is to be mapped. |

### Default

No mapping exists between the MAC address and an IP address.

### Usage Guidelines

Use the **mac-address** command to create a static mapping between a MAC address and an IP address in this subnet.

The value for the *ip-addr* argument must be an IP address within this subnet, but not within any range of IP addresses that you have specified using the **range** command (in DHCP subnet configuration mode).

Use the **no** form of this command to specify the default condition.

### Examples

The following example creates a static mapping between a MAC address and an IP address:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 12.1.1.0/24 name sub2
[local]Redback(config-dhcp-subnet)#range 12.1.1.50 12.1.1.100
[local]Redback(config-dhcp-subnet)#mac-address 02:12:34:56:78:90 ip-address 12.1.1.10
```

### Related Commands

**range**  
**subnet**

# max-hops

**max-hops** *count*

{**no** | **default**} **max-hops** *count*

## Purpose

Configures the maximum hop count allowed for Dynamic Host Configuration Protocol (DHCP) requests.

## Command Mode

DHCP relay server configuration

## Syntax Description

|              |                                            |
|--------------|--------------------------------------------|
| <i>count</i> | Hop count. The range of values is 1 to 16. |
|--------------|--------------------------------------------|

## Default

The maximum hop count is four.

## Usage Guidelines

Use the **max-hops** command to configure the maximum hop count allowed for DHCP requests.

Use the **no** or **default** form of this command to return to the default DHCP relay server maximum hop count of four.

## Examples

The following example configures a maximum of 12 hops allowed for DHCP requests to DHCP server, 10.30.40.50:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50  
[local]Redback(config-dhcp-relay)#max-hops 12  
[local]Redback(config-dhcp-relay)#
```

## Related Commands

- dhcp max-addr**s
- dhcp proxy**
- dhcp relay**
- dhcp relay server**
- forward-all**
- min-wait**
- server-group**
- standby**

## max-lease-time

**max-lease-time** *seconds*

**no max-lease-time** *seconds*

### Purpose

Specifies the maximum allowed time for the lease for this internal Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

### Command Mode

DHCP server configuration

DHCP subnet configuration

### Syntax Description

|                |                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------|
| <i>seconds</i> | Maximum allowed time for the lease (in seconds). The range of values is 900 (15 minutes) to 31,536,000 (one year). |
|----------------|--------------------------------------------------------------------------------------------------------------------|

### Default

The maximum lease time is 24 hours.

### Usage Guidelines

Use the **max-lease-time** command to specify the maximum allowed lease time for this internal DHCP server or one of its subnets. Enter this command in DHCP server configuration mode to specify the maximum allowed lease time for all subnets; enter it in DHCP subnet configuration mode to specify the maximum allowed lease time for that subnet. The value that you specify for a subnet overrides the global value for the server.

Use the **no** form of this command to specify the default value for the maximum allowed lease time.

### Examples

The following example specifies a maximum allowed lease time of 48 hours (172800) for the DHCP server and all its subnets:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#maximum-lease-time 172800
```

### Related Commands

**default-lease-time**

**offer-lease-time**

**subnet**

## min-wait

**min-wait** *interval*

{ **no** | **default** } **min-wait** *interval*

### Purpose

Configures the interval, in seconds, to wait before forwarding requests to the Dynamic Host Configuration Protocol (DHCP) server.

### Command Mode

DHCP relay server configuration

### Syntax Description

*interval*                      Wait interval in seconds. The range of values is 0 to 60.

### Default

The wait interval is 0 seconds.

### Usage Guidelines

Use the **min-wait** command to configure the interval, in seconds, to wait before forwarding requests to the DHCP server.

Use the **no** or **default** form of this command to return to the default DHCP relay server minimum wait interval of 0 seconds.

### Examples

The following example configures a wait interval of 45 seconds for DHCP relay server, 10.30.40.50:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#min-wait 45
[local]Redback(config-dhcp-relay)#
```

### Related Commands

**dhcp relay server**  
**forward-all**  
**max-hops**  
**server-group**  
**standby**

## offer-lease-time

**offer-lease-time** *seconds*

**no offer-lease-time** *seconds*

### Purpose

Specifies the offer lease time for this internal Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

### Command Mode

DHCP server configuration

DHCP subnet configuration

### Syntax Description

|                |                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------|
| <i>seconds</i> | Length of time for the default lease. The range of values is 60 (one minute) to 360 (one hour). |
|----------------|-------------------------------------------------------------------------------------------------|

### Default

The default value for the offer lease time is two minutes.

### Usage Guidelines

Use the **offer-lease-time** command to specify the offer lease time for the DHCP server or one of its subnets. When entered in DHCP server configuration mode, specifies the offer lease time for the server and all its subnets; when entered in DHCP subnet configuration mode, specifies offer lease time for that subnet. The value specified for a subnet overrides the global value for the server.

Use the **no** form of this command to specify the default value for the offer lease time.

### Examples

The following example specifies an offer lease time of 5 minutes (300) for the DHCP server and all its subnets:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#offer-lease-time 300
```

### Related Commands

**default-lease-time**

**max-lease-time**

**subnet**



# option

**option** {*opt-num* | *opt-name*} *opt-arg1* [*opt-arg2* [*opt-arg3* [*opt-arg4*]]]  
**no option** {*opt-num* | *opt-name*}

## Purpose

Specifies an option for this internal Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

## Command Mode

DHCP server configuration  
DHCP subnet configuration

## Syntax Description

|                                     |                                                                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>opt-num</i>                      | DHCP option number; the range of values is 1 to 125. Table 5-6 to Table 5-12 list the option numbers.                                                                |
| <i>opt-name</i>                     | DHCP option name. Table 5-6 to Table 5-12 list the option names.                                                                                                     |
| <i>opt-arg1</i>                     | First argument for the DHCP option. Table 5-6 to Table 5-12 list the arguments for the DHCP options.                                                                 |
| <i>opt-arg2</i> ... <i>opt-arg4</i> | Optional. Additional values for a DHCP option with an IP address argument. If <i>opt-arg1</i> is an IP address, you can specify up to three additional IP addresses. |

## Default

No DHCP options are specified for the DHCP server or for any of its subnets.

## Usage Guidelines

Use the **option** command to specify an option for this internal DHCP server or for one of its subnets. When you enter this command in DHCP server configuration mode, it specifies the DHCP option for the server and all its subnets; when you enter it in DHCP subnet configuration mode, it specifies the option for that subnet. The value specified for a subnet overrides the global value for the server.

You can enter this command multiple times to specify as many different DHCP options as you require. Succeeding entries for the same DHCP option overwrite any previously entered value.

You can specify up to four IP addresses for a DHCP option that requires an IP address. If the DHCP option also requires a netmask argument in addition to the IP address, you can specify up to two IP addresses and their netmask arguments.

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, Section 3 through Section 9 describe the option numbers, names, and arguments. Table 5-6 to Table 5-12 list this data for the options in each section; options are listed by code within each table.

Use the **no** form of this command to remove the option from the internal DHCP server or subnet configuration.

**Note** DHCP can send RADIUS-specified vendor-encapsulated options to the DHCP client. RADIUS sends the vendor-encapsulated options using the Redback vendor-specific attribute (VSA) 102 (DHCP-Vendor-Encap-Option). For more information about the format for VSA 127, see Table A-6 in Appendix A, “RADIUS Attributes.”

**Table 5-6 RFC 1497 Vendor Extensions**

| Option Code | Option Name              | Argument | Argument Description                                                     | Option Description                                         |
|-------------|--------------------------|----------|--------------------------------------------------------------------------|------------------------------------------------------------|
| 1           | subnet-mask              | netmask  | Netmask in the format <i>E.F.G.H</i> .                                   | Configure the subnet mask supplied to the client.          |
| 2           | time-offset              | seconds  | Signed integer; the range of values is -2,147,483,648 to +2,147,483,648. | Configure the time offset value.                           |
| 3           | router                   | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the router that the client can use.              |
| 4           | time-server              | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the time server.                                 |
| 5           | ien116-name-server       | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the IEN116 name server.                          |
| 6           | domain-name-server       | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the domain name server.                          |
| 7           | log-server               | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the log server.                                  |
| 8           | cookie-server            | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the cookie server.                               |
| 9           | lpr-server               | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the line printer (LPR) server.                   |
| 10          | impress-server           | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the impress server.                              |
| 11          | resource-location-server | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the resource location server.                    |
| 12          | host-name                | name     | Name of the host.                                                        | Configure the hostname, which can include its domain name. |
| 13          | boot-size                | size     | File size in 512-octet blocks; the range of values is 0 to 65,535.       | Configure the size of the boot file.                       |
| 14          | merit-dump               | path     | Path, including the filename.                                            | Configure the path to the merit dump file.                 |
| 15          | domain-name              | dom-name | Domain name; must be "redback.com" (without quotes).                     | Configure the domain name.                                 |
| 16          | swap-server              | ip-addr  | IP address in the format <i>A.B.C.D</i> .                                | Configure the swap server.                                 |
| 17          | root-path                | path     | Path to the root disk.                                                   | Configure the path to the root disk.                       |
| 18          | extensions-path          | path     | Path to the extensions.                                                  | Configure the extensions path.                             |

**Table 5-7 IP Layer Parameters for a Host**

| Option Num | Option Name              | Argument     | Argument Description                                                                                                                                                                                        | Option Description                  |
|------------|--------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| 19         | ip-forwarding            | boolean-flag | <ul style="list-style-type: none"> <li>• <b>0</b>—Disables IP layer for forwarding.</li> <li>• <b>1</b>—Enables IP layer for forwarding.</li> </ul>                                                         | Configure IP forwarding.            |
| 20         | non-local-source-routing | boolean-flag | <ul style="list-style-type: none"> <li>• <b>0</b>—Disables forwarding of datagrams with nonlocal source routes.</li> <li>• <b>1</b>—Enables forwarding of datagrams with nonlocal source routes.</li> </ul> | Configure non-local source routing. |

Table 5-7 IP Layer Parameters for a Host (*continued*)

| Option Num | Option Name                   | Argument                         | Argument Description                                                                    | Option Description                                                                    |
|------------|-------------------------------|----------------------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 21         | <b>policy-filter</b>          | <i>ip-addr</i><br><i>netmask</i> | IP address in the format <i>A.B.C.D.</i><br>Netmask in the format <i>E.F.G.H.</i>       | Configure a policy filter.                                                            |
| 22         | <b>max-dgram-reassembly</b>   | <i>max-size</i>                  | Maximum size of any datagram that needs reassembly; the range of values is 0 to 65,535. | Configure the maximum size for datagram reassembly.                                   |
| 23         | <b>default-ip-ttl</b>         | <i>seconds</i>                   | The range of values is 0 to 255.                                                        | Configure the default IP time-to-live value.                                          |
| 24         | <b>path-mtu-aging-timeout</b> | <i>seconds</i>                   | The range of values is 0 to 4,294,967,295.                                              | Configure the timeout value to use when aging path maximum transmission units (MTUs). |
| 25         | <b>path-mtu-plateau-table</b> | <i>mtu</i>                       | The range of values is 0 to 65,535.                                                     | Configure the table of MTU sizes for use when performing Path MTU discovery.          |

Table 5-8 IP Layer Parameters for an Interface

| Option Num | Option Name                        | Argument                         | Argument Description                                                                                                                                                 | Description                                   |
|------------|------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 26         | <b>interface-mtu</b>               | <i>mtu</i>                       | The range of values is 0 to 65,535.                                                                                                                                  | Configure the interface MTU.                  |
| 27         | <b>all-subnets-local</b>           | <i>boolean-flag</i>              | <ul style="list-style-type: none"> <li>• <b>0</b>—Some subnets can have smaller MTUs.</li> <li>• <b>1</b>—All subnets share the same MTU.</li> </ul>                 | Configure all subnets are local.              |
| 28         | <b>broadcast-address</b>           | <i>ip-addr</i>                   | IP address in the format <i>A.B.C.D.</i>                                                                                                                             | Configure the broadcast IP address.           |
| 29         | <b>perform-mask-discovery</b>      | <i>boolean-flag</i>              | <ul style="list-style-type: none"> <li>• <b>0</b>—Client does not perform mask discovery.</li> <li>• <b>1</b>—Client performs mask discovery.</li> </ul>             | Configure mask discovery.                     |
| 30         | <b>mask-supplier</b>               | <i>boolean-flag</i>              | <ul style="list-style-type: none"> <li>• <b>0</b>—Client should not respond.</li> <li>• <b>1</b>—Client should respond.</li> </ul>                                   | Configure the mask supplier.                  |
| 31         | <b>router-discovery</b>            | <i>boolean-flag</i>              | <ul style="list-style-type: none"> <li>• <b>0</b>—Client should perform router discovery.</li> <li>• <b>1</b>—Client should not perform router discovery.</li> </ul> | Configure router discovery.                   |
| 32         | <b>router-solicitation-address</b> | <i>ip-addr</i>                   | IP address in the format <i>A.B.C.D.</i>                                                                                                                             | Configure the router solicitation IP address. |
| 33         | <b>static-route</b>                | <i>ip-addr</i><br><i>netmask</i> | <ul style="list-style-type: none"> <li>• IP address in the format <i>A.B.C.D.</i></li> <li>• Netmask in the format <i>E.F.G.H.</i></li> </ul>                        | Configure the static route.                   |

Table 5-9 Link Layer Parameters for an Interface

| Option Num | Option Name                  | Argument            | Argument Description                                                                                                                                               | Description                                                    |
|------------|------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| 34         | <b>trailer-encapsulation</b> | <i>boolean-flag</i> | <ul style="list-style-type: none"> <li>• <b>0</b>—Client should not attempt to use trailers.</li> <li>• <b>1</b>—Client should attempt to use trailers.</li> </ul> | Configure trailer encapsulation.                               |
| 35         | <b>arp-cache-timeout</b>     | <i>seconds</i>      | The range of values is 0 to 4,294,967,295.                                                                                                                         | Configure the Address Resolution Protocol (ARP) cache timeout. |

Table 5-9 Link Layer Parameters for an Interface (*continued*)

| Option Num | Option Name                    | Argument            | Argument Description                                                                                                                                                                                                               | Description                     |
|------------|--------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| 36         | <b>ieee802-3-encapsulation</b> | <i>boolean-flag</i> | <ul style="list-style-type: none"> <li><b>0</b>—Client should use Ethernet version 2 encapsulation (RFC 894<sup>1</sup>).</li> <li><b>1</b>—Client should use Ethernet IEEE 802.3 encapsulation (RFC 1042<sup>2</sup>).</li> </ul> | Specify Ethernet encapsulation. |

1. RFC 894, *Standard for the Transmission of IP Datagrams over Ethernet Networks*

2. RFC 1042, *Standard for the Transmission of IP Datagrams over IEEE 802 Ethernet Networks*

Table 5-10 TCP Parameters

| Option Num | Option Name                   | Argument            | Argument Description                                                                                                                                 | Description                                                                   |
|------------|-------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| 37         | <b>default-tcp-ttl</b>        | <i>seconds</i>      | The range of values is 0 to 255.                                                                                                                     | Configure the default Transmission Control Protocol (TCP) time-to-live value. |
| 38         | <b>tcp-keepalive-interval</b> | <i>seconds</i>      | The range of values is 0 to 4,294,967,295.                                                                                                           | Configure the TCP keepalive interval.                                         |
| 39         | <b>tcp-keepalive-garbage</b>  | <i>boolean-flag</i> | <ul style="list-style-type: none"> <li><b>0</b>—Client should not send garbage octet.</li> <li><b>1</b>—Client should send garbage octet.</li> </ul> | Configure the use of a TCP keepalive garbage octet.                           |

Table 5-11 Application and Service Parameters

| Option Num | Option Name                        | Argument                                                                                                 | Argument Description                                                                                          | Description                                                                                           |
|------------|------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 40         | <b>nis-domain</b>                  | <i>dom-name</i>                                                                                          | NIS domain                                                                                                    | Configure the Network Information Server (NIS) domain.                                                |
| 41         | <b>nis-server</b>                  | <i>ip-addr</i>                                                                                           | IP address in the format A.B.C.D.                                                                             | Configure the NIS server.                                                                             |
| 42         | <b>ntp-server</b>                  | <i>ip-addr</i>                                                                                           | IP address in the format A.B.C.D.                                                                             | Configure the Network Time Protocol (NTP) server.                                                     |
| 43         | <b>vendor-encapsulated-options</b> | Can be: <ul style="list-style-type: none"> <li><b>numeric num</b></li> <li><b>string name</b></li> </ul> | <ul style="list-style-type: none"> <li><i>num</i>—Option number.</li> <li><i>name</i>—Option name.</li> </ul> | Configure a vendor-encapsulated option.                                                               |
| 44         | <b>netbios-name-server</b>         | <i>ip-addr</i>                                                                                           | IP address in the format A.B.C.D.                                                                             | Configure the NetBIOS name server.                                                                    |
| 45         | <b>netbios-dd-server</b>           | <i>ip-addr</i>                                                                                           | IP address in the format A.B.C.D.                                                                             | Configure the NetBIOS datagram distribution (DD) server.                                              |
| 46         | <b>netbios-node-type</b>           | <i>type</i>                                                                                              | The range of values is 0 to 255.                                                                              | Configure the NetBIOS node type.                                                                      |
| 47         | <b>netbios-scope</b>               | <i>scope</i>                                                                                             | NetBIOS scope parameter.                                                                                      | Configure the NetBIOS scope parameter, as specified in RFCs 1001 <sup>1</sup> and 1002 <sup>2</sup> . |
| 48         | <b>font-server</b>                 | <i>ip-addr</i>                                                                                           | IP address in the format A.B.C.D.                                                                             | Configure the font server.                                                                            |
| 49         | <b>x-display-manager</b>           | <i>ip-addr</i>                                                                                           | IP address in the format A.B.C.D.                                                                             | Configure the X window system display manager.                                                        |
| 64         | <b>nisplus-domain</b>              | <i>dom-name</i>                                                                                          | NIS+ domain.                                                                                                  | Configure the NIS+ domain.                                                                            |

**Table 5-11 Application and Service Parameters** (*continued*)

| Option Num | Option Name                                   | Argument       | Argument Description                     | Description                                                  |
|------------|-----------------------------------------------|----------------|------------------------------------------|--------------------------------------------------------------|
| 65         | <b>nisplus-server</b>                         | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the NIS+ server.                                   |
| 68         | <b>mobile-ip-home-agent</b>                   | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the mobile IP home agent.                          |
| 69         | <b>smtp-server</b>                            | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the Simple Mail Transport Protocol (SMTP) server.  |
| 70         | <b>pop-server</b>                             | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the Post Office Protocol (POP3) server.            |
| 71         | <b>nnntp-server</b>                           | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the Network News Transport Protocol (NNTP) server. |
| 72         | <b>www-server</b>                             | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the WWW server.                                    |
| 73         | <b>finger-server</b>                          | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the finger server.                                 |
| 74         | <b>irc-server</b>                             | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the default Internet Relay Chat (IRC) server.      |
| 75         | <b>streettalk-server</b>                      | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the StreetTalk server.                             |
| 76         | <b>streettalk-directory-assistance-server</b> | <i>ip-addr</i> | IP address in the format <i>A.B.C.D.</i> | Configure the StreetTalk directory assistance (STDA) server. |

1. RFC 1001, *Protocol Standard for a NetBIOS Service on a TCP/UDP transport: Concepts and Methods*

2. RFC 1002, *Protocol Standard for a NetBIOS Service on a TCP/UDP transport: Detailed Specifications*

**Table 5-12 DHCP Extension**

| Option Num | Option Name             | Argument    | Argument Description | Description                                                 |
|------------|-------------------------|-------------|----------------------|-------------------------------------------------------------|
| 66         | <b>tftp-server-name</b> | <i>name</i> | TFTP server name.    | Configure the Trivial File Transfer Protocol (TFTP) server. |
| 67         | <b>bootfile-name</b>    | <i>name</i> | Boot filename.       | Configure the name of the boot loader image file.           |

## Examples

The following example specifies the options for an internal DHCP server (and its subnets), which are overridden by the options for the sub2 subnet:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
! Specify global options (these apply to all subnets)
[local]Redback(config-dhcp-server)#option domain-name redback.com
[local]Redback(config-dhcp-server)#option domain-name-server 10.1.1.254
! Create a subnet; specify options for this subnet, which override the global settings
[local]Redback(config-dhcp-server)#subnet 10.1.1.1/24 name sub2
[local]Redback(config-dhcp-subnet)#option router 10.1.1.1
[local]Redback(config-dhcp-subnet)#option domain-name hot.com
```

## Command Descriptions

---

The following example adds a second IP address for the router option in the sub2 subnet configuration and includes option 21 (**policy-filter**) with two IP addresses and their netmasks:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 10.1.1.1/24 name sub2
[local]Redback(config-dhcp-subnet)#option router 10.1.1.1 10.1.1.2
[local]Redback(config-dhcp-subnet)#option 21 10.1.1.23 255.255.255.255 10.1.1.33
255.255.255.255
```

## Related Commands

**subnet**

## option-82

To specify the Agent-Circuit-Id, the syntax is:

**option-82 circuit-id** *string* [**offset** *position*] {**ip-address** *ip-addr* | **max-addresses** *num-addr*}

**no option-82 circuit-id** *string* [**offset** *position*] {**ip-address** *ip-addr* | **max-addresses** *num-addr*}

To specify the Remote-Agent-Id, the syntax is:

**option-82 remote-id** *string* [**offset** *position*] **ip-address** *ip-addr*

**no option-82 remote-id** *string*

### Purpose

Creates a static mapping between the Agent-Circuit-Id subfield or the Agent-Remote-Id subfield in the option 82 field and an IP address.

### Command Mode

DHCP subnet configuration

### Syntax Description

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>circuit-id</b> <i>string</i>      | Agent-Circuit-Id. A text string, with up to 255 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>remote-id</b> <i>string</i>       | Agent-Remote-Id. A text string, with up to 255 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>offset</b> <i>position</i>        | Optional. Position of the starting octet in the option 82 subfield which is to be matched with the specified <i>string</i> argument, according to one of the following formats: <ul style="list-style-type: none"> <li>• <b>+n</b> or <b>n</b>—Starting octet is the <i>n</i>th octet in the received Id. The matching operation is performed on the <i>n</i>th and succeeding octets for the length of the string specified by the value of the <i>string</i> argument.</li> <li>• <b>–n</b>—Starting octet is the last octet in the received Id minus the previous (<i>n</i>–1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the value of the <i>string</i> argument.</li> </ul> <p>The default value is 1 (the first octet). You can also specify the first octet with a value of 0.</p> |
| <b>ip-address</b> <i>ip-addr</i>     | IP address to which the option 82 subfield is to be mapped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>max-addresses</b> <i>num-addr</i> | Maximum number of IP addresses permitted for the specified Agent-Circuit-Id.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Default

No static mapping is created between an option 82 subfield and any IP address.

### Usage Guidelines

Use the **option-82** command to create a static mapping between the Agent-Circuit-Id subfield or the Agent-Remote-Id subfield in the option 82 field and an IP address. The option 82 field is sent in the DHCP discover packet.

The value for the *ip-addr* argument must be an IP address within this subnet, but not within any range of IP addresses that you have specified using the **range** command (in DHCP subnet configuration mode).

You can specify the Remote-Agent-Id and the Agent-Circuit-Id in Redback® vendor-specific attributes (VSAs) 96 and 97, respectively, using the **radius attribute calling-station-id** and **radius attribute nas-port-id** commands (in context configuration mode). Redback VSAs are described in Appendix A, “RADIUS Attributes.”

Use the **no** form of this command to delete the static mapping.

### Examples

The following example creates a static mapping between option 82 Agent-Circuit-Id subfield, 4:1 vlan 102 and the 12.1.1.11 IP address:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 12.1.1.0/24 name sub2
[local]Redback(config-dhcp-subnet)#range 12.1.1.50 12.1.1.100
[local]Redback(config-dhcp-subnet)#mac-address 02:12:34:56:78:90 ip-address 12.1.1.10
[local]Redback(config-dhcp-subnet)#option-82 circuit-id "4:1 vlan 102" offset 3
ip-address 12.1.1.11
```

### Related Commands

- mac-address**
- radius attribute calling-station-id**
- radius attribute nas-port-id**
- range**



## range

**range** *start-ip-addr end-ip-addr*

**no range** *start-ip-addr end-ip-addr*

### Purpose

Assigns a range of IP addresses to this Dynamic Host Configuration Protocol (DHCP) subnet.

### Command Mode

DHCP subnet configuration

### Syntax Description

|                      |                                   |
|----------------------|-----------------------------------|
| <i>start-ip-addr</i> | Starting IP address of the range. |
| <i>end-ip-addr</i>   | Ending IP address of the range.   |

### Default

No range of IP addresses is assigned to any subnet.

### Usage Guidelines

Use the **range** command to assign a range of IP addresses to this DHCP subnet.

The values of the *start-ip-addr* and *end-ip-addr* arguments must be within the subnet of IP addresses that you have assigned to this subnet using the **subnet** command (in DHCP server configuration mode).

Use the **no** form of this command to delete the range from the subnet configuration.

### Examples

The following example assigns a range of IP addresses to the sub2 subnet:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 13.1.1.1/24 name sub2
[local]Redback(config-dhcp-subnet)#range 13.1.1.50 13.1.1.100
```

### Related Commands

**subnet**

## server-group

**server-group** *group-name*

**no server-group**

### Purpose

Assigns a Dynamic Host Configuration Protocol (DHCP) server to a DHCP server group.

### Command Mode

DHCP relay server configuration

### Syntax Description

*group-name*                      DHCP server group name.

### Default

DHCP servers are assigned to the default DHCP server group.

### Usage Guidelines

Use the **server-group** command to assign a DHCP server to a DHCP server group.

Use the **no** form of this command to assign a DHCP server to the default server group.

### Examples

The following example assigns DHCP server, foofoo, to the int-grp DHCP server group:

```
[local]Redback(config-ctx)#dhcp relay server foofoo  
[local]Redback(config-dhcp-relay)#server-group int-grp  
[local]Redback(config-dhcp-relay)#
```

### Related Commands

**dhcp relay server**  
**forward-all**  
**standby**

## standby

**standby** {*ip-addr* | *hostname*}  
**no standby** {*ip-addr* | *hostname*}

### Purpose

Configures the IP address or hostname of a standby Dynamic Host Configuration Protocol (DHCP) server.

### Command Mode

DHCP relay server configuration

### Syntax Description

|                 |                                        |
|-----------------|----------------------------------------|
| <i>ip-addr</i>  | IP address of the standby DHCP server. |
| <i>hostname</i> | Hostname of the standby DHCP server.   |

### Default

No standby DHCP server is assigned.

### Usage Guidelines

Use the **standby** command to configure the IP address or hostname of a standby DHCP server.

**Note** When a DHCP server is unreachable, you either forward packets to its standby DHCP server, or forward packets to all other DHCP servers in a DHCP server group, but not both; the **standby** and **forward-all** commands are mutually exclusive.

Use the **no** form of this command to remove the assignment of the standby DHCP server.

### Examples

The following example configures 10.30.40.55 as the IP address for the standby DHCP server, where 192.168.1.10 is the IP address for the associated primary DHCP server:

```
[local]Redback(config-ctx)#dhcp relay server 192.168.1.10  
[local]Redback(config-dhcp-relay)#standby 10.30.40.55  
[local]Redback(config-dhcp-relay)#
```

### Related Commands

**dhcp relay server**  
**forward-all**  
**server-group**

## subnet

**subnet** *ip-addr/subnet-mask* [**name** *subnet-name*]

**no subnet** *ip-addr/subnet-mask* [**name** *subnet-name*]

### Purpose

Creates a subnet for this internal Dynamic Host Configuration Protocol (DHCP) server and accesses DHCP subnet configuration mode.

### Command Mode

DHCP server configuration

### Syntax Description

|                                |                                                  |
|--------------------------------|--------------------------------------------------|
| <i>ip-addr/subnet-mask</i>     | IP address and subnet mask for this subnet.      |
| <b>name</b> <i>subnet-name</i> | Optional. Name of the subnet; it must be unique. |

### Default

No subnets are created for any DHCP server.

### Usage Guidelines

Use the **subnet** command to create a subnet for this internal DHCP server and access DHCP subnet configuration mode.

The value of the *ip-addr* and *subnet-mask* arguments must match the value of one of the *ip-addr* and *subnet-mask* arguments that you specified, using the **ip address** command (in interface configuration mode), for the interface that you enabled for this DHCP server, using the **dhcp server** command (in interface configuration mode). For more information about the **ip address** command, see the “Interface Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Use the **name** *subnet-name* construct to assign a unique name to this subnet.

Use the **no** form of this command to delete the subnet from the DHCP server configuration.

### Examples

The following example creates the sub2 subnet:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp-if multibind
[local]Redback(config-if)#ip address 12.1.1.0/24
[local]Redback(config-if)#ip address 13.1.1.1/24 secondary
[local]Redback(config-if)#dhcp server 13.1.1.1
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 12.1.1.0/24 name sub2
[local]Redback(config-dhcp-subnet)#
```

**Related Commands**

|                           |                     |
|---------------------------|---------------------|
| <b>default-lease-time</b> | <b>option</b>       |
| <b>mac-address</b>        | <b>option-82</b>    |
| <b>max-lease-time</b>     | <b>range</b>        |
| <b>offer-lease-time</b>   | <b>vendor-class</b> |

## user-class-id

**user-class-id** *user-class-id* [**offset** *position*] **giaddr** *ip-addr*

**no user-class-id** *user-class-id*

### Purpose

Specifies an IP address for the giaddr field in the header of Dynamic Host Configuration Protocol (DHCP) packets for the specified user class ID (option 77) field.

### Command Mode

DHCP giaddr configuration

### Syntax Description

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>user-class-id</i>          | Identifier to be matched against the contents of the DHCP option 77 ID field in DHCP discover packets, in one of the formats given in the “Usage Guidelines” section, for which this IP address is intended.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>offset</b> <i>position</i> | <p>Optional. Position of the starting octet in the option 77 field which is to be matched with the specified <i>user-class-id</i> argument, according to one of the following formats:</p> <ul style="list-style-type: none"><li>• <i>+n</i> or <i>n</i>—Starting octet is the <i>n</i>th octet in the received ID. The matching operation is performed on the <i>n</i>th and succeeding octets for the length of the string specified by the value of the <i>user-class-id</i> argument.</li><li>• <i>-n</i>—Starting octet is the last octet in the received ID minus the previous (<i>n</i>-1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the value of the <i>user-class-id</i> argument.</li></ul> <p>The default value is 1 (the first octet). You can also specify the first octet with a value of 0.</p> |
| <b>giaddr</b> <i>ip-addr</i>  | IP address to be inserted in the giaddr field in the header of DHCP packets for the specified user class ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### Default

The giaddr field is set to the primary IP address of the interface.

### Usage Guidelines

Use the **user-class-id** command to specify the IP address for the giaddr field in the header of DHCP packets for the specified user class ID (option 77) field. Option 77 is described in RFC 3004, *The User Class Option for DHCP*.

When the SmartEdge router receives a DHCP discover packet, the SmartEdge OS performs a matching operation, comparing the contents of the option 77 field, starting at the octet within the field, as specified by the value of the *position* argument, with the string specified by the value of the *user-class-id* argument.

If more than one user class ID field is present in the option 77 field in the DHCP discover packet, the system uses only the first user class ID field to make the comparison for setting the giaddr field. The remaining user class ID fields are ignored.

If there is a match, the system inserts the specified IP address in the giaddr field in the header of DHCP packets to this client. If there is no match, the system inserts the primary IP address that you have configured for this interface.

Possible formats for the *user-class-id* argument are:

- Alphanumeric string, enclosed in quotation marks (" "); for example, "ABCD1234"
- Alphanumeric string, not enclosed in quotation marks; for example, redback1
- Hex numeric string, not enclosed in quotation marks and prefaced with 0x or 0X; for example, 0Xabcd1234

Use the **giaddr ip-addr** construct to specify an IP address for the specified *user-class-id* argument. This IP address must be one of the secondary IP addresses that you have configured for the interface. You can specify the same IP address or different IP addresses for multiple values of the *user-class-id* argument.

Use the **no** form of this command to delete the giaddr IP address for the specified *user-class-id* argument.

**Note** If you delete this DHCP proxy or relay from the configuration, using the **no** form of the **dhcp proxy** or **dhcp relay** command (in interface configuration mode), you also delete all **user-class-id** commands for that DHCP proxy or relay.

## Examples

The following example specifies secondary IP addresses for the interface in which the DHCP proxy server is configured, and then specifies one of them as the IP address for the giaddr field for the network user class ID:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface voip multibind
[local]Redback(config-if)#ip address 200.1.1.1/24
[local]Redback(config-if)#ip address 200.1.2.1/24 secondary
[local]Redback(config-if)#ip address 200.1.10.1/24 secondary
[local]Redback(config-if)#dhcp proxy 16000
[local]Redback(config-dhcp-giaddr)#user-class-id network giaddr 200.1.2.1
```

## Related Commands

**dhcp proxy**  
**dhcp relay**

## vendor-class

**vendor-class** *vendor-class-id* [**offset** *position*] **subnet-name** *subnet-name*  
**no vendor-class** *vendor-class-id*

### Purpose

Creates a static mapping between a subnet and the specified vendor class ID.

### Command Mode

DHCP server configuration

### Syntax Description

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>vendor-class-id</i>                | Vendor class ID for which a static mapping is to be created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>offset</b> <i>position</i>         | <p>Optional. Position of the starting octet in the option 60 field which is to be matched with the specified <i>vendor-class-id</i> argument, according to one of the following formats:</p> <ul style="list-style-type: none"> <li>• <i>+n</i> or <i>n</i>—Starting octet is the <i>n</i>th octet in the received ID. The matching operation is performed on the <i>n</i>th and succeeding octets for the length of the string specified by the value of the <i>vendor-class-id</i> argument.</li> <li>• <i>-n</i>—Starting octet is the last octet in the received ID minus the previous (<i>n</i>-1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the value of the <i>vendor-class-id</i> argument.</li> </ul> <p>The default value is 1 (the first octet). You can also specify the first octet with a value of 0.</p> |
| <b>subnet-name</b> <i>subnet-name</i> | Subnet name for the specified vendor class ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### Default

No static mapping is created between a subnet and any vendor class ID.

### Usage Guidelines

Use the **vendor-class** command to create a static mapping between a subnet and the specified vendor class ID.

Use the **no** form of this command to delete the static mapping between the vendor class ID and the subnet.

### Examples

The following example specifies the `for - subs` subnet as the subnet for the 123456 vendor class ID:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#vendor-class 123456 offset 1 subnet-name for-subs
```



## Related Commands

`subnet`  
`vendor-class-id`

## vendor-class-id

**vendor-class-id** *vendor-class-id* [**offset** *position*] **giaddr** *ip-addr*

**no vendor-class-id** *vendor-class-id*

### Purpose

Specifies an IP address for the giaddr field in the header in Dynamic Host Configuration Protocol (DHCP) packets for the specified vendor class ID (option 60) field.

### Command Mode

DHCP giaddr configuration

### Syntax Description

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>vendor-class-id</i>        | Identifier to be matched against the contents of the DHCP option 60 ID field in DHCP discover packets, in one of the formats given in the “Usage Guidelines” section, for which this IP address is intended.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>offset</b> <i>position</i> | <p>Optional. Position of the starting octet in the option 60 field which is to be matched with the specified <i>vendor-class-id</i> argument, according to one of the following formats:</p> <ul style="list-style-type: none"><li>• <i>+n</i> or <i>n</i>—Starting octet is the <i>n</i>th octet in the received ID. The matching operation is performed on the <i>n</i>th and succeeding octets for the length of the string specified by the value of the <i>vendor-class-id</i> argument.</li><li>• <i>-n</i>—Starting octet is the last octet in the received ID minus the previous (<i>n</i>-1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the value of the <i>vendor-class-id</i> argument.</li></ul> <p>The default value is 1 (the first octet). You can also specify the first octet with a value of 0.</p> |
| <b>giaddr</b> <i>ip-addr</i>  | IP address to be inserted in the giaddr field in the header of DHCP packets for the specified vendor class ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### Default

The giaddr field is set to the primary IP address of the interface.

### Usage Guidelines

Use the **vendor-class-id** command to specify the IP address for the giaddr field in DHCP packets for the specified vendor class ID (option 60) field. option 60 is described in RFC 2131, *DHCP Options and BootP Vendor Extensions*.

When the SmartEdge router receives a DHCP discover packet, the SmartEdge OS performs a matching operation, comparing the contents of the option 60 field, starting at the octet within the field, as specified by the value of the *position* argument, with the string specified by the value of the *vendor-class-id* argument.

If there is a match, the system inserts the specified IP address in the `giaddr` field in the header of DHCP packets to this client. If there is no match, the system inserts the primary IP address that you have configured for this interface.

Possible formats for the *vendor-class-id* argument are:

- Alphanumeric string, enclosed in quotation marks (“ ”); for example, “ABCD1234”
- Alphanumeric string, not enclosed in quotation marks; for example, `redback1`
- Hex numeric string, not enclosed in quotation marks and prefaced with `0x` or `0X`; for example, `0Xabcd1234`

Use the **giaddr** *ip-addr* construct to specify an IP address for the specified *vendor-class-id* argument. This IP address must be one of the secondary IP addresses that you have configured for the interface. You can specify the same IP address or different IP addresses for multiple values of the *vendor-class-id* argument.

Use the **no** form of this command to delete the `giaddr` IP address for the specified *vendor-class-id* argument.

**Note** If you delete this DHCP proxy or relay from the configuration, using the **no** form of the **dhcp proxy** or **dhcp relay** command (in interface configuration mode), you also delete all **vendor-class-id** commands for that DHCP proxy or relay.

## Examples

The following example specifies secondary IP addresses for the interface in which the DHCP proxy server is configured, and then specifies one of them as the IP address for the `giaddr` field for the `redback` vendor class ID:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface voip multibind
[local]Redback(config-if)#ip address 200.1.1.1/24
[local]Redback(config-if)#ip address 200.1.2.1/24 secondary
[local]Redback(config-if)#ip address 200.1.10.1/24 secondary
[local]Redback(config-if)#dhcp proxy 16000
[local]Redback(config-dhcp-giaddr)#vendor-class-id redback offset -17 giaddr 200.1.2.1
```

## Related Commands

**dhcp proxy**  
**dhcp relay**



# IP Services

---

This part describes the tasks and commands used to configure Domain Name System (DNS), HTTP redirect, and access control lists (ACLs) for IP services and policies. It consists of the following chapters:

- Chapter 6, “DNS Configuration”
- Chapter 7, “HTTP Redirect Configuration”
- Chapter 8, “ACL Configuration”



# DNS Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS Domain Name System (DNS) features.

For information about the tasks and commands used to monitor, troubleshoot, and administer DNS features, see the “DNS Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

**Note** When IP Version 6 (IPv6) addresses are not referenced or explicitly specified, the term, IP address, can refer generally to IP Version 4 (IPv4) addresses, IPv6 addresses, or IP addressing. In instances where IPv6 addresses are referenced or explicitly specified, the term, IP address, refers only to IPv4 addresses. For a description of IPv6 addressing and the types of IPv6 addresses, see RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

DNS maps hostnames to IP addresses. When a command refers to a hostname, the SmartEdge OS consults the host table for mappings to IP addresses. If the information is not in the table, the SmartEdge OS generates a DNS query to resolve the hostname. DNS is enabled on a per-context basis, with one domain name allowed per context.

# Configuration Tasks

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure DNS, perform the tasks described in the following sections:

- Configure DNS
- Enable DNS to Establish Subscriber Sessions (Optional)
- Configure Static Hostname-to-IP Address Mappings (Optional)

## Configure DNS

To configure DNS, perform the tasks described in Table 6-1; enter all commands in context configuration mode.

**Table 6-1 Configure DNS**

| Task                                                                                                         | Root Command             | Notes                                                                        |
|--------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------------------------------------------------------|
| Specify a domain name (or alias) for the context.                                                            | <b>ip domain-name</b>    | You can create up to six domain names per context.                           |
| Specify the IP address of a primary (and, optionally, secondary) DNS server with one of the following tasks: |                          | For DNS resolution to function, there must be an IP route to the DNS server. |
| • Specify IPv4 addresses.                                                                                    | <b>ip name-servers</b>   |                                                                              |
| • Specify IPv6 addresses.                                                                                    | <b>ipv6 name-servers</b> |                                                                              |
| Enable the SmartEdge OS to use DNS resolution to look up hostname-to-IP address mappings.                    | <b>ip domain-lookup</b>  | For DNS resolution to function, you must configure domain-name lookup.       |

## Enable DNS to Establish Subscriber Sessions (Optional)

To enable subscriber sessions to be established using DNS, perform the task described in Table 6-2.

**Table 6-2 Enable DNS to Establish Subscriber Sessions (Optional)**

| Task                                                                                        | Root Command | Notes                                                |
|---------------------------------------------------------------------------------------------|--------------|------------------------------------------------------|
| Configure the IP address of a primary or secondary DNS server that a subscriber should use. | <b>dns</b>   | Enter this command in subscriber configuration mode. |



## Configure Static Hostname-to-IP Address Mappings (Optional)

In addition to having DNS perform dynamic resolution, you can configure static hostname-to-IP address mappings. To do so, perform the task described in Table 6-3; enter all commands in context configuration mode.

**Table 6-3** Configure Static Hostname-to-IP Address Mappings

| Task                                                                                             | Root Command     | Notes                                                                                                                                             |
|--------------------------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Create static hostname-to-IP address mappings in the host table with one of the following tasks: |                  | The SmartEdge OS always consults the host table prior to generating a DNS lookup query. You can create up to 64 static entries in the host table. |
| • Create a mapping with an IPv4 address.                                                         | <b>ip host</b>   |                                                                                                                                                   |
| • Create a mapping with an IPv6 address.                                                         | <b>ipv6 host</b> |                                                                                                                                                   |

## Configuration Examples

The following example configures the `redback.com` domain for the `local` context and configures a connection to a remote DNS server at IP address, `155.53.130.200`. The **ip domain-lookup** command enables DNS resolution.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#ip domain-lookup
[local]Redback(config-ctx)#ip domain-name redback.com
[local]Redback(config-ctx)#ip name-servers 155.53.130.200
```

## Command Descriptions

This section describes the syntax and usage guidelines for the commands used to configure DNS features. The commands are presented in alphabetical order.

|                         |                          |
|-------------------------|--------------------------|
| <b>dns</b>              | <b>ip name-servers</b>   |
| <b>ip domain-lookup</b> | <b>ipv6 host</b>         |
| <b>ip domain-name</b>   | <b>ipv6 name-servers</b> |
| <b>ip host</b>          |                          |

## dns

**dns** {primary | secondary} *ip-addr*  
**no dns** {primary | secondary} *ip-addr*

### Purpose

Configures the IP address of a primary (and, optionally, secondary) Domain Name System (DNS) server for a subscriber.

### Command Mode

subscriber configuration

### Syntax Description

|                  |                                                      |
|------------------|------------------------------------------------------|
| <b>primary</b>   | Configures the IP address of a primary DNS server.   |
| <b>secondary</b> | Configures the IP address of a secondary DNS server. |
| <i>ip-addr</i>   | DNS server IP address.                               |

### Default

There are no preconfigured DNS servers.

### Usage Guidelines

Use the **dns** command to configure the IP address of a primary (and, optionally, secondary) DNS server for a subscriber.

Use the **no** form of this command to remove the DNS server information from a subscriber record.

### Examples

The following example configures a primary DNS server address of 10.2.3.4 for subscriber, kenny:

```
[local]Redback(config-ctx)#subscriber name kenny  
[local]Redback(config-sub)#dns primary 10.2.3.4
```

### Related Commands

**ip domain-lookup**  
**ip domain-name**  
**ip host**  
**ip name-servers**  
**ipv6 host**  
**ipv6 name-servers**

## ip domain-lookup

**ip domain-lookup**

**no ip domain-lookup**

### Purpose

Enables the SmartEdge OS to use Domain Name System (DNS) resolution to look up hostname-to-IP address mappings in the host table for the context.

### Command Mode

context configuration

### Syntax Description

This command has no arguments or keywords.

### Default

DNS lookup is disabled.

### Usage Guidelines

Use the **ip domain-lookup** command to enable the SmartEdge OS to use DNS resolution to look up hostname-to-IP address mappings in the host table for the context.

This command allows a user to ping or Telnet to a host using a hostname, instead of having to know the host's specific IP address. When a command references a hostname, the SmartEdge OS consults the local host table to obtain the hostname-to-IP address mapping. If the information is not in the local host table, the SmartEdge OS generates a DNS query to resolve the hostname.

For DNS resolution to function, one or more DNS servers must be specified using the **ip name-servers** command. Hostnames that are statically entered into the local host table using the **ip host** command are also used for DNS resolution.

Use the **no** form of this command to disable DNS resolution lookup.

### Examples

The following example enables DNS resolution:

```
[local]Redback(config-ctx)#ip domain-lookup
```

### Related Commands

**dns**

**ip domain-name**

**ip host**

**ip name-servers**

**ipv6 host**

**ipv6 name-servers**

## ip domain-name

**ip domain-name** *name*

**no ip domain-name** *name*

### Purpose

Creates a Domain Name System (DNS) name (or alias) for the context.

### Command Mode

context configuration

### Syntax Description

|             |                                                |
|-------------|------------------------------------------------|
| <i>name</i> | Name (or alias) of the domain for the context. |
|-------------|------------------------------------------------|

### Default

No domain names are created for the context.

### Usage Guidelines

Use the **ip domain-name** command to create a domain name (or alias) for the context.

You can create up to six domain names for each context.

Use the **no** form of this command to remove the domain name (or alias) from the configuration.

### Examples

The following example creates a domain name for the `local` context, `redback.com`:

```
[local]Redback(config-ctx)#ip domain-name redback.com
```

### Related Commands

- dns**
- ip domain-lookup**
- ip host**
- ip name-servers**
- ipv6 host**
- ipv6 name-servers**

# ip host

**ip host** *hostname ip-addr*

**no ip host** *hostname ip-addr*

## Purpose

Creates a static hostname-to-IPv4 address Domain Name System (DNS) mapping in the host table for the context.

## Command Mode

context configuration

## Syntax Description

|                 |                           |
|-----------------|---------------------------|
| <i>hostname</i> | Name of the host.         |
| <i>ip-addr</i>  | IPv4 address of the host. |

## Default

No static mappings are preconfigured.

## Usage Guidelines

Use the **ip host** command to create a static hostname-to-IPv4 address DNS mapping in the host table for the context.

You can create up to 64 static entries in the host table. The SmartEdge OS always consults the host table prior to generating a DNS lookup query.

Use the **no** form of this command to remove the specified static entry. Specifying a new IPv4 address for an existing hostname removes the previously specified IPv4 address.

## Examples

The following example statically maps the hostname, hamachi, to the IPv4 address, 192.168.42.105:

```
[local]Redback(config-ctx)#ip host hamachi 192.168.42.105
```

## Related Commands

**dns**  
**ip domain-lookup**  
**ip domain-name**  
**ip name-servers**

## ip name-servers

**ip name-servers** *primary-ip-addr* [*secondary-ip-addr*]

**no ip name-servers**

### Purpose

Specifies the IPv4 address of a primary (and, optionally, a secondary) Domain Name System (DNS) server.

### Command Mode

context configuration

### Syntax Description

|                          |                                                     |
|--------------------------|-----------------------------------------------------|
| <i>primary-ip-addr</i>   | IPv4 address of the primary DNS server.             |
| <i>secondary-ip-addr</i> | Optional. IPv4 address of the secondary DNS server. |

### Default

There are no preconfigured DNS server IPv4 addresses.

### Usage Guidelines

Use the **ip name-servers** command to specify the IPv4 address of a primary (and, optionally, a secondary) DNS server.

For DNS resolution to function, you must configure domain-name lookup using the **ip domain-lookup** command (in context configuration mode), and there must be an IP route to the DNS servers.

Use the **no** form of this command to remove the specified DNS server association. If you delete the primary DNS server, any configured secondary DNS server becomes the primary server.

### Examples

The following command configures an association with a primary DNS server at IPv4 address, 128.215.33.47, and a secondary server at IPv4 address, 196.145.92.33:

```
[local]Redback(config-ctx)#ip name-servers 128.215.33.47 196.145.92.33
```

The following command removes the primary DNS server, making the server that was previously the secondary into the primary:

```
[local]Redback(config-ctx)#no ip name-servers 128.215.33.47
```

### Related Commands

|                         |                       |
|-------------------------|-----------------------|
| <b>dns</b>              | <b>ip domain-name</b> |
| <b>ip domain-lookup</b> | <b>ip host</b>        |

## ipv6 host

**ipv6 host** *hostname ipv6-addr*

**no ipv6 host** *hostname ipv6-addr*

### Purpose

Creates a static hostname-to-IP Version 6 (IPv6) address Domain Name System (DNS) mapping in the host table for the context.

### Command Mode

context configuration

### Syntax Description

|                  |                           |
|------------------|---------------------------|
| <i>hostname</i>  | Name of the host.         |
| <i>ipv6-addr</i> | IPv6 address of the host. |

### Default

No static mappings are preconfigured.

### Usage Guidelines

Use the **ipv6 host** command to create a static hostname-to-IPv6 address DNS mapping in the host table for the context.

You can create up to 64 static entries in the host table. The SmartEdge OS always consults the host table prior to generating a DNS lookup query.

Use the **no** form of this command to remove the specified static entry. Specifying a new IPv6 address for an existing hostname removes the previously specified IPv6 address.

### Examples

The following example statically maps the hostname, hamachi, to the IPv6 address, 2007::1:

```
[local]Redback(config-ctx)#ipv6 host hamachi 2007::1
```

### Related Commands

**dns**  
**ip domain-lookup**  
**ip domain-name**  
**ipv6 name-servers**

## ipv6 name-servers

**ipv6 name-servers** *primary-ipv6-addr* [*secondary-ipv6-addr*]

**no ipv6 name-servers**

### Purpose

Specifies the IP Version 6 (IPv6) address of a primary (and, optionally, a secondary) Domain Name System (DNS) server.

### Command Mode

context configuration

### Syntax Description

|                            |                                                     |
|----------------------------|-----------------------------------------------------|
| <i>primary-ipv6-addr</i>   | IPv6 address of the primary DNS server.             |
| <i>secondary-ipv6-addr</i> | Optional. IPv6 address of the secondary DNS server. |

### Default

There are no preconfigured DNS server IPv6 addresses.

### Usage Guidelines

Use the **ipv6 name-servers** command to specify the IPv6 address of a primary (and, optionally, a secondary) DNS server.

For DNS resolution to function, you must configure the domain name lookup using the **ip domain-lookup** command (in context configuration mode), and there must be an IPv6 route to the DNS servers.

Use the **no** form of this command to remove the specified DNS server association. If you delete the primary DNS server, any configured secondary DNS server becomes the primary server.

### Examples

The following command configures an association with a primary DNS server at IPv6 address, 2007::1, and a secondary server at IPv6 address, 2007::2:

```
[local]Redback(config-ctx)#ipv6 name-servers 2007::1 2007::2
```

The following command removes the primary DNS server, making the server that was previously the secondary into the primary:

```
[local]Redback(config-ctx)#no ipv6 name-servers 2007::1
```

### Related Commands

|                         |                       |
|-------------------------|-----------------------|
| <b>dns</b>              | <b>ip domain-name</b> |
| <b>ip domain-lookup</b> | <b>ipv6 host</b>      |



# HTTP Redirect Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS HTTP redirect features. For information about tasks and commands used to monitor, troubleshoot, and administer HTTP redirect features, see the “HTTP Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

HTTP redirect enables service providers to interrupt subscriber HTTP sessions and to redirect them to a preconfigured URL. Applications include the ability to require customer registration, to direct customers to web sites for downloading virus protection software, and to advertise new services or software updates.

**Note** In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

The SmartEdge router provides a lightweight HTTP server on its controller card. When a subscriber initiates an HTTP session, authentication triggers an HTTP redirect when two conditions are in place: an HTTP redirect profile containing a new URL is attached to the subscriber record, and a forward policy that redirects HTTP traffic to the HTTP server on the controller card is attached to the subscriber circuit. HTTP packets must be permitted to pass through to the external HTTP server that hosts the redirect URL. The subscriber session opens to the web page indicated by the redirect URL. The forward policy that performs the redirection is removed through the subscriber reauthorization mechanism.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure HTTP redirect features, perform the tasks described in the following sections:

- Configure Subscriber Authentication and Reauthorization
- Configure an IP ACL and Apply It to Subscribers
- Configure the HTTP Server on the Active Controller Card
- Configure and Attach an HTTP Redirect Profile to Subscribers
- Configure a Policy ACL That Classifies HTTP Packets
- Configure and Attach a Forward Policy to Redirect HTTP Packets

### Configure Subscriber Authentication and Reauthorization

To configure subscriber authentication and reauthorization, see the “Configure Subscriber Authentication” and “Configure Dynamic Subscriber Reauthorization” sections in Chapter 15, “AAA Configuration.”

### Configure an IP ACL and Apply It to Subscribers

To redirect subscriber traffic to the new web page to which subscriber circuits are to be redirected, you configure an IP access control list (ACL) that permits access to that web page and apply it to the subscriber circuits (their records or profiles) that are to be redirected. To configure and apply an IP ACL, see the “Configure an IP ACL” and “Apply an IP ACL” sections in Chapter 8, “ACL Configuration.”

### Configure the HTTP Server on the Active Controller Card

To configure the HTTP server on the active controller card, perform the tasks described in Table 7-1.

**Table 7-1** Configure the HTTP Server on the Controller Card

| #  | Task                                                                                              | Root Command                | Notes                                                          |
|----|---------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------------------------------|
| 1. | Enable the HTTP server on the controller card and access HTTP redirect server configuration mode. | <b>http-redirect server</b> | Enter this command in global configuration mode.               |
| 2. | Optional. Select the port on which HTTP server listens.                                           | <b>port</b>                 | Enter this command in HTTP redirect server configuration mode. |

## Configure and Attach an HTTP Redirect Profile to Subscribers

To configure and attach an HTTP redirect profile to subscribers, perform the tasks described in Table 7-2.

**Table 7-2** Configure and Attach an HTTP Redirect Profile to Subscribers

| #  | Task                                                                                                                    | Root Command                 | Notes                                                           |
|----|-------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------------------------------------|
| 1. | Configure an HTTP redirect profile and access HTTP redirect profile configuration mode.                                 | <b>http-redirect profile</b> | Enter this command in context configuration mode.               |
| 2. | Configure the URL to which subscriber sessions are to be redirected.                                                    | <b>url</b>                   | Enter this command in HTTP redirect profile configuration mode. |
| 3. | Attach the HTTP redirect profile to a subscriber record, a named subscriber profile, or the default subscriber profile. | <b>http-redirect profile</b> | Enter this command in subscriber configuration mode.            |



**Caution** Risk of redirect loop. Redirect can recur until an IP ACL that permits access to the new web page is applied to the subscriber record or profile. To reduce the risk, before modifying an existing URL, ensure that the subscriber record includes an IP ACL that permits access to the new URL.

The SmartEdge OS applies an HTTP profile in the following order of precedence:

1. Uses the Redback<sup>®</sup> vendor-specific attribute (VSA) 107, HTTP-Redirect-Profile-Name, in the subscriber record returned by the Remote Authentication Dial-In User Service (RADIUS) server in Access-Accept packets for the subscriber.
2. If the RADIUS server does not return an HTTP profile name, it uses the HTTP profile attached to the named subscriber configured in the context.
3. If the named subscriber does not have an HTTP profile attached to it, it uses the HTTP profile attached to the named subscriber profile configured in the context.
4. If the subscriber profile does not have an HTTP profile attached to it, it uses the HTTP profile attached to the default subscriber profile configured in the context.

## Configure a Policy ACL That Classifies HTTP Packets

To configure a policy access control list (ACL) that classifies HTTP packets for the forward policy that redirects HTTP packets, perform the tasks described in Table 7-3.

**Table 7-3 Configure a Policy ACL That Classifies HTTP Packets**

| #  | Task                                                                                         | Root Command              | Notes                                                                                                                                                                                                                                                                                                          |
|----|----------------------------------------------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select the policy ACL and enter access control list configuration mode.            | <b>policy access-list</b> | Enter this command in context configuration mode.                                                                                                                                                                                                                                                              |
| 2. | Assign HTTP packets that are destined to the web server hosting the URL to a separate class. | <b>permit</b>             | Enter this command in access control list configuration mode.<br>Use the following construct:<br><b>permit tcp any host <i>ip-addr</i> eq www class <i>class-name</i></b><br>where the <i>ip-addr</i> argument is the IP address of the web server hosting the URL that you configured in step 2 in Table 7-2. |
| 3. | Assign all other HTTP packets to a different class.                                          | <b>permit</b>             | Enter this command in access control list configuration mode.<br>Use the following construct:<br><b>permit tcp any any eq www class <i>class-name</i></b><br>where the <i>class-name</i> argument is distinct from the one you just configured in step 2.                                                      |

## Configure and Attach a Forward Policy to Redirect HTTP Packets

To configure a forward policy to redirect HTTP packets and attach it to a circuit or subscriber, perform the tasks described in Table 7-4.

**Table 7-4 Configure and Attach a Forward Policy to Redirect HTTP Packets**

| #  | Task                                                                                                                  | Root Command                      | Notes                                                                                                                                                                                                                                       |
|----|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select the forward policy and access forward policy configuration mode.                                     | <b>forward policy</b>             | Enter this command in global configuration mode.<br>For more information about forward policies, see Chapter 9, "Forward Policy Configuration."                                                                                             |
| 2. | Apply the policy ACL that you configured in Table 7-3 to the forward policy and access policy ACL configuration mode. | <b>access-group</b>               | Enter this command in forward policy configuration mode.                                                                                                                                                                                    |
| 3. | Specify all HTTP packets and access policy ACL class configuration mode.                                              | <b>class</b>                      | Enter this command in policy ACL configuration mode.<br>Use the <i>class-name</i> argument that you specified in step 3 in Table 7-3.                                                                                                       |
| 4. | Redirect HTTP packets to the HTTP server on the controller card.                                                      | <b>redirect destination local</b> | Enter this command in policy ACL class configuration mode.                                                                                                                                                                                  |
| 5. | Attach the forward policy to a circuit, a subscriber record, named subscriber profile, or default subscriber profile. | <b>forward policy in</b>          | Enter this command in ATM DS-3, ATM OC, ATM PVC, dot1q PVC, DS-0 group, DS-1, DS-3, Frame Relay PVC, port, or subscriber configuration mode.<br>For more information about forward policies, see Chapter 9, "Forward Policy Configuration." |

# Configuration Examples

The following example provides a simple HTTP redirect configuration:

```
!First enable the HTTP redirect server on the controller card:
[local]Redback(config)#http-redirect server
[local]Redback(config-hr-server)#port 80 8080
[local]Redback(config-hr-server)#exit
!Configure the HTTP redirect profile and url:
[local]Redback(config)#context local
[local]Redback(config-ctx)#http-redirect profile Redirect
[local]Redback(config-hr-profile)#url http://www.Redirect.com
[local]Redback(config-hr-profile)#exit
!Attach the HTTP redirect profile to the default subscriber profile:
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#http-redirect profile Redirect
[local]Redback(config-sub)#exit
!Create a policy ACL:
[local]Redback(config-ctx)#policy access-list http-packets
!Create class abc for HTTP packets that are destined to the web server with the new URL:
[local]Redback(config-access-list)#permit tcp any host 10.1.1.1 eq www class abc
!Create class xyz for all other HTTP packets to be redirected using the forward policy:
[local]Redback(config-access-list)#permit tcp any any eq www class xyz
[local]Redback(config-ctx)#exit
!Create the forward policy:
[local]Redback(config)#forward policy www-redirect
!Apply the policy ACL that classifies HTTP packets:
[local]Redback(config-policy-frwd)#access-group http-packets local
!Redirect all HTTP packets except those destined to the web server (class xyz):
!to the HTTP server on the controller card:
[local]Redback(config-policy-acl)#class xyz
[local]Redback(config-policy-acl-class)#redirect destination local
[local]Redback(config-policy-acl-class)#exit
!Packets that are destined to the web server (class abc) use normal routing (no action).
[local]Redback(config-policy-acl)#class abc
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#exit
[local]Redback(config-policy-frwd)#exit
!Attach the forward policy to incoming packets on ATM PVC 3 5:
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm)#no shutdown
[local]Redback(config-atm-oc)#atm pvc 3 5 profile atm-pro encapsulation bridge1483
[local]Redback(config-atm-pvc)#forward policy www-redirect in
!Bind the appropriate subscriber record to the ATM PVC:
[local]Redback(config-atm-pvc)#bind subscriber joe@local
```

# Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure HTTP redirect features. The commands are presented in alphabetical order.

|                              |                                   |
|------------------------------|-----------------------------------|
| <b>http-redirect profile</b> | <b>redirect destination local</b> |
| <b>http-redirect server</b>  | <b>url</b>                        |
| <b>port</b>                  |                                   |

## http-redirect profile

**http-redirect profile** *prof-name*

**no http-redirect profile** *prof-name*

### Purpose

In context configuration mode, configures an HTTP redirect profile and enters HTTP redirect profile configuration mode.

In subscriber configuration mode, applies an HTTP redirect profile to a subscriber record, a named subscriber profile, or the default subscriber profile.

### Command Mode

context configuration  
subscriber configuration

### Syntax Description

*prof-name* HTTP redirect profile name.

### Default

An HTTP redirect profile is not preconfigured.

### Usage Guidelines

Use the **http-redirect profile** command in context configuration mode to configure an HTTP redirect profile and to enter HTTP redirect profile configuration mode.

Use the **http-redirect profile** command in subscriber configuration mode to apply an HTTP redirect profile to a subscriber record, a named subscriber profile, or the default subscriber profile.

Use the **no** form of this command delete an HTTP redirect profile or to remove an HTTP redirect profile from a subscriber record, a named subscriber profile, or the default subscriber profile.

### Examples

The following example configures the HTTP profile, Redirect, and enters HTTP redirect profile configuration mode:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#http-redirect profile Redirect
[local]Redback(config-hr-profile)#
```

The following example applies the HTTP profile, Redirect, to the default subscriber record in the local context:

```
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#http-redirect profile Redirect
```

Related Commands

None



## http-redirect server

**http-redirect server**  
**no http-redirect server**

### Purpose

Enables an HTTP server on the controller card and accesses HTTP redirect server configuration mode.

### Command Mode

global configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Disabled.

### Usage Guidelines

Use the **http-redirect server** command to enable an HTTP server on the controller card and access HTTP redirect server configuration mode.

Use the **no** form of this command to disable the HTTP server on the controller card.

### Examples

The following example enables the HTTP server on the controller card and enters HTTP redirect server configuration mode:

```
[local]Redback(config)#http-redirect server  
[local]Redback(config-hr-server)#
```

### Related Commands

**http-redirect profile**  
**port**  
**redirect destination local**  
**url**

# port

**port** [80] [8080]

## Purpose

Selects the port (or ports) on which the HTTP server on the controller card listens.

## Command Mode

HTTP redirect server configuration

## Syntax Description

|             |                                                                                      |
|-------------|--------------------------------------------------------------------------------------|
| <b>80</b>   | Optional. Configures the HTTP server to listen on port 80. This is the default port. |
| <b>8080</b> | Optional. Configures the HTTP server to listen on port 8080.                         |

## Default

The HTTP server listens on port 80.

## Usage Guidelines

Use the **port** command to select the port (or ports) on which the HTTP server on the controller card listens.

By default, the HTTP server listens on port 80. You can configure the HTTP server to listen on port 80, port 8080, or on both ports.

## Examples

The following example configures the HTTP server to listen on ports 80 and 8080:

```
[ local ]Redback(config)#http-redirect server  
[ local ]Redback(config-hr-server)#port 80 8080
```

## Related Commands

**http-redirect server**

## redirect destination local

**redirect destination local**

**no redirect destination**

### Purpose

In forward policy configuration mode, redirects packets not associated with a class to the HTTP server on the controller card.

In policy ACL configuration mode, redirects only packets associated with a class to the HTTP server on the controller card.

### Command Mode

forward policy configuration  
policy ACL class configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Packets are not redirected.

### Usage Guidelines

In forward policy configuration mode, use the **redirect destination local** command to redirect packets not associated with a class to the HTTP server on the controller card. In policy ACL configuration mode, use the **redirect destination local** command to redirect only packets associated with a class to the HTTP server on the controller card.

Use the **no** form of this command to disable the redirecting of packets.

### Examples

The following example configures the forward policy, Business-Redirect, which redirects packets associated with the class, Redirect, to the HTTP server on the controller card:

```
[local]Redback(config)#forward policy Business-Redirect
[local]Redback(config-policy-frwd)#redirect destination local
[local]Redback(config-policy-frwd)#access-group bus-redirect local
[local]Redback(config-policy-acl)#class Redirect
[local]Redback(config-policy-acl)#redirect destination local
```

### Related Commands

**http-redirect server**  
**redirect destination circuit**  
**redirect destination next-hop**

## url

**url** *url*

**no url** *url*

### Purpose

Configures the URL to which the current subscriber HTTP session is to be redirected.

### Command Mode

HTTP redirect profile configuration

### Syntax Description

*url* URL to which the subscriber HTTP session is to be redirected. You can add a backslash at the end of the URL followed by any of these wildcards to personalize the URL:

- %d—Domain portion of the subscriber name.
- %u—Username portion of the subscriber name.
- %U—Entire subscriber name used in Point-to-Point Protocol (PPP) authentication.

### Default

An HTTP redirect URL is not configured.

### Usage Guidelines

Use the **url** command to configure the URL to which the current subscriber session is to be redirected.



**Caution** Risk of redirect loop. Risk of redirect loop. Redirect can recur until an IP ACL that permits access to the new web page is applied to the subscriber record or profile. To reduce the risk, before modifying an existing URL, ensure that the subscriber record includes an IP ACL that permits access to the new URL.

**Note** If the URL contains a question mark (?), press the **Escape (Esc)** key before you enter the ? character. Otherwise, the SmartEdge OS command-line interface (CLI) interprets the ? character as a request for help and does not allow you to complete the URL.

Use the **no** form of this command to delete the URL from the HTTP redirect profile.

### Examples

The following example configures the URL, `www.Redirect.com`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#http-redirect profile Redirect
[local]Redback(config-hr-profile)#url http://www.Redirect.com
```

## Related Commands

`http-redirect profile`  
`http-redirect server`  
`redirect destination local`



# ACL Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS access control list (ACLs).

For information about the tasks and commands used to monitor, troubleshoot, and administer ACLs, see the “ACL Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

SmartEdge OS ACLs are described in the following subsections:

- IP ACLs
- Policy ACLs

**Note** In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

## IP ACLs

IP ACLs are lists of packet filters used to control the type of service that packets should receive. All IP ACLs are defined within a context. The following sections describe IP ACLs:

- IP ACL Applications
- IP ACL Statements
- IP ACL Packet Filtering

### IP ACL Applications

Using an IP ACL, you can filter traffic on traffic card circuits, the Ethernet management port, and subscriber circuits, and administrative traffic, as described in the following subsections:

- Traffic Card Circuits
- Ethernet Management Port
- Subscriber Circuits
- Administrative

#### Traffic Card Circuits

To filter packets in either the inbound or outbound direction on traffic card circuits, you apply an IP ACL to the interface to which the circuits are bound.

#### Ethernet Management Port

To filter packets in either the inbound or outbound direction on the Ethernet management port on the active controller card, you apply an IP ACL to the interface to which the management port is bound. Both inbound and outbound filters are supported.

#### Subscriber Circuits

To filter packets in either the inbound or outbound direction for a subscriber circuit, you apply an IP ACL to the subscriber record, a named subscriber profile, or the default subscriber profile. Both inbound and outbound filters are supported.

#### Administrative

To filter inbound packets that are delivered to the kernel, you apply an IP ACL to a context. These ACLs are independent of the interface and circuit on which they were received.

**Note** To ensure that all inbound packets are filtered before being delivered to the kernel, you must apply an IP ACL to each and every context that you have configured.

### IP ACL Statements

In IP ACL each statement (referred to as a rule) defines the action, either permit or deny, to be taken for a packet if the packet satisfies the rule. A **permit** statement causes any packet matching the criteria to be accepted. A **deny** statement causes any packet matching the criteria to be dropped. A packet that does not match the criteria of the first statement is subjected to the criteria of the second statement, and so on, until the end of the IP ACL is reached; at which point, the packet is dropped due to an implicit **deny any any** statement at the end of every IP ACL.

You can use the optional **seq seq-num** construct with any **permit** or **deny** command to establish a sequence number for the statement you are creating. If you do not use the **seq seq-num** construct, the system automatically assigns sequence numbers to the statements that you enter, in increments of 10.



The first statement that you enter is assigned the sequence number of 10, the second is assigned the number 20, and so on. This allows room to assign intermediate sequence numbers to statements that you might want to add later. The assigned sequence numbers for the various statements are displayed in the output of the **show configuration acl** and **show ip access-list** commands.

If manually assigned sequence numbers leave no room for insertion of additional entries in the IP ACL, you can use the **resequence ip access-list** command (in context configuration mode) to reassign the sequence numbers so that they are in increments of 10. The **no seq seq-num** construct removes an individual statement from the IP ACL.

## IP ACL Packet Filtering

Based on the rules specified in the ACLs associated with the packet, the SmartEdge OS decides whether the packet is forwarded or dropped. Statement criteria include all Internet protocols and can be specified by the protocol numbers established in RFC 1700, *Assigned Numbers*. A subset of these options can also be specified by keyword.

All packets that are permitted or dropped as a result of an IP ACL can be counted and logged (denied packets only) if you enable the count and log functions when you apply an IP ACL. By default, the counting and logging of packets is disabled because these functions have an impact on system performance. We recommend that you only enable logging or counting when required for diagnostic purposes.

The SmartEdge router uses IP ACLs to filter packets in the following order:

1. ACLs applied to interfaces for inbound traffic on traffic card circuits and the Ethernet management port.
2. ACLs applied to subscriber records and profiles for inbound traffic on subscriber circuits.
3. ACLs applied to contexts for administrators (inbound only).
4. ACLs applied to outbound traffic on traffic card circuits and the Ethernet management port.
5. ACLs applied to subscriber records and profiles for outbound traffic on subscriber circuits.

## Policy ACLs

Policy ACLs are lists of packet filters used to control the type of service that packets should receive. A policy ACL, unlike an IP ACL, does not define the action for each rule; instead a policy ACL defines classes of packets and leaves the action for each class to be determined by the policy to which the policy ACL is applied. All policy ACLs are defined within a context. The following subsections describe policy ACLs:

- Policy ACL Applications
- Policy ACL Statements
- Policy ACL Packet Filtering

### Policy ACL Applications

You can apply a policy ACLs to forwarding, Network Address Translation (NAT), or quality of service (QoS) policies to filter packets. When applied to a forward, NAT, or QoS policy, a policy ACL allows different actions to be applied to different classes of packets.

For information about forward policies, see Chapter 9, “Forward Policy Configuration.” For information about NAT policies, see Chapter 10, “NAT Policy Configuration.” For information about QoS policing and metering policies, see Chapter 12, “QoS Rate- and Class-Limiting Configuration.”

### Policy ACL Statements

All statements in a policy ACL are **permit** statements. Each statement defines the criteria for packets to be assigned to a particular class. A packet that does not match the criteria of the first statement is subjected to the criteria of the second statement, and so on, until the end of the policy ACL is reached; at which point, the packet is considered to be assigned to the default class.

You can use the optional **seq seq-num** construct with the **permit** command to establish a sequence number for the statement you are creating. If you do not use the **seq seq-num** construct, the system automatically assigns sequence numbers to the statements that you enter, in increments of 10. The first statement you enter is assigned the sequence number of 10, the second is assigned the number 20, and so on. This allows room to assign intermediate sequence numbers to statements that you might want to add later. The assigned sequence numbers for the various statements are displayed in the output of the **show configuration acl**, **show configuration policy**, and **show policy access-list** commands.

If manually assigned sequence numbers leave no room for insertion of additional entries in the policy ACL, you can use the **resequence policy access-list** command (in context configuration mode) to reassign the sequence numbers so they are in increments of 10. The **no seq seq-num** construct removes an individual statement from the policy ACL.

### Policy ACL Packet Filtering

A policy ACL defines classes of packets through the use of the classification statements. Statement criteria includes all Internet protocols and can be specified by the protocol numbers established in RFC 1700, *Assigned Numbers*. A subset of these options can also be specified by keyword. Based on classification, a forward, NAT, or QoS policy defines the type of action to be performed on the packets in a particular class. All packets that match the criteria can be counted by the statement if you enable the count when you apply a policy ACL. By default, the counting of packets is disabled because this function has an impact on system performance. We recommend that you enable counting only when required for diagnostic purposes.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure ACLs, perform the tasks described in the following sections:

- Configuration Guidelines
- Configure an IP ACL
- Apply an IP ACL
- Enable ACL Counters or Logging for a Subscriber
- Modify IP ACL Conditions in Real Time

- Configure a Policy ACL
- Apply a Policy ACL
- Modify Policy ACL Conditions in Real Time

## Configuration Guidelines

The following guidelines apply to the configuration of IP and policy ACLs:

- The optional construct, **seq** *seq-num*, for **permit** and **deny** commands, allows you assign a sequence number to a particular statement, affecting where it is located within a series of statements in an ACL. If you do not use this construct, the SmartEdge OS automatically assigns sequence numbers in increments of 10. The first statement you enter is assigned the sequence number of 10, the second is assigned the number 20, and so on.
- IP ACL and policy ACL statements that do not reference time range conditions are considered static, because their action (permit/deny) or the resulting class name are constant. They cannot be modified until you modify or remove the statements themselves. However, statements that reference time range conditions are considered dynamic, because their action or the resulting class name depends on the current date and time as defined in the corresponding condition statement.
- ACL conditions re-define the rule's action or the rule's class name based on specified date and time ranges. You can configure any combination of up to seven absolute (one specific time interval) or periodic (recurring time interval) statements in an ACL condition. When an IP ACL rule or a policy ACL rule references an ACL condition, the rule's action (permit/deny) or the rule's class name is determined by the action and the class name defined in the condition.
- ACL conditions are configured with individual IDs to make them unique. The *cond-id* argument used with the **condition** command must match the condition ID specified in the ACL rule.
- An IP or policy ACL can contain multiple entries and the order is significant. Each entry is processed in the order it appears in the configuration file. As soon as an entry matches, the corresponding action is taken and no further processing takes place.

The following filtering rules apply to IP ACLs:

- Each IP ACL has an implicit **deny any any** statement at the end. If a packet does not match any explicit filter statement in the list, it is dropped. Unlike the explicit statements in the ACL, this implicit final statement is not displayed in the output of the **show configuration acl** or **show ip access-list** command (in any mode).
- You apply IP ACLs to interfaces, subscriber records, and contexts. Administrative access control is context-specific. To ensure that all inbound packets are filtered before being delivered to the kernel, you must apply an IP ACL to each and every configured context.
- If you apply an IP ACL to a multibind interface, it does not affect the IP traffic on the subscriber sessions that are bound to that interface; the ACL is applied only to the IP traffic on circuits that are statically bound to the interface using the **bind interface** command (in the circuit's configuration mode).
- If a nonexistent IP ACL is applied to an interface, all packets are forwarded with no filtering.
- If a nonexistent IP ACL is applied to a subscriber record, the subscriber session will not come up; this restriction also applies if a nonexistent ACL is applied to a Remote Authentication Dial-In User Service (RADIUS) attribute.

The following rules apply to policy ACLs:

- If a packet does not match any classifying rule, it is considered to belong to the default class.
- If a nonexistent policy ACL is applied to a NAT policy, a QoS policing or metering policy, or a forward policy, it is ignored and packets are forwarded according to a policy action with no classification.

## Configure an IP ACL

To configure an IP ACL, perform the tasks described in Table 8-1; enter all commands in access control list configuration mode, unless otherwise noted.

**Table 8-1 Configure an IP ACL**

| #  | Task                                                                                             | Root Command                     | Notes                                                                                              |
|----|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------|
| 1. | Create or select an ACL and enter access control list configuration mode.                        | <b>ip access-list</b>            | Enter this command in context configuration mode.                                                  |
| 2. | Optional. Associate a description with an IP ACL.                                                | <b>description</b>               |                                                                                                    |
| 3. | Optional. Create ACL statements using either or both of the following tasks:                     |                                  |                                                                                                    |
|    | Create an ACL statement using <b>permit</b> conditions.                                          | <b>permit</b>                    | There is an implicit <b>deny any any</b> statement at the end of any <b>permit</b> statement.      |
|    | Create an ACL statement using <b>deny</b> conditions.                                            | <b>deny</b>                      |                                                                                                    |
| 4. | Optional. Create an ACL condition using a unique ID and access ACL condition configuration mode. | <b>condition</b>                 | Enter the following commands in ACL condition configuration mode.                                  |
| 5. | Optional. Configure absolute time condition statements.                                          | <b>absolute</b>                  | An absolute time ACL statement redefines an ACL rule's action for only one specific time interval. |
| 6. | Optional. Configure periodic time condition statements.                                          | <b>periodic</b>                  | A periodic time ACL statement redefines the ACL rule action for a recurring time interval.         |
| 7. | Optional. Resequence statements in an IP ACL.                                                    | <b>resequence ip access-list</b> | Enter this command in context configuration mode.                                                  |

## Apply an IP ACL

To apply an IP ACL to packets associated with a context, an interface, or a subscriber record, named profile, or default profile, perform the appropriate task described in Table 8-2.

**Table 8-2 Apply an IP ACL**

| Task                                                                                          | Root Command              | Notes                                                                    |
|-----------------------------------------------------------------------------------------------|---------------------------|--------------------------------------------------------------------------|
| Apply an IP ACL to an interface or to a subscriber record, named profile, or default profile. | <b>ip access-group</b>    | Enter this command in either interface or subscriber configuration mode. |
| Apply an IP ACL to a context.                                                                 | <b>admin-access-group</b> | Enter this command in context configuration mode.                        |

## Enable ACL Counters or Logging for a Subscriber

To enable ACL counters or logging for a subscriber through the subscriber record, the default subscriber profile, or a named subscriber profile, perform the task described in Table 8-3.

**Table 8-3 Enable ACL Counters or Logging for a Subscriber**

| Task                                                                                                                   | Root Command       | Notes                                                |
|------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------|
| Enable ACL counters or logging for a subscriber record, the default subscriber profile, or a named subscriber profile. | <b>access-list</b> | Enter this command in subscriber configuration mode. |

## Modify IP ACL Conditions in Real Time

To modify the action for an IP ACL condition, in real time, without requiring the reconfiguration of the ACL condition statements, perform the task described in Table 8-4.

**Table 8-4 Modify IP ACL Condition Actions in Real Time**

| Task                                                       | Root Command                 | Notes                            |
|------------------------------------------------------------|------------------------------|----------------------------------|
| Modify the action for a condition referenced by an IP ACL. | <b>modify ip access-list</b> | Enter this command in exec mode. |

## Configure a Policy ACL

To configure a policy ACL, perform the tasks described in Table 8-5; enter all commands in access control list configuration mode, unless otherwise noted.

**Table 8-5 Configure a Policy ACL**

| #  | Task                                                                                                   | Root Command                         | Notes                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select a policy ACL and enter access control list configuration mode.                        | <b>policy access-list</b>            | Enter this command in context configuration mode.                                                                        |
| 2. | Optional. Associate a description with a policy ACL.                                                   | <b>description</b>                   |                                                                                                                          |
| 3. | Optional. Create policy ACL statements to allow packets that meet the specified criteria.              | <b>permit</b>                        | Enter this command multiple times to specify multiple classes.                                                           |
| 4. | Optional. Create a policy ACL condition using a unique ID and access ACL condition configuration mode. | <b>condition</b>                     | Enter the following commands in ACL condition configuration mode. You can create up to seven conditions in a policy ACL. |
| 5. | Optional. Configure absolute time condition statements.                                                | <b>absolute</b>                      | An absolute time ACL condition statement applies an ACL rule for only one specific time interval.                        |
| 6. | Optional. Configure periodic time condition statements.                                                | <b>periodic</b>                      | A periodic time ACL statement applies an ACL rule for a recurring time interval.                                         |
| 7. | Optional. Resequence statements in a policy ACL.                                                       | <b>resequence policy access-list</b> | Enter this command in context configuration mode.                                                                        |

# Apply a Policy ACL

To apply a policy ACL to packets associated with a forward, NAT or QoS metering or policing policy and complete the configuration of the policy, perform the tasks described in Chapter 9, “Forward Policy Configuration,” Chapter 10, “NAT Policy Configuration,” and Chapter 12, “QoS Rate- and Class-Limiting Configuration,” respectively.

# Modify Policy ACL Conditions in Real Time

To modify the class name for a policy ACL condition, in real time, without requiring the reconfiguration of the ACL condition statements, perform the task described in Table 8-6.

**Table 8-6    Modify Policy ACL Condition Actions in Real Time**

| Task                                                           | Root Command                     | Notes                            |
|----------------------------------------------------------------|----------------------------------|----------------------------------|
| Modify the action for a class name referenced by a policy ACL. | <b>modify policy access-list</b> | Enter this command in exec mode. |

# Configuration Examples

---

This section provides ACL configuration examples as described in the following subsections:

- Configure an ACL Statement
- Add an ACL Statement
- Resequence ACL Statements
- Configure an Absolute Time Condition Statement
- Configure a Periodic Time Condition Statement
- Configure an IP ACL
- Configure a Policy ACL Associated with a QoS Policing Policy
- Configure a Policy ACL Associated with a Forward Policy
- Configure a Policy ACL Associated with a NAT Policy

# Configure an ACL Statement

The following example configures a policy ACL to prioritize web and voice-over-IP (VOIP) traffic:

```
[ local]Redback(config-ctx)#policy access-list QoSACL-1
[ local]Redback(config-access-list)#permit tcp any any eq 80 class Web
[ local]Redback(config-access-list)#permit udp any any eq 1000 class VOIP
[ local]Redback(config-access-list)#permit any any class default
```

The following example uses a policy ACL to define classes of traffic to be mirrored:

```
[local]Redback(config-ctx)#policy access-list PBR_ACL
[local]Redback(config-access-list)#seq 10 permit tcp any eq www any class WEB
[local]Redback(config-access-list)#seq 20 permit tcp any any eq www class WEB
[local]Redback(config-access-list)#seq 30 permit udp any class UDP
[local]Redback(config-access-list)#seq 40 permit ip any class IP
```

The following example specifies that all IP traffic to destination host 10.25.1.1 is to be denied, and all other traffic on subnet 10.25.1/24 is to be permitted:

```
[local]Redback(config-ctx)#ip access-list protect201
[local]Redback(config-access-list)#deny ip any host 10.25.1.1
[local]Redback(config-access-list)#permit ip any 10.25.1.0 0.0.0.255
```

## Add an ACL Statement

The following example shows how to use the **seq** keyword to modify the existing tc1 ACL, adding a statement between the statements with sequence numbers 20 and 30:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#ip access-list tc1
[local]Redback(config-access-list)#seq 25 deny tcp 10.10.10.4 0.0.0.0 any eq 80
```

The output of the **show configuration acl** command now includes the new statement, with sequence number 25:

```
!
ip access-list tc1
description This is a sample access control list
seq 10 deny ip host 10.10.10.2 host 10.10.20.2
seq 20 deny tcp host 10.10.10.3 any eq www
seq 25 deny tcp host 10.10.10.4 any eq www
seq 30 deny udp host 10.10.10.3 any
seq 40 deny ip host 10.10.10.4 any
seq 50 deny ip host 10.10.10.5 any
seq 60 permit ip any any
```

## Resequence ACL Statements

The following example displays the current sequencing of an IP ACL:

```
[local]Redback#show configuration acl

Building configuration...
!
ip access-list tc1
description This is a sample access control list
seq 10 deny ip host 10.10.10.2 host 10.10.20.2
seq 20 deny tcp host 10.10.10.5 any eq telnet
seq 25 deny tcp host 10.10.10.4 any eq www
```

```
seq 30 deny udp host 10.10.10.3 any
seq 50 deny ip host 10.10.10.5 any
seq 60 permit ip any any
```

The following example resequences the statements in the IP ACL to increments of 10 and displays the new sequence of statements:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#ip access-list tc1
[local]Redback(config-access-list)#resequence access-list tc1
```

```
[local]Redback#show configuration
```

Building configuration...

Current configuration:

context local

ip access-list tc1

description This is a sample access control list

seq 10 deny ip host 10.10.10.2 host 10.10.20.2

seq 20 deny tcp host 10.10.10.5 any eq telnet

seq 30 deny tcp host 10.10.10.4 any eq www

seq 40 deny udp host 10.10.10.3 any

seq 50 deny ip host 10.10.10.5 any

seq 60 permit ip any any

## Configure an Absolute Time Condition Statement

The following example creates an absolute time ACL condition statement for ACL condition 342, which is defined in the IP ACL, `ip-acl-1`. The absolute time ACL condition applies a deny action to all IP ACL statements that reference the ACL condition for the time interval beginning on December 15, 2003 at 9:00 p.m. (21:00) and ending on the same day at 11:00 p.m (23:00).

```
[local]Redback(config-ctx)#ip access-list ip-acl-1
[local]Redback(config-access-list)#condition 342 time-range
[local]Redback(config-acl-condition)#absolute start 2003:12:15:21:00 end
2003:12:15:23:00 deny
```

## Configure a Periodic Time Condition Statement

The following example creates an periodic ACL condition statement for the ACL condition 101, which is referenced by the IP ACL, `ip-acl-2`, such that all packets traveling between 9 a.m. and 5 p.m. (9:00 to 17:00 in 24-hour format) on weekdays are permitted:

```
[local]Redback(config-ctx)#ip access-list ip-acl-2
[local]Redback(config-access-list)#condition 101 time-range
[local]Redback(config-acl-condition)#periodic weekdays 9:00 to 17:00 permit
```



The following example creates a periodic ACL condition statement for the ACL condition 342, which is referenced by the policy ACL `policy_acl_1`, such that all packets traveling every weekday (Monday to Friday) from 9:00 p.m. to 11:00 p.m (9:00 to 23:00 in 24-hour format) are permitted:

```
[local]Redback(config-ctx)#policy access-list policy_acl_1
[local]Redback(config-access-list)#condition 342 time-range
[local]Redback(config-acl-condition)#periodic weekdays 21:00 to 23:00 permit
```

## Configure an IP ACL

The following example creates an IP ACL, `tc1`, and applies the list to an interface, `oc1`:

```
[local]Redback(config-ctx)#ip access-list tc1
[local]Redback(config-access-list)#description This is a sample access control list
[local]Redback(config-access-list)#deny ip 10.10.10.2 0.0.0.0 10.10.20.2 0.0.0.0
[local]Redback(config-access-list)#deny tcp 10.10.10.3 0.0.0.0 any eq 80
[local]Redback(config-access-list)#deny udp 10.10.10.3 0.0.0.0 any
[local]Redback(config-access-list)#deny ip 10.10.10.4 0.0.0.0 any
[local]Redback(config-access-list)#deny ip 10.10.10.5 0.0.0.0 any
[local]Redback(config-access-list)#permit ip any any
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#interface oc1
[local]Redback(config-if)#ip access-group tc1 in log
```

## Configure a Policy ACL Associated with a QoS Policing Policy

The following example applies the conditions set by the ACL qos created for any circuit to which the QoS policing policy, `class`, is attached. Packets are classified into three classes: `web`, `voice over IP (VOIP)`, and `default`.

```
[local]Redback(config-ctx)#policy access-list qos
[local]Redback(config-access-list)#permit tcp any any eq 80 class Web
[local]Redback(config-access-list)#permit udp any any eq 1000 class VOIP
[local]Redback(config-access-list)#permit any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#qos policy class policing
[local]Redback(config-policy-policing)#access-group qos local
[local]Redback(config-policy-acl)#class web
[local]Redback(config-policy-acl-class)#rate 5000 burst 1000
[local]Redback(config-policy-class-rate)#conform mark dscp AF11
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class voip
[local]Redback(config-policy-acl-class)#mark dscp ef
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class default
[local]Redback(config-policy-acl-class)#mark dscp df
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#exit
[local]Redback(config-policy-policing)#exit
```

```
[local]Redback(config)#port ethernet 3/0
[local]Redback(config-port)#bind interface eth1 local
[local]Redback(config-port)#qos policy policing class
```

Web traffic that conforms to the traffic rate of 5000 kbps is marked with a Differentiated Services Code Point (DSCP) value of AF11. Web traffic exceeding that rate is dropped by default. Packets classified as VOIP are prioritized over both web and default traffic through the DSCP setting of ef, or expedited forwarding. Packets classified as default are set to the DSCP value of df, or default.

## Configure a Policy ACL Associated with a Forward Policy

The policy ACL and forward policy configuration is as follows:

```
[local]Redback(config-ctx)#policy access-list PBR_Drop_ACL
[local]Redback(config-access-list)#seq 10 permit icmp host 51.1.1.2 class ICMP
[local]Redback(config-access-list)#seq 20 permit pim any class PIM
[local]Redback(config-access-list)#exit
[local]Redback(config-access-list)#exit
[local]Redback(config)#forward policy DropPolicy
[local]Redback(config-policy-frwd)#access-group PBR_Drop_ACL local
[local]Redback(config-policy-acl)#class ICMP
[local]Redback(config-policy-acl-class)#drop
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class PIM
[local]Redback(config-policy-acl-class)#drop
```

The following configuration applies the forward policy to the incoming\_traffic interface:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface incoming_traffic local
[local]Redback(config-port)#forward policy DropPolicy in
[local]Redback(config-port)#exit
```

## Configure a Policy ACL Associated with a NAT Policy

The following example creates a policy ACL and applies it to a NAT policy with dynamic translations in which all packets except those classified as CLASS3 are ignored (that is, the NAT policy is not applied to them). All source IP addresses for incoming packets classified as CLASS3 are translated using IP addresses from the pool\_dyn pool.

```
!Create the NAT pool
[local]Redback(config-ctx)#ip nat pool pool_dyn
[local]Redback(config-nat-pool)#address 11.11.11.0/24
[local]Redback(config-nat-pool)#exit
!Create the policy ACL
[local]Redback(config-ctx)#policy access-list NAT-ACL
[local]Redback(config-access-list)#seq 10 permit ip 10.10.10.0 0.0.0.255 class CLASS3
[local]Redback(config-access-list)#exit
```

```
!Create the NAT policy and apply the policy ACL
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-nat-pool)#ignore
[local]Redback(config-nat-pool)#access-group NAT-ACL
[local]Redback(config-policy-acl)#class CLASS3
[local]Redback(config-policy-acl-class)#pool pool_dyn local
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure ACLs. The commands are presented in alphabetical order.

|                           |                                      |
|---------------------------|--------------------------------------|
| <b>absolute</b>           | <b>ip access-list</b>                |
| <b>access-group</b>       | <b>modify ip access-list</b>         |
| <b>access-list</b>        | <b>modify policy access-list</b>     |
| <b>admin-access-group</b> | <b>periodic</b>                      |
| <b>class</b>              | <b>permit</b>                        |
| <b>condition</b>          | <b>policy access-list</b>            |
| <b>deny</b>               | <b>resequence ip access-list</b>     |
| <b>description</b>        | <b>resequence policy access-list</b> |
| <b>ip access-group</b>    |                                      |

## absolute

**absolute start** *yyyy:mm:dd:hh:mm* **end** *yyyy:mm:dd:hh:mm* [:ss] { **permit** | **deny** } | **class** *class-name* }

**no absolute start** *yyyy:mm:dd:hh:mm* **end** *yyyy:mm:dd:hh:mm*

### Purpose

Creates an absolute time access control list (ACL) condition statement.

### Command Mode

ACL condition configuration

### Syntax Description

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>start</b> <i>yyyy:mm:dd:hh:mm</i> [:ss] | Date and time to start the ACL condition. Arguments are defined as follows: <ul style="list-style-type: none"> <li><i>yyyy</i>—Year.</li> <li><i>mm</i>—Month. The range of values is 1 to 12.</li> <li><i>dd</i>—Day The range of values is 1 to 31.</li> <li><i>hh</i>—Hour in 24-hour format. The range of values is 0 to 23.</li> <li><i>mm</i>—Minutes. The range of values is 0 to 59.</li> <li><i>ss</i>—Seconds. Optional. The range of values is 0 to 60.</li> </ul> |
| <b>end</b> <i>yyyy:mm:dd:hh:mm</i> [:ss]   | Date and time to stop the ACL condition. Arguments are defined as follows: <ul style="list-style-type: none"> <li><i>yyyy</i>—Year.</li> <li><i>mm</i>—Month. The range of values is 1 to 12.</li> <li><i>dd</i>—Day. The range of values is 1 to 31.</li> <li><i>hh</i>—Hour 24-hour format. The range of values is 0 to 23.</li> <li><i>mm</i>—Minutes. The range of values is 0 to 59.</li> <li><i>ss</i>—Seconds. Optional. The range of values is 0 to 60.</li> </ul>    |
| <b>permit</b>                              | Applies a permit action to packets processed during the specified time range.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>deny</b>                                | Applies a deny action to packets processed during the specified time range. Used only with IP ACLs.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>class</b> <i>class-name</i>             | Name of the class assigned to policy ACL statements that reference the ACL condition. Used only with policy ACLs.                                                                                                                                                                                                                                                                                                                                                             |

### Default

No ACL condition statements are configured.

## Usage Guidelines

Use the **absolute** command to create an absolute time ACL condition statement that, when referenced in an IP ACL statement, permits or denies packets, based on specific date and time ranges. Use this command to create an absolute time ACL conditional statement that, when referenced in a policy ACL statement, assigns a class name to packets.

Use the **no** form of this command to delete the absolute time ACL condition statement.

## Examples

The following example creates an absolute time ACL condition statement for the ACL condition 500, which is referenced in the policy ACL, `policy-acl-forward`. The absolute time ACL condition applies the `Bar003` class name to all policy ACL statements that reference the ACL condition during the time interval beginning on December 15, 2003 at 9:00 p.m. (21:00) and ending on the same day at 11:00 p.m. (23:00).

```
[local]Redback(config-ctx)#policy access-list policy-acl-forward
[local]Redback(config-access-list)#condition 500 time-range
[local]Redback(config-acl-condition)#absolute start 2003:12:15:21:00 end
2003:12:15:23:00 class Bar003
```

## Related Commands

- condition**
- deny**
- ip access-list**
- periodic**
- permit**
- policy access-list**

## access-group

**access-group** *acl-name ctx-name*

**no access-group** *acl-name ctx-name*

### Purpose

Applies a policy access control list (ACL) to a Network Address Translation (NAT) policy, to a quality of service (QoS) metering or policing policy, or to a forward policy, and enters policy ACL configuration mode.

### Command Mode

forward policy configuration  
metering policy configuration  
NAT policy configuration  
policing policy configuration

### Syntax Description

|                 |                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------|
| <i>acl-name</i> | Name of the policy ACL created using the <b>policy access-list</b> command (in context configuration mode). |
| <i>ctx-name</i> | Name of the context in which the policy ACL was created.                                                    |

### Default

None

### Usage Guidelines

Use the **access-group** command to apply a policy ACL to a NAT policy, to a QoS policing or metering policy, or to a forward policy, and enter policy ACL configuration mode.

Use the **no** form of this command to disassociate the access group from the specified policy.

### Examples

The following example applies the QoS policing policy, **GE-in**, as specified by the rules in the policy ACL, **myacl**. The **myacl** access group has one class, **voip**, and packets in this class are marked with the Differentiated Service Code Point (DSCP) code, **af13**.

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl local
[local]Redback(config-policy-acl)#class voip
[local]Redback(config-policy-acl-class)#mark dscp af13
```

The following example applies the forward policy, `RedirectPolicy`, as specified by the rules in the policy ACL `PBR_Redirect_ACL`. The `PBR_Redirect_ACL` access group has one class, `Web`, and packets in this class are redirected to the next hop in the route at IP address, `100.1.1.0`.

```
[local]Redback(config)#forward policy RedirectPolicy
[local]Redback(config-policy-frwd)#access-group PBR_Redirect_ACL local
[local]Redback(config-policy-acl)#class Web
[local]Redback(config-policy-acl-class)#redirect destination next-hop 100.1.1.0
```

## Related Commands

- `access-group`
- `class`
- `conform mark dscp`
- `policy access-list`

## access-list

**access-list** {**count** *counter-type* | **log ip**}

**no access-list** {**count** *counter-type* | **log ip**}

### Purpose

Enables access control list (ACL) counters or logging for the default subscriber profile, this named subscriber profile, or this named subscriber record.

### Command Mode

subscriber configuration

### Syntax Description

|                                  |                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>count</b> <i>counter-type</i> | ACL counter type, according to one of the following keywords: <ul style="list-style-type: none"> <li>• <b>ip</b>—Specifies IP ACL counters.</li> <li>• <b>policy</b>—Specifies policy ACL counters.</li> </ul> |
| <b>log ip</b>                    | Enables logging of dropped counters for IP ACL.                                                                                                                                                                |

### Default

ACL counters are not enabled for any subscriber records or profiles.

### Usage Guidelines

Use the **access-list** command to enable ACL counters or logging for the default subscriber profile, this named subscriber profile, or this named subscriber record.

Use the **no** form of this command to disable ACL counters for the default subscriber profile, this named subscriber profile, or this named subscriber record.

### Examples

The following example enables ACL IP counters for the default subscriber profile:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#access-list count ip
```

### Related Commands

None



## admin-access-group

**admin-access-group** *acl-name* **in** [**count**] [**log**]

**no admin-access-group** *acl-name* **in** [**count**] [**log**]

### Purpose

Applies access control to all inbound packets delivered to the kernel, regardless of the interface through which packets are received.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                 |
|-----------------|-----------------------------------------------------------------|
| <i>acl-name</i> | Name of the IP ACL being applied.                               |
| <b>in</b>       | Specifies that the IP ACL is to be applied to incoming packets. |
| <b>count</b>    | Optional. Enables ACL packet counting.                          |
| <b>log</b>      | Optional. Enables ACL packet logging.                           |

### Default

No administrative access control is applied.

### Usage Guidelines

Use the **admin-access-group** command to apply access control to all inbound packets delivered to the kernel, regardless of the interface through which they are received. This is referred to as administrative access control and used with IP ACLs only.



**Caution** Risk of security breach. Administrative access control is context-specific. To ensure that all inbound packets are filtered before being delivered to the kernel, you must apply an administrative ACL to each and every context that is configured.

When you use the **count** keyword, the system keeps track of the number of packet matches that occur. When you use the **log** keyword, the system keeps track of the number of packets that were denied as a result of the ACL. Count and log information is displayed in the output of the **show access-group** command.



**Caution** Risk of system performance impact. By default, counting and logging of packets is disabled because these functions have an impact on system performance. To reduce the risk, we recommend that you only enable logging or counting when required for diagnostic purposes.

Use the **no** form of this command to remove the application of an ACL to traffic inbound to the kernel.

### Examples

The following example applies the `test_2` ACL to traffic inbound to the kernel for the `local` context:

```
[local]Redback(config-ctx)#admin-access-group test_2 in count log
```

### Related Commands

**ip access-list**

## class

**class** *class-name*  
**no class** *class-name*

### Purpose

Creates a class and accesses policy access control list (ACL) class configuration mode.

### Command Mode

policy ACL configuration

### Syntax Description

|                   |                                                                                                                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>class-name</i> | Class name. This argument must match the name specified in the <i>class-name</i> argument specified by a <b>permit</b> command (in access control list configuration mode) for this policy ACL. |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

None

### Usage Guidelines

Use the **class** command to create a class and access policy ACL class configuration mode. This command allows a Network Address Translation (NAT) policy, a quality of service (QoS) policing or metering policy, or a forward policy to apply a different action to different sets (classes) of packets as determined by the policy ACL.

The *class-name* argument must match the *class-name* argument at the end of the **permit** command construct. To access the **permit** command, enter the **policy access-list** command (in context configuration mode).

Use the **no** form of this command to remove the specified class.

### Examples

The following example applies the QoS policing policies determined by the policy ACL, QoSACL-1, to the class, **Web**, and prioritizes incoming traffic packets using a DSCP value of DF. For the **VOIP** class, incoming traffic packets are prioritized with a DSCP value of AF11.

```
[local]Redback(config-policy-policing)#access-group QoSACL-1
[local]Redback(config-policy-acl)#class Web
[local]Redback(config-policy-acl-class)#rate 6000 burst 3000
[local]Redback(config-policy-class-rate)#exceed mark dscp DF
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class VOIP
[local]Redback(config-policy-acl-class)#mark dscp AF11
```

## Command Descriptions

---

The following example applies the forward policy determined by the policy ACL, PBR\_ACL, to the class Web and mirrors all traffic to the mirror output destination, WebTraffic:

```
[local]Redback(config)#forward policy MirrorPolicy
[local]Redback(config-policy-frwd)#access-group PBR_ACL local
[local]Redback(config-policy-acl)#class Web
[local]Redback(config-policy-acl-class)#mirror destination WebTraffic all
```

## Related Commands

- access-group**
- permit**
- policy access-list**

## condition

**condition** *cond-id* **time-range**

**no condition** *cond-id*

### Purpose

Creates an access control list (ACL) condition and enters ACL condition configuration mode:

### Command Mode

access control list configuration

### Syntax Description

|                   |                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------|
| <i>cond-id</i>    | Condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295. |
| <b>time-range</b> | Specifies a time range condition type.                                                      |

### Default

None

### Usage Guidelines

Use the **condition** command to create an ACL condition, and to enter ACL condition configuration mode.

An ACL condition is comprised of up to seven ACL condition statements (using any combination of the **absolute** and **periodic** commands in ACL condition configuration mode). When an ACL statement references an ACL condition, the ACL condition statements apply those time-dependent rules to the referencing IP ACL or policy ACL statement.

Use the **no** form of this command to delete an ACL condition.

### Examples

The following example creates the time range condition identified as 342 for the IP ACL, protect, and enters ACL condition configuration mode:

```
[local]Redback(config-ctx)#ip access-list protect
[local]Redback(config-access-list)#condition 342 time-range
[local]Redback(config-acl-condition)#
```

The following example creates the time range condition identified as 10.1.2.3 for the policy ACL, control, and enters ACL condition configuration mode:

```
[local]Redback(config-ctx)#policy access-list control
[local]Redback(config-access-list)#condition 10.1.2.3 time-range
[local]Redback(config-acl-condition)#
```

### Related Commands

- `absolute`
- `ip access-list`
- `periodic`
- `policy access-list`

## deny

```
[seq seq-num] deny [protocol] {src src-wildcard | any | host src} [cond port | range port end-port]
[dest dest-wildcard | any | host dest] [cond port | range port end-port] [length {cond length |
range length end-length}] [icmp-type icmp-type [icmp-code icmp-code]] [igmp-type igmp-type]
[dscp eq dscp-value] [established] [precedence prec-value] [tos tos-value] [condition cond-id]
no seq seq-num
```

### Purpose

Creates an IP access control list (ACL) statement that denies packets that meet the specified criteria.

### Command Mode

access control list configuration

### Syntax Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>seq</b> <i>seq-num</i> | Optional. Sequence number for the statement. The range of values is 1 to 4,294,967,295.                                                                                                                                                                                                                                                                                                                     |
| <i>protocol</i>           | Optional. Number indicating a protocol as specified in RFC 1700, <i>Assigned Numbers</i> . The range of values is 0 to 255 or one of the keywords listed in Table 8-7.                                                                                                                                                                                                                                      |
| <i>src</i>                | Source address to be included in the permit or deny criteria. An IP address in the form <i>A.B.C.D</i> .                                                                                                                                                                                                                                                                                                    |
| <i>src-wildcard</i>       | Indication of which bits in the <i>src</i> argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the <i>src-wildcard</i> argument mean that the corresponding bits in the <i>src</i> argument must match; one-bits in the <i>src-wildcard</i> argument mean that the corresponding bits in the <i>src</i> argument are ignored. |
| <b>any</b>                | Specifies a completely wildcarded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.                                                                                                                                                                                           |
| <b>host</b> <i>src</i>    | Address of a single-host source with no wild-carded address bits. The <b>host source</b> construct is identical to the <i>src src-wildcard</i> construct if the wildcard address indicates that all bits should be matched (0.0.0.0).                                                                                                                                                                       |
| <i>cond</i>               | Optional. Matching condition for the <i>port</i> or <i>length</i> argument, according to one of the keywords listed in Table 8-8.                                                                                                                                                                                                                                                                           |
| <i>port</i>               | Optional. TCP or UDP source or destination port. This construct is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 8-9 and Table 8-10.                                                                                                                                                                                |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>range</b> <i>port end-port</i> | Optional. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. This construct is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 8-9 and Table 8-10.                                               |
| <b>dest</b>                       | Optional. Destination address to be included in the permit or deny criteria. An IP address in the form <i>A.B.C.D</i> .                                                                                                                                                                                                                                                                                          |
| <b>dest-wildcard</b>              | Indication of which bits in the <i>dest</i> argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the <i>dest-wildcard</i> argument mean that the corresponding bits in the <i>dest</i> argument must match; one-bits in the <i>dest-wildcard</i> argument mean that the corresponding bits in the <i>dest</i> argument are ignored. |
| <b>host dest</b>                  | Address of a single-host destination with no wildcarded address bits. The <b>host dest</b> construct is identical to the <i>dest dest-wildcard</i> construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).                                                                                                                                                                       |
| <b>length</b>                     | Optional. Indicates that packet length is to be used as a filter. The packet length is the length of the network-layer packet, beginning with the IP header. This is true irrespective of the specified protocol.                                                                                                                                                                                                |
| <b>length</b>                     | Packet length. The range of values is 20 to 65,535.                                                                                                                                                                                                                                                                                                                                                              |
| <b>range length end-length</b>    | Packets that fall into the range of specified lengths. Each value ( <i>length</i> and <i>end-length</i> ) can be from 20 to 65,535.                                                                                                                                                                                                                                                                              |
| <b>icmp-type icmp-type</b>        | Optional. Type of ICMP packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 8-11. This argument is only available if you specify <b>icmp</b> for the <i>protocol</i> argument.                                                                                                                                                                                           |
| <b>icmp-code icmp-code</b>        | Optional if you use the <b>icmp-type icmp-type</b> construct. A particular ICMP message code to be matched. The range of values is 0 to 255. This argument is only accepted if you specified <b>icmp</b> for the <i>protocol</i> argument.                                                                                                                                                                       |
| <b>igmp-type igmp-type</b>        | Optional. Type of IGMP packet to be matched. This argument is only accepted if you specified <b>igmp</b> as the <i>protocol</i> argument. The range of values is 0 to 15 or one of the keywords listed in Table 8-12.                                                                                                                                                                                            |
| <b>dscp eq dscp-value</b>         | Optional. Packet's Differentiated Services Code Point (DSCP) value must be equal to the value specified in the <i>dscp-value</i> argument to match the criteria. The range of values is 0 to 63 or one of the keywords listed in Table 8-13.                                                                                                                                                                     |
| <b>established</b>                | Optional. Specifies that only established connections are to be matched. This keyword is only available if you specify <b>tcp</b> for the <i>protocol</i> argument.                                                                                                                                                                                                                                              |
| <b>precedence prec-value</b>      | Optional. Precedence value of packets to be considered a match. The range of values is 0 to 7, 7 being the highest precedence, or one of the keywords listed in Table 8-14.                                                                                                                                                                                                                                      |



|                                 |                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>tos</b> <i>tos-value</i>     | Optional. Type of service (ToS) to be considered a match. The range of values is 0 to 15 or one of the keywords listed in Table 8-15. |
| <b>condition</b> <i>cond-id</i> | Optional. ACL condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295.                             |

## Default

None

## Usage Guidelines

Use the **deny** command to create the IP ACL statement to deny packets that meet the specified criteria.

The *cond port* and *cond length* constructs are mutually exclusive with the **range** construct for the *port* and *length* arguments, respectively.

Use the **no** form of this command to delete the statement with the specified sequence number from the ACL.

Table 8-7 lists the valid keyword substitutions for the *protocol* argument.

**Table 8-7 Valid Keyword Substitutions for the *protocol* Argument**

| Keyword | Definition                                    |
|---------|-----------------------------------------------|
| ahp     | Specifies Authentication Header Protocol.     |
| esp     | Specifies Encapsulation Security Payload.     |
| gre     | Specifies Generic Routing Encapsulation.      |
| host    | Specifies host source address.                |
| icmp    | Specifies Internet Control Message Protocol.  |
| igmp    | Specifies Internet Group Management Protocol. |
| ip      | Specifies any IP protocol.                    |
| ipinip  | Specifies IP-in-IP tunneling.                 |
| ospf    | Specifies Open Shortest Path First.           |
| pcp     | Specifies Payload Compression Protocol.       |
| pim     | Specifies Protocol Independent Multicast.     |
| tcp     | Specifies Transmission Control Protocol.      |
| udp     | Specifies User Datagram Protocol.             |

Table 8-8 lists the valid keyword substitutions for the *cond* argument.

**Table 8-8 Valid Keyword Substitutions for the *cond* Argument**

| Keyword | Description                                                                                              |
|---------|----------------------------------------------------------------------------------------------------------|
| eq      | Specifies that values must be equal to those specified by the <i>port</i> or <i>length</i> argument.     |
| gt      | Specifies that values must be greater than those specified by the <i>port</i> or <i>length</i> argument. |

**Table 8-8 Valid Keyword Substitutions for the *cond* Argument (continued)**

| Keyword    | Description                                                                                              |
|------------|----------------------------------------------------------------------------------------------------------|
| <b>lt</b>  | Specifies that values must be less than those specified by the <i>port</i> or <i>length</i> argument.    |
| <b>neq</b> | Specifies that values must not be equal to those specified by the <i>port</i> or <i>length</i> argument. |

Table 8-9 lists the valid keyword substitutions for the *port* argument when it is used to specify a TCP port.

**Table 8-9 Valid Keyword Substitutions for the *port* Argument (TCP Port)**

| Keyword            | Definition                                   | Corresponding Port Number |
|--------------------|----------------------------------------------|---------------------------|
| <b>bgp</b>         | Border Gateway Protocol (BGP)                | 179                       |
| <b>chargen</b>     | Character generator                          | 19                        |
| <b>cmd</b>         | Remote commands (rcmd)                       | 514                       |
| <b>daytime</b>     | Daytime                                      | 13                        |
| <b>discard</b>     | Discard                                      | 9                         |
| <b>domain</b>      | Domain Name System                           | 53                        |
| <b>echo</b>        | Echo                                         | 7                         |
| <b>exec</b>        | Exec (rsh)                                   | 512                       |
| <b>finger</b>      | Finger                                       | 79                        |
| <b>ftp</b>         | File Transfer Protocol                       | 21                        |
| <b>ftp-data</b>    | FTP data connections (used infrequently)     | 20                        |
| <b>gopher</b>      | Gopher                                       | 70                        |
| <b>hostname</b>    | Network interface card (NIC) hostname server | 101                       |
| <b>ident</b>       | Identification protocol                      | 113                       |
| <b>irc</b>         | Internet Relay Chat                          | 194                       |
| <b>klogin</b>      | Kerberos login                               | 543                       |
| <b>kshell</b>      | Kerberos Shell                               | 544                       |
| <b>login</b>       | Login (rlogin)                               | 513                       |
| <b>lpd</b>         | Printer service                              | 515                       |
| <b>nntp</b>        | Network News Transport Protocol              | 119                       |
| <b>pim-auto-rp</b> | Protocol Independent Multicast Auto-RP       | 496                       |
| <b>pop2</b>        | Post Office Protocol Version 2               | 109                       |
| <b>pop3</b>        | Post Office Protocol Version 3               | 110                       |
| <b>shell</b>       | Remote command shell                         | 514                       |
| <b>smtp</b>        | Simple Mail Transport Protocol               | 25                        |
| <b>ssh</b>         | Secure Shell                                 | 22                        |
| <b>sunrpc</b>      | Sun Remote Procedure Call                    | 111                       |

**Table 8-9 Valid Keyword Substitutions for the *port* Argument (TCP Port) (continued)**

| Keyword       | Definition                                       | Corresponding Port Number |
|---------------|--------------------------------------------------|---------------------------|
| <b>syslog</b> | System logger                                    | 514                       |
| <b>tacacs</b> | Terminal Access Controller Access Control System | 49                        |
| <b>talk</b>   | Talk                                             | 517                       |
| <b>telnet</b> | Telnet                                           | 23                        |
| <b>time</b>   | Time                                             | 37                        |
| <b>uucp</b>   | Unix-to-Unix Copy Program                        | 540                       |
| <b>whois</b>  | Nickname                                         | 43                        |
| <b>www</b>    | World Wide Web (HTTP)                            | 80                        |

Table 8-10 lists the valid keyword substitutions for the *port* argument when it is used to specify a UDP port.

**Table 8-10 Valid Keyword Substitutions for the *port* Argument (UDP Port)**

| Keyword            | Definition                                                         | Corresponding Port Number |
|--------------------|--------------------------------------------------------------------|---------------------------|
| <b>biff</b>        | Biff (Mail Notification, Comsat)                                   | 512                       |
| <b>bootpc</b>      | Bootstrap Protocol client                                          | 68                        |
| <b>bootps</b>      | Bootstrap Protocol server                                          | 67                        |
| <b>discard</b>     | Discard                                                            | 9                         |
| <b>dnsix</b>       | DNSIX Security Protocol Auditing                                   | 195                       |
| <b>domain</b>      | Domain Name System                                                 | 53                        |
| <b>echo</b>        | Echo                                                               | 7                         |
| <b>isakmp</b>      | Internet Security Association and Key Management Protocol (ISAKMP) | 500                       |
| <b>mobile-ip</b>   | Mobile IP Registration                                             | 434                       |
| <b>nameserver</b>  | IEN116 Name Service (obsolete)                                     | 42                        |
| <b>netbios-dgm</b> | NetBIOS Datagram Service                                           | 138                       |
| <b>netbios-ns</b>  | NetBIOS Name Service                                               | 137                       |
| <b>netbios-ss</b>  | NetBIOS Session Service                                            | 139                       |
| <b>ntp</b>         | Network Time Protocol                                              | 123                       |
| <b>pim-auto-rp</b> | Protocol Independent Multicast Auto-RP                             | 496                       |
| <b>rip</b>         | Router Information Protocol (router, in.routed)                    | 520                       |
| <b>snmp</b>        | Simple Network Management Protocol                                 | 161                       |
| <b>snmptrap</b>    | SNMP Traps                                                         | 162                       |
| <b>sunrpc</b>      | Sun Remote Procedure Call                                          | 111                       |
| <b>syslog</b>      | System logger                                                      | 514                       |

**Table 8-10 Valid Keyword Substitutions for the *port* Argument (UDP Port) (continued)**

| Keyword       | Definition                                       | Corresponding Port Number |
|---------------|--------------------------------------------------|---------------------------|
| <b>tacacs</b> | Terminal Access Controller Access Control System | 49                        |
| <b>talk</b>   | Talk                                             | 517                       |
| <b>tftp</b>   | Trivial File Transfer Protocol                   | 69                        |
| <b>time</b>   | Time                                             | 37                        |
| <b>who</b>    | Who Service (rwho)                               | 513                       |
| <b>xdmcp</b>  | X Display Manager Control Protocol               | 177                       |

Table 8-11 lists the valid keyword substitutions for the *icmp-type* argument.

**Table 8-11 Valid Keyword Substitutions for the *icmp-type* Argument**

| Keyword                            | Description                                               |
|------------------------------------|-----------------------------------------------------------|
| <b>administratively-prohibited</b> | Administratively prohibited                               |
| <b>alternate-address</b>           | Alternate address                                         |
| <b>conversion-error</b>            | Datagram conversion                                       |
| <b>dod-host-prohibited</b>         | Host prohibited                                           |
| <b>dod-net-prohibited</b>          | Net prohibited                                            |
| <b>echo</b>                        | Echo (ping)                                               |
| <b>echo-reply</b>                  | Echo reply                                                |
| <b>general-parameter-problem</b>   | General parameter problem                                 |
| <b>host-isolated</b>               | Host isolated                                             |
| <b>host-precedence-unreachable</b> | Host unreachable for precedence                           |
| <b>host-redirect</b>               | Host redirect                                             |
| <b>host-tos-redirect</b>           | Host redirect for ToS                                     |
| <b>host-tos-unreachable</b>        | Host unreachable for ToS                                  |
| <b>host-unknown</b>                | Host unknown                                              |
| <b>host-unreachable</b>            | Host unreachable                                          |
| <b>information-reply</b>           | Information replies                                       |
| <b>information-request</b>         | Information requests                                      |
| <b>log</b>                         | Log matches against this entry                            |
| <b>log-input</b>                   | Log matches against this entry, including input interface |
| <b>mask-reply</b>                  | Mask replies                                              |
| <b>mask-request</b>                | Mask requests                                             |
| <b>mobile-redirect</b>             | Mobile host redirects                                     |
| <b>net-redirect</b>                | Network redirect                                          |

**Table 8-11 Valid Keyword Substitutions for the *icmp-type* Argument** (*continued*)

| Keyword                       | Description                                          |
|-------------------------------|------------------------------------------------------|
| <b>net-tos-redirect</b>       | Network redirect for ToS                             |
| <b>net-tos-unreachable</b>    | Network unreachable for ToS                          |
| <b>net-unreachable</b>        | Network unreachable                                  |
| <b>network-unknown</b>        | Network unknown                                      |
| <b>no-room-for-option</b>     | Parameter required but no room                       |
| <b>option-missing</b>         | Parameter required but not present                   |
| <b>packet-too-big</b>         | Fragmentation needed and DF set                      |
| <b>parameter-problem</b>      | All parameter problems                               |
| <b>port-unreachable</b>       | Port unreachable                                     |
| <b>precedence</b>             | Match packets with given precedence value            |
| <b>precedence-unreachable</b> | Precedence cutoff                                    |
| <b>protocol-unreachable</b>   | Protocol unreachable                                 |
| <b>reassembly-timeout</b>     | Reassembly timeout                                   |
| <b>redirect</b>               | All redirects                                        |
| <b>router-advertisement</b>   | Router discovery advertisement                       |
| <b>router-solicitation</b>    | Router discovery solicitation                        |
| <b>source-quench</b>          | Source quenches                                      |
| <b>source-route-failed</b>    | Source route failed                                  |
| <b>time-exceeded</b>          | All time exceeded messages                           |
| <b>time-range</b>             | Specify a time-range                                 |
| <b>timestamp-reply</b>        | Timestamp replies                                    |
| <b>timestamp-request</b>      | Timestamp requests                                   |
| <b>tos</b>                    | Match packets with given type of service (ToS) value |
| <b>traceroute</b>             | Traceroute                                           |
| <b>ttl-exceeded</b>           | TTL Exceeded                                         |
| <b>unreachable</b>            | All unreachables                                     |

Table 8-12 lists the valid keyword substitutions for the *igmp-type* argument.

**Table 8-12 Valid Keyword Substitutions for the *igmp-type* Argument**

| Keyword            | Description                                           |
|--------------------|-------------------------------------------------------|
| <b>dvmrp</b>       | Specifies Distance-Vector Multicast Routing Protocol. |
| <b>Host-query</b>  | Specifies host query.                                 |
| <b>Host-report</b> | Specifies host report.                                |
| <b>pim</b>         | Specifies Protocol Independent Multicast.             |

Table 8-13 lists the valid keyword substitutions for the *dscp-value* argument.

**Table 8-13 Valid Keyword Substitutions for the *dscp-value* Argument**

| Keyword     | Definition                                   |
|-------------|----------------------------------------------|
| <b>af11</b> | Assured Forwarding—Class 1/Drop precedence 1 |
| <b>af12</b> | Assured Forwarding—Class 1/Drop precedence 2 |
| <b>af13</b> | Assured Forwarding—Class 1/Drop precedence 3 |
| <b>af21</b> | Assured Forwarding—Class 2/Drop precedence 1 |
| <b>af22</b> | Assured Forwarding—Class 2/Drop precedence 2 |
| <b>af23</b> | Assured Forwarding—Class 2/Drop precedence 3 |
| <b>af31</b> | Assured Forwarding—Class 3/Drop precedence 1 |
| <b>af32</b> | Assured Forwarding—Class 3/Drop precedence 2 |
| <b>af33</b> | Assured Forwarding—Class 3/Drop precedence 3 |
| <b>af41</b> | Assured Forwarding—Class 4/Drop precedence 1 |
| <b>af42</b> | Assured Forwarding—Class 4/Drop precedence 2 |
| <b>af43</b> | Assured Forwarding—Class 4/Drop precedence 3 |
| <b>cs0</b>  | Class Selector 0                             |
| <b>cs1</b>  | Class Selector 1                             |
| <b>cs2</b>  | Class Selector 2                             |
| <b>cs3</b>  | Class Selector 3                             |
| <b>cs4</b>  | Class Selector 4                             |
| <b>cs5</b>  | Class Selector 5                             |
| <b>cs6</b>  | Class Selector 6                             |
| <b>cs7</b>  | Class Selector 7                             |
| <b>df</b>   | Default Forwarding (same as cs0)             |
| <b>ef</b>   | Expedited Forwarding                         |

Table 8-14 lists the valid keyword substitutions for the *prec-value* argument.

**Table 8-14 Valid Keyword Substitutions for the *prec-value* Argument**

| Keyword               | Description                                            |
|-----------------------|--------------------------------------------------------|
| <b>tine</b>           | Specifies routine precedence (value = 0).              |
| <b>priority</b>       | Specifies priority precedence (value = 1).             |
| <b>immediate</b>      | Specifies immediate precedence (value = 2).            |
| <b>flash</b>          | Specifies flash precedence (value = 3).                |
| <b>flash-override</b> | Specifies flash override precedence (value = 4).       |
| <b>critical</b>       | Specifies critical precedence (value = 5).             |
| <b>internet</b>       | Specifies internetwork control precedence (value = 6). |
| <b>network</b>        | Specifies network control precedence (value = 7).      |

Table 8-15 lists the valid keyword substitutions for the *tos-value* argument.

**Table 8-15 Valid Keyword Substitutions for the *tos-value* Argument**

| Keyword                  | Description                                      |
|--------------------------|--------------------------------------------------|
| <b>max-reliability</b>   | Specifies maximum reliable ToS (value = 2).      |
| <b>max-throughput</b>    | Specifies maximum throughput ToS (value = 4).    |
| <b>min-delay</b>         | Specifies minimum delay ToS (value = 8).         |
| <b>min-monetary-cost</b> | Specifies minimum monetary cost ToS (value = 1). |
| <b>normal</b>            | Specifies normal ToS (value = 0).                |

## Examples

The following example specifies that all IP traffic to destination host, 10.25.1.1, is to be denied, and all other traffic on subnet 10.25.1/24 is to be permitted:

```
[local]Redback(config-ctx)#ip access-list protect201
[local]Redback(config-access-list)#deny ip any host 10.25.1.1
[local]Redback(config-access-list)#permit ip any 10.25.1.0 0.0.0.255
```

## Related Commands

```
ip access-group
ip access-list
permit
resequence ip access-list
```

## description

**description** *text*

**no description**

## Purpose

Associates a text description with an IP access control list (ACL) or a policy ACL.

## Command Mode

access control list configuration

## Syntax Description

|             |                                                              |
|-------------|--------------------------------------------------------------|
| <i>text</i> | Alphanumeric text description to be associated with the ACL. |
|-------------|--------------------------------------------------------------|

## Default

No description is associated with the ACL.

## Usage Guidelines

Use the **description** command to associate a text description with the ACL.

You can use a text description to notate what an ACL consists of or how it is to be used. Only one description can be associated with a single ACL. To revise a description, create a new one, and the old one is overwritten.

Use the **no** form of this command to remove the description from an ACL.

## Examples

The following example creates a text description to be associated with the IP ACL, restricted:

```
[local]Redback(config-ctx)#ip access-list restricted
[local]Redback(config-access-list)#description private net
```

The following example creates a text description to be associated with the policy ACL, trafficin:

```
[local]Redback(config-ctx)#policy access-list trafficin
[local]Redback(config-access-list)#description inbound traffic web
```

## Related Commands

**ip access-list**  
**policy access-list**



## ip access-group

**ip access-group** *acl-name* {**in** | **out**} [**count**] [**log**]

**no ip access-group** *acl-name* {**in** | **out**} [**count**] [**log**]

### Purpose

Applies an IP access control list (ACL) to packets associated with an interface or subscriber.

### Command Mode

interface configuration

subscriber configuration

### Syntax Description

|                 |                                                                                        |
|-----------------|----------------------------------------------------------------------------------------|
| <i>acl-name</i> | Name of the IP ACL to apply to the interface.                                          |
| <b>in</b>       | Specifies that the ACL is to be applied to incoming packets.                           |
| <b>out</b>      | Specifies that the ACL is to be applied to outgoing packets.                           |
| <b>count</b>    | Optional. Enables ACL packet counting. Not available in subscriber configuration mode. |
| <b>log</b>      | Optional. Enables ACL packet logging. Not available in subscriber configuration mode.  |

### Default

No ACL is applied.

### Usage Guidelines

Use the **ip access-group** command to apply an IP ACL to packets associated with an interface or subscriber, restricting the flow of traffic through the SmartEdge router.

**Note** Applying an ACL to an interface has no effect if the named ACL has not yet been defined. All packets are permitted as if no restrictions were in place.

When you use the **count** keyword, the system keeps track of the number of matches that occur. When you use the **log** keyword, the system keeps track of the number of packets that were denied. By default, counting and logging of packets is disabled.



**Caution** Risk of performance loss. Enabling the count and log functions can affect system performance. To reduce the risk, exercise caution when enabling these features on a production system.

To disable packet counting or logging, enter the **ip access-group** command again, omitting the **count** or **log** keyword.

Use the **no** form of this command to remove an applied IP ACL from association with the interface.

### Examples

The following example applies the IP ACL, WebCacheACL, to the interface, topgun, and enables both packet counting and logging:

```
[local]Redback(config)#context fighter  
[local]Redback(config-ctx)#interface topgun  
[local]Redback(config-if)#ip access-group WebCacheACL in log count
```

The following example applies the ACL, WebCacheACL, to the subscriber, joe:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#subscriber name joe  
[local]Redback(config-sub)#ip access-group WebCacheACL out
```

### Related Commands

**deny**  
**ip access-list**  
**permit**

## ip access-list

**ip access-list** *acl-name*

**no ip access-list** *acl-name*

### Purpose

Configures an IP access control list (ACL) and enters access control list configuration mode.

### Command Mode

context configuration

### Syntax Description

|                 |                                                     |
|-----------------|-----------------------------------------------------|
| <i>acl-name</i> | Name of the ACL. Must be unique within the context. |
|-----------------|-----------------------------------------------------|

### Default

None

### Usage Guidelines

Use the **ip access-list** command to configure an IP ACL and enter access control list configuration mode, where you can define statements using the **permit** and **deny** commands. All IP ACLs have an implicit **deny any any** statement at the end.

When the IP ACL is created and its conditions have been set, you can apply the list to any of these entities:

- An interface to restrict the flow of traffic through the SmartEdge router with the **ip access-group** command (in interface configuration mode).
- Local inbound traffic coming into the SmartEdge kernel with the **(admin-access-group** command (in context configuration mode).
- An interface enabled with reverse path forwarding (RPF) to allow packets that fail the RPF check but match the ACL to pass through with the **ip verify unicast source** command (in interface configuration mode).

A reference to an IP ACL that does not exist or does not contain any configured entries implicitly matches and permits all packets.

Use the **no** form of this command to remove an ACL from the configuration.

### Examples

The following example creates an IP ACL, WebCacheACL:

```
[local]Redback(config-ctx)#ip access-list WebCacheACL
[local]Redback(config-access-list)#
```

### Related Commands

**admin-access-group**  
**deny**  
**ip access-group**  
**permit**

# modify ip access-list

**modify ip access-list** *acl-name* **condition** *cond-id* {**permit** | **deny**}

## Purpose

Modifies, in real time, the action for the specified condition referenced by statements in the IP access control list (ACL), without requiring reconfiguration of the IP ACL.

## Command Mode

exec

## Syntax Description

|                                 |                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------|
| <i>acl-name</i>                 | Name of the ACL to be modified.                                                                 |
| <b>condition</b> <i>cond-id</i> | ACL condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295. |
| <b>permit</b>                   | Applies a permit action.                                                                        |
| <b>deny</b>                     | Applies a deny action.                                                                          |

## Default

None

## Usage Guidelines

Use the **modify ip access-list** command to modify, in real time, the action for the specified condition referenced by statements in the IP ACL, without requiring reconfiguration of the IP ACL.

**Note** If the specified condition ID is already configured (using the **condition** command in access control list configuration mode), the **modify ip access-list** command is ignored. If a condition ID is configured using the **condition** command and the changes are saved, any condition ID that may be currently applied using the **modify ip access-list** command at runtime is immediately overwritten.

For information about the **condition** and **ip access-list** commands in context configuration mode, see the “ACL Configuration Commands” chapter in the *IP Services and Security Command Reference* for the SmartEdge OS.

## Examples

With the following configuration, using the **modify ip access-list list\_cond condition 200 deny** command will change the action of the ACL condition 200 in statement 20 in the IP ACL *list\_cond* from **permit** to **deny**. However, using the **modify ip access-list list\_cond condition 100 permit** command will not affect the **deny** action of the ACL condition 100 because it has already been configured.

```
[local]Redback(config-ctx)#ip access-list list_cond
[local]Redback(config-access-list)#condition 100 time-range
```

## Command Descriptions

---

```
[local]Redback(config-acl-condition)#absolute start 2005:01:01:01:00 end  
2006:01:01:01:01 permit  
[local]Redback(config-acl-condition)#exit  
[local]Redback(config-access-list)#seq 10 deny tcp any any eq 80 cond 100  
[local]Redback(config-access-list)#seq 20 permit tcp any any eq 81 cond 200
```

## Related Commands

**modify policy access-list**

# modify policy access-list

**modify policy access-list** *acl-name* **condition** *cond-id* **class** *class-name*

## Purpose

Modifies, in real time, the action for the specified condition referenced by statements in the policy access control list (ACL), without requiring reconfiguration of the policy ACL.

## Command Mode

exec

## Syntax Description

|                                 |                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------|
| <i>acl-name</i>                 | Name of the ACL to be modified.                                                                 |
| <b>condition</b> <i>cond-id</i> | ACL condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295. |
| <b>class</b> <i>class-name</i>  | Class name applied to statements in the policy ACL.                                             |

## Default

None

## Usage Guidelines

Use the **modify policy access-list** command to modify, in real time, the action for the specified condition referenced by statements in the policy ACL, without requiring reconfiguration of the policy ACL.

**Note** If the specified condition ID is already configured (using the **condition** command in access control list configuration mode), the **modify policy access-list** command is ignored. If a condition ID is configured using the **condition** command and the changes are saved, any condition ID that may be currently applied using the **modify policy access-list** command at runtime is immediately overwritten.

## Examples

With the following configuration, using the **modify policy access-list list\_cond condition 200 deny** command will change the action of the ACL condition, 200, in statement 20 in the IP ACL, *list\_cond*, from permit to deny. However, using the **modify policy access-list list\_cond condition 100 permit** command will not affect the deny action of the ACL condition, 100, because it has already been configured.

```
[local]Redback(config-ctx)#policy access-list list_cond
[local]Redback(config-access-list)#condition 100 time-range
[local]Redback(config-acl-condition)#absolute start 2005:01:01:01:00 end
2006:01:01:01:01 permit
[local]Redback(config-acl-condition)#exit
[local]Redback(config-access-list)#seq 10 deny tcp any any eq 80 cond 100
[local]Redback(config-access-list)#seq 20 permit tcp any any eq 81 cond 200
```

## Related Commands

**condition**  
**modify ip access-list**  
**policy access-list**



## periodic

**periodic** *day...* *hh:mm to hh:mm* {{**permit** | **deny**} | **class** *class-name*}

**no periodic** *day...* *hh:mm to hh:mm*

### Purpose

Creates a periodic time access control list (ACL) condition statement.

### Command Mode

ACL condition configuration

### Syntax Description

|                                |                                                                                                                                        |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <i>day...</i>                  | One or more days of the week in which the ACL condition is applied.                                                                    |
| <i>hh:mm</i>                   | Hour and minute, for each specified day of the week, to start the ACL condition.                                                       |
| <b>to</b> <i>hh:mm</i>         | Hour and minute, for each specified day of the week, to stop the ACL condition.                                                        |
| <b>permit</b>                  | Applies permit action, during the specified time ranges, to all ACL statements that reference the ACL condition.                       |
| <b>deny</b>                    | Applies deny action, during the specified time ranges, to all ACL statements that reference the ACL condition. Used only with IP ACLs. |
| <b>class</b> <i>class-name</i> | Name of the class assigned to policy ACL statements that reference the ACL condition. Used only with policy ACLs.                      |

### Default

None

### Usage Guidelines

Use the **periodic** command to create a periodic time ACL condition statement that permits or denies packets, or assigns packets to a class, based on specific date and time ranges. A periodic time ACL condition is referenced by either an IP ACL statement or a policy ACL statement.

Each ACL condition statement can include up to seven absolute or periodic time statements in any combination.

Use the **no** form of this command to delete the periodic time ACL condition statement.

### Examples

The following example creates a periodic ACL condition statement for the ACL condition, 55, which is referenced by the policy ACL, `policy_acl_2`, such that the `Bar003` class name is applied every Wednesday from 9:00 p.m. to 11:00 p.m (21:00 to 23:00 in 24-hour format) to packets assigned to the `Bar003` class.

```
[local]Redback(config-ctx)#policy access-list policy_acl_2  
[local]Redback(config-access-list)#condition 55 time-range  
[local]Redback(config-acl-condition)#periodic wednesday 21:00 to 23:00 class Bar003
```

### Related Commands

- absolute**
- condition**
- ip access-list**
- policy access-list**

## permit

```
[seq seq-num] permit [protocol] {src src-wildcard | any | host src} [cond port | range port end-port]
[dest dest-wildcard | any | host dest] [cond port | range port end-port] [length {cond length |
range length end-length}] [icmp-type icmp-type [icmp-code icmp-code]] [igmp-type igmp-type]
[dscp eq dscp-value] [established] [precedence prec-value] [tos tos-value] [class class-name]
[condition cond-id]

no seq seq-num
```

### Purpose

Creates an IP or policy access control list (ACL) statement to allow packets that meet the specified criteria.

### Command Mode

access control list configuration

### Syntax Description

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>seq seq-num</b>  | Optional. Sequence number for the statement. The range of values is 1 to 4,294,967,295.                                                                                                                                                                                                                                                                                                                        |
| <i>protocol</i>     | Optional. Number indicating a protocol as specified in RFC 1700, <i>Assigned Numbers</i> . The range of values is 0 to 255 or one of the keywords listed in Table 8-16.                                                                                                                                                                                                                                        |
| <i>src</i>          | Source address to be included in the permit or deny criteria. An IP address in the form <i>A.B.C.D</i> .                                                                                                                                                                                                                                                                                                       |
| <i>src-wildcard</i> | Indication of which bits in the <i>source</i> argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the <i>src-wildcard</i> argument mean that the corresponding bits in the <i>src</i> argument must match; one-bits in the <i>src-wildcard</i> argument mean that the corresponding bits in the <i>src</i> argument are ignored. |
| <b>any</b>          | Specifies a completely wildcarded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.                                                                                                                                                                                              |
| <b>host source</b>  | Address of a single-host source with no wild-carded address bits. The <b>host source</b> construct is identical to the <i>src src-wildcard</i> construct if the wildcard address indicates that all bits should be matched (0.0.0.0).                                                                                                                                                                          |
| <i>cond</i>         | Optional. Matching condition for the <i>port</i> or <i>length</i> argument, according to one of the keywords listed in Table 8-17.                                                                                                                                                                                                                                                                             |
| <i>port</i>         | Optional. TCP or UDP source or destination port. This construct is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 8-18 and Table 8-19.                                                                                                                                                                                  |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>range</b> <i>port end-port</i>     | Optional. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. This construct is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 8-18 and Table 8-19.                                              |
| <i>dest</i>                           | Optional. Destination address to be included in the permit or deny criteria. An IP address in the form <i>A.B.C.D</i> .                                                                                                                                                                                                                                                                                          |
| <i>dest-wildcard</i>                  | Indication of which bits in the <i>dest</i> argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the <i>dest-wildcard</i> argument mean that the corresponding bits in the <i>dest</i> argument must match; one-bits in the <i>dest-wildcard</i> argument mean that the corresponding bits in the <i>dest</i> argument are ignored. |
| <b>length</b>                         | Optional. Indicates that packet length is to be used as a filter. The packet length is the length of the network-layer packet, beginning with the IP header. This is true irrespective of the specified protocol.                                                                                                                                                                                                |
| <i>length</i>                         | Packet length. The range of values is 20 to 65,535.                                                                                                                                                                                                                                                                                                                                                              |
| <b>range</b> <i>length end-length</i> | Packets that fall into the range of specified lengths. Each value ( <i>length</i> and <i>end-length</i> ) can be from 20 to 65,535.                                                                                                                                                                                                                                                                              |
| <b>host</b> <i>dest</i>               | Address of a single-host destination with no wildcarded address bits. The <b>host</b> <i>dest</i> construct is identical to the <i>dest dest-wildcard</i> construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).                                                                                                                                                                |
| <b>icmp-type</b> <i>icmp-type</i>     | Optional. Type of ICMP packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 8-20. This argument is only available if you specify the ICMP protocol.                                                                                                                                                                                                                      |
| <b>icmp-code</b> <i>icmp-code</i>     | Optional if you use the <b>icmp-type</b> <i>icmp-type</i> construct. A particular ICMP message code to be matched. The range of values is 0 to 255. This argument is only accepted if you specified <b>icmp</b> as the <i>protocol</i> argument.                                                                                                                                                                 |
| <b>igmp-type</b> <i>igmp-type</i>     | Optional. Type of IGMP packet to be matched. This argument is only accepted if you specified <b>igmp</b> as the <i>protocol</i> argument. The range of values is 0 to 15 or one of the keywords listed in Table 8-21.                                                                                                                                                                                            |
| <b>dscp eq</b> <i>dscp-value</i>      | Optional. Packet's Differentiated Services Code Point (DSCP) value must be equal to the value specified in the <i>dscp-value</i> argument to match the criteria. The range of values is 0 to 63 or one of the keywords listed in Table 8-22.                                                                                                                                                                     |
| <b>established</b>                    | Optional. Specifies that only established connections are to be matched. This keyword is only available if you specified <b>tcp</b> for the <i>protocol</i> argument.                                                                                                                                                                                                                                            |
| <b>precedence</b> <i>prec-value</i>   | Optional. Precedence value of packets to be considered a match. The range of values is 0 to 7, 7 being the highest precedence, or one of the keywords listed in Table 8-23.                                                                                                                                                                                                                                      |
| <b>tos</b> <i>tos-value</i>           | Optional. Type of service (ToS) to be considered a match. The range of values is 0 to 15 or one of the keywords listed in Table 8-24.                                                                                                                                                                                                                                                                            |

|                                 |                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>class</b> <i>class-name</i>  | Optional. Policy-based class name. Available for policy ACLs only.                                        |
| <b>condition</b> <i>cond-id</i> | Optional. ACL condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295. |

## Default

None

## Usage Guidelines

Use the **permit** command to create the IP or policy ACL statement to allow packets that meet the specified criteria.

The *cond port* and *cond length* constructs are mutually exclusive with the **range** construct for the *port* and *length* arguments, respectively.

**Note** There is an implicit **deny any any** statement at the end of every ACL.

Use the **no** form of this command to delete the statement with the specified sequence number from the ACL.

Table 8-16 lists the valid keyword substitutions for the *protocol* argument.

**Table 8-16 Valid Keyword Substitutions for the *protocol* Argument**

| Keyword | Definition                                    |
|---------|-----------------------------------------------|
| ahp     | Specifies Authentication Header Protocol.     |
| esp     | Specifies Encapsulation Security Payload.     |
| gre     | Specifies Generic Routing Encapsulation.      |
| host    | Specifies host source address.                |
| icmp    | Specifies Internet Control Message Protocol.  |
| igmp    | Specifies Internet Group Management Protocol. |
| ip      | Specifies any IP protocol.                    |
| ipinip  | Specifies IP-in-IP tunneling.                 |
| ospf    | Specifies Open Shortest Path First.           |
| pcp     | Specifies Payload Compression Protocol.       |
| pim     | Specifies Protocol Independent Multicast.     |
| tcp     | Specifies Transmission Control Protocol.      |
| udp     | Specifies User Datagram Protocol.             |

Table 8-17 lists the valid keyword substitutions for the *cond* argument.

**Table 8-17 Valid Keyword Substitutions for the *cond* Argument**

| Keyword    | Description                                                                                              |
|------------|----------------------------------------------------------------------------------------------------------|
| <b>eq</b>  | Specifies that values must be equal to those specified by the <i>port</i> or <i>length</i> argument.     |
| <b>gt</b>  | Specifies that values must be greater than those specified by the <i>port</i> or <i>length</i> argument. |
| <b>lt</b>  | Specifies that values must be less than those specified by the <i>port</i> or <i>length</i> argument.    |
| <b>neq</b> | Specifies that values must not be equal to those specified by the <i>port</i> or <i>length</i> argument. |

Table 8-18 lists the valid keyword substitutions for the *port* argument when it is used to specify a TCP port.

**Table 8-18 Valid Keyword Substitutions for the *port* Argument (TCP Port)**

| Keyword            | Definition                                   | Corresponding Port Number |
|--------------------|----------------------------------------------|---------------------------|
| <b>bgp</b>         | Border Gateway Protocol (BGP)                | 179                       |
| <b>chargen</b>     | Character generator                          | 19                        |
| <b>cmd</b>         | Remote commands (rcmd)                       | 514                       |
| <b>daytime</b>     | Daytime                                      | 13                        |
| <b>discard</b>     | Discard                                      | 9                         |
| <b>domain</b>      | Domain Name System                           | 53                        |
| <b>echo</b>        | Echo                                         | 7                         |
| <b>exec</b>        | Exec (rsh)                                   | 512                       |
| <b>finger</b>      | Finger                                       | 79                        |
| <b>ftp</b>         | File Transfer Protocol                       | 21                        |
| <b>ftp-data</b>    | FTP data connections (used infrequently)     | 20                        |
| <b>gopher</b>      | Gopher                                       | 70                        |
| <b>hostname</b>    | Network interface card (NIC) hostname server | 101                       |
| <b>ident</b>       | Identification protocol                      | 113                       |
| <b>irc</b>         | Internet Relay Chat                          | 194                       |
| <b>klogin</b>      | Kerberos login                               | 543                       |
| <b>kshell</b>      | Kerberos Shell                               | 544                       |
| <b>login</b>       | Login (rlogin)                               | 513                       |
| <b>lpd</b>         | Printer service                              | 515                       |
| <b>nntp</b>        | Network News Transport Protocol              | 119                       |
| <b>pim-auto-rp</b> | Protocol Independent Multicast Auto-RP       | 496                       |
| <b>pop2</b>        | Post Office Protocol Version 2               | 109                       |
| <b>pop3</b>        | Post Office Protocol Version 3               | 110                       |
| <b>shell</b>       | Remote command shell                         | 514                       |

**Table 8-18 Valid Keyword Substitutions for the *port* Argument (TCP Port) (continued)**

| Keyword       | Definition                                       | Corresponding Port Number |
|---------------|--------------------------------------------------|---------------------------|
| <b>smtp</b>   | Simple Mail Transport Protocol                   | 25                        |
| <b>ssh</b>    | Secure Shell                                     | 22                        |
| <b>sunrpc</b> | Sun Remote Procedure Call                        | 111                       |
| <b>syslog</b> | System logger                                    | 514                       |
| <b>tacacs</b> | Terminal Access Controller Access Control System | 49                        |
| <b>talk</b>   | Talk                                             | 517                       |
| <b>telnet</b> | Telnet                                           | 23                        |
| <b>time</b>   | Time                                             | 37                        |
| <b>uucp</b>   | Unix-to-Unix Copy Program                        | 540                       |
| <b>whois</b>  | Nickname                                         | 43                        |
| <b>www</b>    | World Wide Web (HTTP)                            | 80                        |

Table 8-19 lists the valid keyword substitutions for the *port* argument when it is used to specify a UDP port.

**Table 8-19 Valid Keyword Substitutions for the *port* Argument (UDP Port)**

| Keyword            | Definition                                                         | Corresponding Port Number |
|--------------------|--------------------------------------------------------------------|---------------------------|
| <b>biff</b>        | Biff (Mail Notification, Comsat)                                   | 512                       |
| <b>bootpc</b>      | Bootstrap Protocol client                                          | 68                        |
| <b>bootps</b>      | Bootstrap Protocol server                                          | 67                        |
| <b>discard</b>     | Discard                                                            | 9                         |
| <b>dnsix</b>       | DNSIX Security Protocol Auditing                                   | 195                       |
| <b>domain</b>      | Domain Name System                                                 | 53                        |
| <b>echo</b>        | Echo                                                               | 7                         |
| <b>isakmp</b>      | Internet Security Association and Key Management Protocol (ISAKMP) | 500                       |
| <b>mobile-ip</b>   | Mobile IP Registration                                             | 434                       |
| <b>nameserver</b>  | IEN116 Name Service (obsolete)                                     | 42                        |
| <b>netbios-dgm</b> | NetBIOS Datagram Service                                           | 138                       |
| <b>netbios-ns</b>  | NetBIOS Name Service                                               | 137                       |
| <b>netbios-ss</b>  | NetBIOS Session Service                                            | 139                       |
| <b>ntp</b>         | Network Time Protocol                                              | 123                       |
| <b>pim-auto-rp</b> | Protocol Independent Multicast Auto-RP                             | 496                       |
| <b>rip</b>         | Router Information Protocol (router, in.routed)                    | 520                       |
| <b>snmp</b>        | Simple Network Management Protocol                                 | 161                       |

**Table 8-19 Valid Keyword Substitutions for the *port* Argument (UDP Port) (continued)**

| Keyword         | Definition                                       | Corresponding Port Number |
|-----------------|--------------------------------------------------|---------------------------|
| <b>snmptrap</b> | SNMP Traps                                       | 162                       |
| <b>sunrpc</b>   | Sun Remote Procedure Call                        | 111                       |
| <b>syslog</b>   | System logger                                    | 514                       |
| <b>tacacs</b>   | Terminal Access Controller Access Control System | 49                        |
| <b>talk</b>     | Talk                                             | 517                       |
| <b>tftp</b>     | Trivial File Transfer Protocol                   | 69                        |
| <b>time</b>     | Time                                             | 37                        |
| <b>who</b>      | Who Service (rwho)                               | 513                       |
| <b>xdmcp</b>    | X Display Manager Control Protocol               | 177                       |

Table 8-20 lists the valid keyword substitutions for the *icmp-type* argument.

**Table 8-20 Valid Keyword Substitutions for the *icmp-type* Argument**

| Keyword                            | Description                                               |
|------------------------------------|-----------------------------------------------------------|
| <b>administratively-prohibited</b> | Administratively prohibited                               |
| <b>alternate-address</b>           | Alternate address                                         |
| <b>conversion-error</b>            | Datagram conversion                                       |
| <b>dod-host-prohibited</b>         | Host prohibited                                           |
| <b>dod-net-prohibited</b>          | Net prohibited                                            |
| <b>echo</b>                        | Echo (ping)                                               |
| <b>echo-reply</b>                  | Echo reply                                                |
| <b>general-parameter-problem</b>   | General parameter problem                                 |
| <b>host-isolated</b>               | Host isolated                                             |
| <b>host-precedence-unreachable</b> | Host unreachable for precedence                           |
| <b>host-redirect</b>               | Host redirect                                             |
| <b>host-tos-redirect</b>           | Host redirect for ToS                                     |
| <b>host-tos-unreachable</b>        | Host unreachable for ToS                                  |
| <b>host-unknown</b>                | Host unknown                                              |
| <b>host-unreachable</b>            | Host unreachable                                          |
| <b>information-reply</b>           | Information replies                                       |
| <b>information-request</b>         | Information requests                                      |
| <b>log</b>                         | Log matches against this entry                            |
| <b>log-input</b>                   | Log matches against this entry, including input interface |
| <b>mask-reply</b>                  | Mask replies                                              |



**Table 8-20 Valid Keyword Substitutions for the *icmp-type* Argument** (*continued*)

| Keyword                       | Description                                          |
|-------------------------------|------------------------------------------------------|
| <b>mask-request</b>           | Mask requests                                        |
| <b>mobile-redirect</b>        | Mobile host redirects                                |
| <b>net-redirect</b>           | Network redirect                                     |
| <b>net-tos-redirect</b>       | Network redirect for ToS                             |
| <b>net-tos-unreachable</b>    | Network unreachable for ToS                          |
| <b>net-unreachable</b>        | Network unreachable                                  |
| <b>network-unknown</b>        | Network unknown                                      |
| <b>no-room-for-option</b>     | Parameter required but no room                       |
| <b>option-missing</b>         | Parameter required but not present                   |
| <b>packet-too-big</b>         | Fragmentation needed and DF set                      |
| <b>parameter-problem</b>      | All parameter problems                               |
| <b>port-unreachable</b>       | Port unreachable                                     |
| <b>precedence</b>             | Match packets with given precedence value            |
| <b>precedence-unreachable</b> | Precedence cutoff                                    |
| <b>protocol-unreachable</b>   | Protocol unreachable                                 |
| <b>reassembly-timeout</b>     | Reassembly timeout                                   |
| <b>redirect</b>               | All redirects                                        |
| <b>router-advertisement</b>   | Router discovery advertisement                       |
| <b>router-solicitation</b>    | Router discovery solicitation                        |
| <b>source-quench</b>          | Source quenches                                      |
| <b>source-route-failed</b>    | Source route failed                                  |
| <b>time-exceeded</b>          | All time exceeded messages                           |
| <b>time-range</b>             | Specify a time-range                                 |
| <b>timestamp-reply</b>        | Timestamp replies                                    |
| <b>timestamp-request</b>      | Timestamp requests                                   |
| <b>tos</b>                    | Match packets with given type of service (ToS) value |
| <b>traceroute</b>             | Traceroute                                           |
| <b>ttl-exceeded</b>           | TTL Exceeded                                         |
| <b>unreachable</b>            | All unreachables                                     |

Table 8-21 lists the valid keyword substitutions for the *igmp-type* argument.

**Table 8-21 Valid Keyword Substitutions for the *igmp-type* Argument**

| Keyword            | Description                                           |
|--------------------|-------------------------------------------------------|
| <b>dvmrp</b>       | Specifies Distance-Vector Multicast Routing Protocol. |
| <b>Host-query</b>  | Specifies host query.                                 |
| <b>Host-report</b> | Specifies host report.                                |
| <b>pim</b>         | Specifies Protocol Independent Multicast.             |

Table 8-22 lists the valid keyword substitutions for the *dscp-value* argument.

**Table 8-22 Valid Keyword Substitutions for the *dscp-value* Argument**

| Keyword     | Definition                                   |
|-------------|----------------------------------------------|
| <b>af11</b> | Assured Forwarding—Class 1/Drop precedence 1 |
| <b>af12</b> | Assured Forwarding—Class 1/Drop precedence 2 |
| <b>af13</b> | Assured Forwarding—Class 1/Drop precedence 3 |
| <b>af21</b> | Assured Forwarding—Class 2/Drop precedence 1 |
| <b>af22</b> | Assured Forwarding—Class 2/Drop precedence 2 |
| <b>af23</b> | Assured Forwarding—Class 2/Drop precedence 3 |
| <b>af31</b> | Assured Forwarding—Class 3/Drop precedence 1 |
| <b>af32</b> | Assured Forwarding—Class 3/Drop precedence 2 |
| <b>af33</b> | Assured Forwarding—Class 3/Drop precedence 3 |
| <b>af41</b> | Assured Forwarding—Class 4/Drop precedence 1 |
| <b>af42</b> | Assured Forwarding—Class 4/Drop precedence 2 |
| <b>af43</b> | Assured Forwarding—Class 4/Drop precedence 3 |
| <b>cs0</b>  | Class Selector 0                             |
| <b>cs1</b>  | Class Selector 1                             |
| <b>cs2</b>  | Class Selector 2                             |
| <b>cs3</b>  | Class Selector 3                             |
| <b>cs4</b>  | Class Selector 4                             |
| <b>cs5</b>  | Class Selector 5                             |
| <b>cs6</b>  | Class Selector 6                             |
| <b>cs7</b>  | Class Selector 7                             |
| <b>df</b>   | Default Forwarding (same as cs0)             |
| <b>ef</b>   | Expedited Forwarding                         |

Table 8-23 lists the valid keyword substitutions for the *prec-value* argument.

**Table 8-23 Valid Keyword Substitutions for the *prec-value* Argument**

| Keyword               | Description                                            |
|-----------------------|--------------------------------------------------------|
| <b>tine</b>           | Specifies routine precedence (value = 0).              |
| <b>priority</b>       | Specifies priority precedence (value = 1).             |
| <b>immediate</b>      | Specifies immediate precedence (value = 2).            |
| <b>flash</b>          | Specifies flash precedence (value = 3).                |
| <b>flash-override</b> | Specifies flash override precedence (value = 4).       |
| <b>critical</b>       | Specifies critical precedence (value = 5).             |
| <b>internet</b>       | Specifies internetwork control precedence (value = 6). |
| <b>network</b>        | Specifies network control precedence (value = 7).      |

Table 8-24 lists the valid keyword substitutions for the *tos-value* argument.

**Table 8-24 Valid Keyword Substitutions for the *tos-value* Argument**

| Keyword                  | Description                                      |
|--------------------------|--------------------------------------------------|
| <b>max-reliability</b>   | Specifies maximum reliable ToS (value = 2).      |
| <b>max-throughput</b>    | Specifies maximum throughput ToS (value = 4).    |
| <b>min-delay</b>         | Specifies minimum delay ToS (value = 8).         |
| <b>min-monetary-cost</b> | Specifies minimum monetary cost ToS (value = 1). |
| <b>normal</b>            | Specifies normal ToS (value = 0).                |

## Examples

The following example specifies that all IP traffic from subnet 10.25/16 is to be allowed. All other traffic is dropped because of the implicit **deny any any** statement at the end of the ACL:

```
[local]Redback(config-ctx)#ip access-list protect201
[local]Redback(config-access-list)#permit ip 10.25.0.0 0.0.255.255 any
```

The following example shows how to use the **seq** keyword to edit the existing qos-acl-1 ACL, adding a statement using sequence number 25:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list qos-acl-1
[local]Redback(config-access-list)#seq 25 permit tcp 10.10.10.4 0.0.0.0 any eq 80
```

## Related Commands

```
ip access-list
policy access-list
resequence ip access-list
resequence policy access-list
```

## policy access-list

**policy access-list** *acl-name*

**no policy access-list** *acl-name*

### Purpose

Configures a policy access control list (ACL) and enters access control list configuration mode.

### Command Mode

context configuration

### Syntax Description

*acl-name*                      Policy ACL name.

### Default

None

### Usage Guidelines

Use the **policy access-list** command to configure a policy ACL and to enter access control list configuration mode, where you can define statements using the **permit** command.

A reference to a policy ACL that does not exist is ignored.

Use the **no** form of this command to remove the policy ACL.

### Examples

The following example uses a policy ACL to prioritize Web and VOIP traffic on a circuit, marking these packet types as DF and AF11, respectively. All other traffic is marked as DF also.

```
[local]Redback(config-ctx)#policy access-list QoSACL-1
[local]Redback(config-access-list)#permit tcp any any eq 80 class Web
[local]Redback(config-access-list)#permit udp any any eq 1000 class VOIP
[local]Redback(config-access-list)#permit any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#qos policy PolicingAndMarking policing
[local]Redback(config-policy-policing)#access-group QoSACL-1
[local]Redback(config-policy-acl)#class Web
[local]Redback(config-policy-acl-class)#mark dscp DF
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class VOIP
[local]Redback(config-policy-acl-class)#mark dscp AF11
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class default
[local]Redback(config-policy-acl-class)#mark dscp DF
```

```
[local]Redback(config-policy-acl-class)#exit  
[local]Redback(config-policy-acl)#exit  
[local]Redback(config-policy-policing)#exit  
[local]Redback(config)#port ethernet 3/0  
[local]Redback(config-port)#bind interface FromSubscriber local  
[local]Redback(config-port)#qos policy policing PolicingAndMarking
```

## Related Commands

- forward policy**
- nat policy**
- permit**
- qos policy metering**
- qos policy policing**
- resequence policy access-list**

## resequence ip access-list

**resequence ip access-list** *acl-name*

### Purpose

Reassigns sequence numbers to the entries in the specified IP access control list (ACL) to be in increments of 10.

### Command Mode

context configuration

### Syntax Description

*acl-name*                      Name of the ACL to be resequenced.

### Default

No resequencing is performed.

### Usage Guidelines

Use the **resequence ip access-list** command to reassign sequence numbers to the entries in the specified IP ACL to be in increments of 10. This command is useful in the case where manually assigned sequence numbers have left no room between entries for insertion of additional entries.

### Examples

The following example resequences the statements in the ACL, fremont1:

```
[local]Redback(config-ctx)#resequence ip access-list fremont1
```

### Related Commands

**ip access-list**

# resequence policy access-list

**resequence policy access-list** *acl-name*

## Purpose

Reassigns sequence numbers to the entries in the specified policy access control list (ACL) to be in increments of 10.

## Command Mode

context configuration

## Syntax Description

*acl-name*                      Name of the ACL to be resequenced.

## Default

No resequencing is performed.

## Usage Guidelines

Use the **resequence policy access-list** command to reassign sequence numbers to the entries in the specified policy ACL to be in increments of 10. This command is useful if manually assigned sequence numbers have left no further room between entries for insertion of additional entries.

## Examples

The following example resequences the statements in the policy ACL, oakland2:

```
[local]Redback(config-ctx)#resequence policy access-list oakland2
```

## Related Commands

**policy access-list**





# IP Service Policies

---

This part describes the tasks and commands used to configure forward policies, service policies, and Network Address Translation (NAT) policies. It consists of the following chapters:

- Chapter 9, “Forward Policy Configuration”
- Chapter 10, “NAT Policy Configuration”
- Chapter 11, “Service Policy Configuration”



# Forward Policy Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS forward policy features.

For information about the tasks and commands used to monitor, troubleshoot, and administer forward policies, see the “Forward Policy Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter includes the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

A forward policy applies only to IP traffic. A forward policy can be a combination of three actions:

- Mirroring

Mirroring copies packets forwards the duplicated packets to a designated outgoing port. Mirrored traffic (forwarded, dropped, or both) is typically sent to a packet sniffer (or similar device) so that traffic patterns can be analyzed. You can mirror all traffic, a sampling of traffic, or mirror only IP packet headers. You can mirror both incoming and outgoing packets.

- Redirect

Redirect forwards packets to IP addresses that are different than their original destination. You can redirect incoming packets only.

- Drop

The drop function specifies that particular packets are dropped, rather than forwarded; you can drop incoming packets only.

You can apply forward policies at one of two levels or at both levels simultaneously. One level applies to all packets on a circuit and is referred to as circuit-based forwarding. Another level applies only to a specific class of packets traveling across a circuit and is referred to as class-based forwarding.

These levels of forwarding policies are described in the following sections:

- Circuit-Based Forwarding
- Class-Based Forwarding
- Circuit- and Class-Based Forwarding

## Circuit-Based Forwarding

When you attach a forward policy that does not include a policy access control list (ACL) to a circuit, all traffic traveling over the circuit is treated in one manner, that is, it is mirrored, redirected, or dropped.

## Class-Based Forwarding

You configure a class using a policy ACL, which specifies classification filters that treat particular packets traveling over the same circuit differently. Each policy ACL supports up to eight unique classes. You can classify a packet according to its IP precedence value, protocol number, IP source and destination address, Internet Control Management Protocol (ICMP) attributes, Internet Group Management Protocol (IGMP) attributes, Transmission Control Protocol (TCP) attributes, and User Datagram Protocol (UDP) attributes.

To configure class-based forwarding for a circuit, you apply a policy ACL to a forward policy and then attach the forward policy to the circuit. For more information about policy ACLs, see Chapter 8, “ACL Configuration.”

## Circuit- and Class-Based Forwarding

You can combine circuit-based and class-based forwarding, so that a class of packets can be treated in one manner, dependent on a policy ACL, while all remaining packets traveling across the circuit are treated strictly according to the forward policy conditions.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure a forward policy, perform the tasks described in the following sections:

- Configure a Forward Policy
- Apply a Policy ACL to a Forward Policy

## Configure a Forward Policy

To configure a forward policy for circuit-based forwarding, for class-based forwarding, or for circuit- and class-based forwarding, perform the tasks described in Table 9-1; enter all commands in forward policy configuration mode, unless otherwise noted. You must have already configured the class in the policy ACL.

**Table 9-1 Configure a Forward Policy**

| #  | Task                                                                                                                                                                                                             | Root Command                                                                | Notes                                                                                                                                                                                                                                                                           |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select a policy and access forward policy configuration mode.                                                                                                                                          | <b>forward policy</b>                                                       | Enter this command in global configuration mode.                                                                                                                                                                                                                                |
| 2. | Redirect incoming packets not associated with a class with one of the following tasks: <ul style="list-style-type: none"> <li>To the specified output destination.</li> <li>To a next-hop IP address.</li> </ul> | <b>redirect destination circuit</b><br><b>redirect destination next-hop</b> |                                                                                                                                                                                                                                                                                 |
| 3. | Drop incoming packets not associated with a class.                                                                                                                                                               | <b>drop</b>                                                                 |                                                                                                                                                                                                                                                                                 |
| 4. | Mirror specified incoming or outgoing packets not associated with a class to a specified output destination.                                                                                                     | <b>mirror destination</b>                                                   |                                                                                                                                                                                                                                                                                 |
| 5. | Optional. Configure class-based forwarding for this policy.                                                                                                                                                      | See the "Apply a Policy ACL to a Forward Policy" section.                   |                                                                                                                                                                                                                                                                                 |
| 6. | Specify the destination circuit.                                                                                                                                                                                 | <b>forward output</b>                                                       | Enter this command in ATM PVC, Frame Relay PVC, GRE tunnel, or port configuration mode.<br>Select a different circuit from the circuits you have configured for the traffic being mirrored or redirected.                                                                       |
| 7. | Attach the policy to a circuit, using one of the following tasks: <ul style="list-style-type: none"> <li>To incoming traffic.</li> <li>To outgoing traffic.</li> </ul>                                           | <b>forward policy in</b><br><b>forward policy out</b>                       | Enter either of these commands in ATM DS-3, ATM OC, ATM PVC, dot1q PVC, DS-0 group, DS-1, DS-3, E1, E3, Frame Relay PVC, port, or subscriber configuration mode.<br><br>Only incoming packets can be redirected or dropped. Both incoming and outgoing packets can be mirrored. |

## Apply a Policy ACL to a Forward Policy

To apply a policy ACL to a forward policy for class-based forwarding, perform the tasks described in Table 9-2; enter all commands in policy ACL class configuration mode, unless otherwise noted.

**Table 9-2 Apply a Policy ACL to a Forward Policy**

| #  | Task                                                                                | Root Command        | Notes                                                                                                                                                         |
|----|-------------------------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Apply a policy ACL to the forward policy, and access policy ACL configuration mode. | <b>access-group</b> | Enter this command in forward policy configuration mode.                                                                                                      |
| 2. | Specify a class and access policy ACL class configuration mode.                     | <b>class</b>        | Enter this command in policy ACL configuration mode.<br>The class name must match the name of a class specified in a <b>permit</b> command in the policy ACL. |

**Table 9-2**    **Apply a Policy ACL to a Forward Policy** (*continued*)

| #  | Task                                                                                                                                                                                                                      | Root Command                                                                | Notes |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------|
| 3. | Optional. Redirect incoming packets associated with the class with one of the following tasks: <ul style="list-style-type: none"><li>• To the specified output destination.</li><li>• To a next-hop IP address.</li></ul> | <b>redirect destination circuit</b><br><b>redirect destination next-hop</b> |       |
| 4. | Optional. Drop incoming packets associated with the class.                                                                                                                                                                | <b>drop</b>                                                                 |       |
| 5. | Mirror specified packets associated with the class to a specified output destination.                                                                                                                                     | <b>mirror destination</b>                                                   |       |

---

# Configuration Examples

---

This section provides forward policy configuration examples in the following sections:

- Traffic Mirroring
- Traffic Redirect
- Traffic Drop
- Combination of Traffic Mirror, Redirect, and Drop in One Policy

## Traffic Mirroring

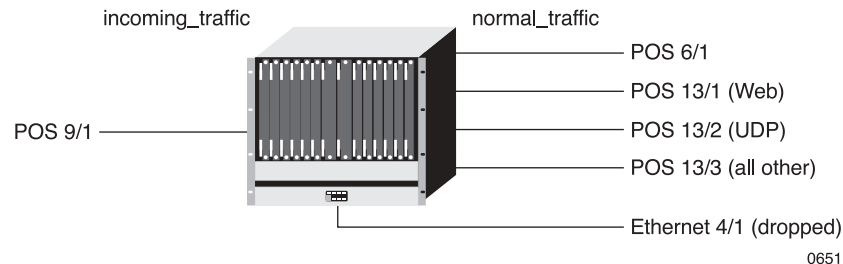
The following example implements traffic mirroring for:

- Web traffic-to-POS port 13/1
- Forwarded UDP traffic-to-POS port 13/2
- Dropped IP packets-to-Ethernet port 4/1 not more frequently than once every three seconds
- Other traffic-to-POS port 13/3

Traffic comes in through the interface, `incoming_traffic`, and leaves the router through the interface, `normal_traffic`.

Figure 9-1 displays the network topology for this example.

**Figure 9-1 Basic Traffic Mirroring Network Topology**



The interface configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface e1
[local]Redback(config-if)#ip address 31.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface incoming_traffic
[local]Redback(config-if)#ip address 51.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface normal_traffic
[local]Redback(config-if)#ip address 41.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p1
[local]Redback(config-if)#ip address 21.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p2
[local]Redback(config-if)#ip address 22.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p3
[local]Redback(config-if)#ip address 23.1.1.1/24
```

The policy ACL configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list PBR_ACL
[local]Redback(config-access-list)#seq 10 permit tcp any eq www any class WEB
[local]Redback(config-access-list)#seq 20 permit tcp any any eq www class WEB
[local]Redback(config-access-list)#seq 30 permit udp any class UDP
[local]Redback(config-access-list)#seq 40 permit ip any class IP
```

The forward policy configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#forward policy MirrorPolicy
[local]Redback(config-policy-frwd)#mirror destination DroppedTraffic dropped sampling 3000
[local]Redback(config-policy-frwd)#access-group PBR_ACL local
[local]Redback(config-policy-acl)#class WEB
[local]Redback(config-policy-acl-class)#mirror destination WebTraffic all
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class UDP
[local]Redback(config-policy-acl-class)#mirror destination UdpTraffic forwarded
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class IP
[local]Redback(config-policy-acl-class)#mirror destination IpTraffic all
```

The following configuration attaches the forward policy to incoming circuits and defines the forward output destinations:

```
[local]Redback#config
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface e1 local
[local]Redback(config-port)#forward output DroppedTraffic
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 6/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface normal_traffic local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface incoming_traffic local
[local]Redback(config-port)#forward policy MirrorPolicy in
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p1 local
[local]Redback(config-port)#forward output WebTraffic
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p2 local
[local]Redback(config-port)#forward output UdpTraffic
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/3
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p3 local
[local]Redback(config-port)#forward output IpTraffic
```



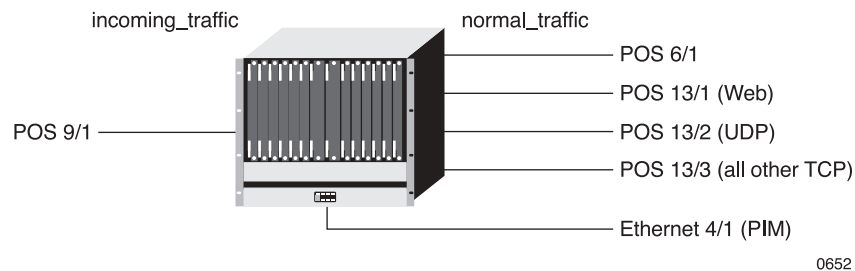
## Traffic Redirect

The following example implements traffic redirection for:

- Web traffic-to-network 100.1.1.0 with load balancing
- Forwarded UDP traffic-to-network 100.1.1.0 with load balancing
- Other TCP traffic-to-POS port 13/3 (multipath redirect)
- Protocol Independent Multicast (PIM) traffic-to-Ethernet port 4/1 (redirect to circuit)

This configuration allows all other traffic flow in the normal path. Traffic comes in through the interface, `incoming_traffic`, and leaves the router through the interface, `normal_traffic`. Figure 9-2 displays the network topology for this example.

**Figure 9-2 Basic Traffic Redirect Network Topology**



0652

The interface configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface e1
[local]Redback(config-if)#ip address 31.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface incoming_traffic
[local]Redback(config-if)#ip address 51.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface normal_traffic
[local]Redback(config-if)#ip address 41.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p1
[local]Redback(config-if)#ip address 21.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p2
[local]Redback(config-if)#ip address 22.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p3
[local]Redback(config-if)#ip address 23.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#ip route 100.1.1.0/24 21.1.1.2
[local]Redback(config-ctx)#ip route 100.1.1.0/24 22.1.1.2
```

The policy ACL configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list PBR_Redirect_ACL
[local]Redback(config-access-list)#seq 10 permit tcp any eq www any class WEB
[local]Redback(config-access-list)#seq 20 permit tcp any any eq www class WEB
[local]Redback(config-access-list)#seq 30 permit tcp any class TCP
[local]Redback(config-access-list)#seq 40 permit udp any class UDP
[local]Redback(config-access-list)#seq 50 permit pim any class PIM
```

The forward policy configuration is as follows:

```
[local]Redback(config)#forward policy RedirectPolicy
[local]Redback(config-policy-frwd)#access-group PBR_Redirect_ACL local
[local]Redback(config-policy-acl)#class WEB
[local]Redback(config-policy-acl-class)#redirect destination next-hop 100.1.1.0
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class UDP
[local]Redback(config-policy-acl-class)#redirect destination next-hop 100.1.1.0
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class PIM
[local]Redback(config-policy-acl-class)#redirect destination circuit PIM_OUT
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class TCP
[local]Redback(config-policy-acl-class)#redirect destination next-hop 23.1.1.11
23.1.1.12 23.1.1.13 23.1.1.14
```

The following configuration attaches the forward policy to an incoming circuit and defines the forward output destinations:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface e1 local
[local]Redback(config-port)#forward output PIM_OUT
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 6/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface normal_traffic local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface incoming_traffic local
[local]Redback(config-port)#forward policy RedirectPolicy in
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p1 local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p2 local
[local]Redback(config-port)#exit
```

```
[local]Redback(config)#port pos 13/3
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p3 local
```

## Traffic Drop

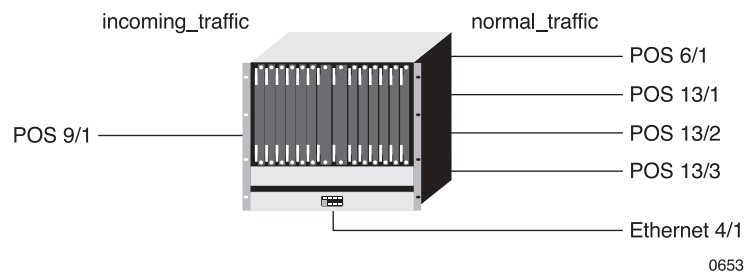
The following example implements traffic dropping for:

- ICMP traffic from host 51.1.1.2
- PIM packets

This configuration allows all other traffic flow in the normal path.

Traffic comes in through the interface, `incoming_traffic`, and leaves the router through the interface, `normal_traffic`. Figure 9-3 displays the network topology for this example.

**Figure 9-3 Basic Traffic Drop Network Topology**



The interface configuration is as follows:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface e1
[local]Redback(config-if)#ip address 31.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface incoming_traffic
[local]Redback(config-if)#ip address 51.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface normal_traffic
[local]Redback(config-if)#ip address 41.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p1
[local]Redback(config-if)#ip address 21.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p2
[local]Redback(config-if)#ip address 22.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p3
[local]Redback(config-if)#ip address 23.1.1.1/24
```

The policy ACL configuration is as follows:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list PBR_Drop_ACL
[local]Redback(config-access-list)#seq 10 permit icmp host 51.1.1.2 class ICMP
[local]Redback(config-access-list)#seq 20 permit pim any class PIM
```

The forward policy configuration is as follows:

```
[local]Redback(config)#forward policy DropPolicy
[local]Redback(config-policy-frwd)#access-group PBR_Drop_ACL local
[local]Redback(config-policy-acl)#class ICMP
[local]Redback(config-policy-acl-class)#drop
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class PIM
[local]Redback(config-policy-acl-class)#drop
```

The following configuration attaches the forward policy to an incoming circuit and binds interfaces to output ports:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface e1 local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 6/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface normal_traffic local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface incoming_traffic local
[local]Redback(config-port)#forward policy DropPolicy in
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p1 local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p2 local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/3
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p3 local
```

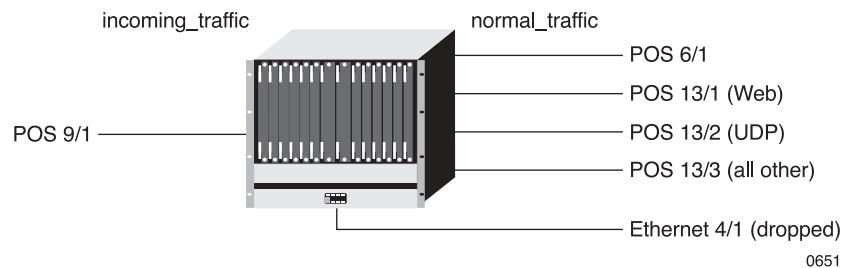
## Combination of Traffic Mirror, Redirect, and Drop in One Policy

The following example implements these functions:

- Redirects all web traffic to 100.1.1.2
- Mirrors all forwarded UDP traffic to POS port 13/2
- Mirrors all dropped IP packets to Ethernet port 4/1 not more frequently than once every three seconds
- Drops all ICMP traffic from 50.1.1.2
- Drops all PIM traffic
- Mirrors all other traffic to POS port 13/3

Traffic comes in through the interface, `incoming_traffic`, and leaves the box through the interface, `normal_traffic`. Figure 9-4 displays the network topology for the configuration example with traffic mirroring, redirect, and drop conditions in one policy.

**Figure 9-4 Basic Network Topology for Mirroring, Redirect, and Drop in One Policy**



The interface configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface e1
[local]Redback(config-if)#ip address 31.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface incoming_traffic
[local]Redback(config-if)#ip address 51.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface normal_traffic
[local]Redback(config-if)#ip address 41.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p1
[local]Redback(config-if)#ip address 21.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p2
[local]Redback(config-if)#ip address 22.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface p3
[local]Redback(config-if)#ip address 23.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#ip route 100.1.1.0/24 21.1.1.2
```

The policy ACL configuration is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list PBR_ACL
[local]Redback(config-access-list)#seq 10 permit tcp any eq www any class WEB
[local]Redback(config-access-list)#seq 20 permit tcp any any eq www class WEB
[local]Redback(config-access-list)#seq 30 permit udp any class UDP
[local]Redback(config-access-list)#seq 40 permit icmp host 50.1.1.2 class ICMP
[local]Redback(config-access-list)#seq 50 permit pim any class PIM
[local]Redback(config-access-list)#seq 60 permit ip any class IP
```

The forward policy configuration is as follows:

```
[local]Redback(config)#forward policy GeneralPolicy
[local]Redback(config-policy-frwd)#mirror destination DroppedTraffic dropped sampling 3000
[local]Redback(config-policy-frwd)#access-group PBR_ACL local
[local]Redback(config-policy-acl)#class WEB
[local]Redback(config-policy-acl-class)#redirect destination next-hop 100.1.1.2
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class UDP
[local]Redback(config-policy-acl-class)#mirror destination UdpTraffic forwarded
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class ICMP
[local]Redback(config-policy-acl-class)#drop
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class PIM
[local]Redback(config-policy-acl-class)#drop
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class IP
[local]Redback(config-policy-acl-class)#mirror destination IpTraffic all
```

The following configuration applies the policy to an incoming circuit and defines the output destinations:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface e1 local
[local]Redback(config-port)#forward output DroppedTraffic
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 6/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface normal_traffic local
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface incoming_traffic local
[local]Redback(config-port)#forward policy GeneralPolicy in
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p1 local
[local]Redback(config-port)#exit
```

```
[local]Redback(config)#port pos 13/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p2 local
[local]Redback(config-port)#forward output UdpTraffic
[local]Redback(config-port)#exit
[local]Redback(config)#port pos 13/3
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface p3 local
[local]Redback(config-port)#forward output IpTraffic
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure forward policies. The commands are presented in alphabetical order.

|                          |                                      |
|--------------------------|--------------------------------------|
| <b>drop</b>              | <b>forward policy out</b>            |
| <b>forward output</b>    | <b>mirror destination</b>            |
| <b>forward policy</b>    | <b>redirect destination circuit</b>  |
| <b>forward policy in</b> | <b>redirect destination next-hop</b> |

**Note** The **redirect destination local** command is used only for HTTP redirect and is described in Chapter 7, “HTTP Redirect Configuration.”

# drop

**drop**  
**no drop**

## Purpose

Drops incoming packets for this forward policy or this policy access control list (ACL) class.

## Command Mode

forward policy configuration  
policy ACL class configuration

## Syntax Description

This command has no keywords or arguments.

## Default

Packets are not dropped.

## Usage Guidelines

Use the **drop** command to drop incoming packets according to the applied forward policy.

Use the **no** form of this command to disable the dropping of packets.

## Examples

The following example configures the DropPolicy policy, which drops incoming packets that belong to the classes ICMP and PIM:

```
[local]Redback#config
[local]Redback(config)#forward policy DropPolicy
[local]Redback(config-policy-frwd)#access-group PBR_Drop_ACL local
[local]Redback(config-policy-acl)#class ICMP
[local]Redback(config-policy-acl-class)#drop
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class PIM
[local]Redback(config-policy-acl-class)#drop
```

The following example configures the DropAllPolicy policy, which drops all incoming packets on the circuit:

```
[local]Redback#config
[local]Redback(config)#forward policy DropAllPolicy
[local]Redback(config-policy-frwd)#drop
```



## Related Commands

forward policy in

## forward output

**forward output** *dest-name*

**no forward output** *dest-name*

### Purpose

Specifies a circuit as the output destination for mirrored or redirected traffic.

### Command Mode

ATM PVC configuration  
Frame Relay PVC configuration  
GRE tunnel configuration  
port configuration

### Syntax Description

*dest-name*                      Output destination name for mirrored or redirected traffic.

### Default

No output destination for mirrored or redirected traffic is specified.

### Usage Guidelines

Use the **forward output** command to specify a circuit as the output destination for mirrored or redirected traffic.

**Note** You can use an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), an Ethernet port, a Frame Relay PVC, a Generic Routing Encapsulation (GRE) tunnel, or a Packet over SONET/SDH (POS) port as the output destination for mirrored or redirected traffic.

You cannot use the circuit referencing the forward policy as the forward output port. The selected circuit should be different from the circuit used for the traffic being mirrored or redirected.

Use the **no** form of this command to remove the circuit as the output destination for mirrored or redirected traffic.

### Examples

The following example configures two forward outputs, snoop1 and snoop2, on Ethernet ports, and one forward output, snoop\_gre, on a GRE tunnel circuit:

```
[local]Redback(config)#port ethernet 5/12
[local]Redback(config-port)#forward output snoop1
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#forward output snoop2
[local]Redback(config-port)#exit
```

```
[local]Redback(config)#tunnel map  
[local]Redback(config-tunnel-map)#gre-tunnel tunnel01 local key 1  
[local]Redback(config-gre-tunnel)#forward output snoop_gre
```

## Related Commands

**forward policy in**  
**forward policy out**  
**mirror destination**  
**redirect destination circuit**  
**redirect destination next-hop**

## forward policy

**forward policy** *name*

**no forward policy** *name*

### Purpose

Configures a forward policy name and enters forward policy configuration mode.

### Command Mode

global configuration

### Syntax Description

*name* Forward policy name.

### Default

No forward policy is configured.

### Usage Guidelines

Use the **forward policy** command to configure a forward policy name and to enter forward policy configuration mode.

A forward policy can contain a combination of mirror, redirect, and drop functionalities.

Use the **no** form of this command to remove the forward policy from the configuration.

### Examples

The following example configures the forward policy, `MirrorPolicy`, and enters forward policy configuration mode:

```
[ local ]Redback(config)#forward policy MirrorPolicy
[ local ]Redback(config-policy-frwd)#
```

### Related Commands

**drop**

**mirror destination**

**redirect destination circuit**

**redirect destination local**

**redirect destination next-hop**

## forward policy in

**forward policy** *name* **in** [**acl-counters**]

**no forward policy** *name* **in** [**acl-counters**]

### Purpose

Attaches a forward policy to incoming traffic on a circuit, port, or subscriber record.

### Command Mode

ATM DS-3 configuration  
ATM OC configuration  
ATM PVC configuration  
dot1q PVC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
Frame Relay PVC configuration  
port configuration  
subscriber configuration

### Syntax Description

|                     |                                                                                 |
|---------------------|---------------------------------------------------------------------------------|
| <i>name</i>         | Forward policy name.                                                            |
| <b>acl-counters</b> | Optional. Enables per-rule statistics for the policy access control list (ACL). |

### Default

No policy is attached.

### Usage Guidelines

Use the **forward policy in** command to attach a forward policy to incoming traffic on a circuit, port, or subscriber record.

Use the **acl-counters** keyword to track the number of packets mirrored, redirected, or dropped.

Use the **no** form of this command to remove a forward policy from a circuit, port, or subscriber record.

### Examples

The following example attaches the forward policy, `MirrorPolicy`, to incoming traffic on a Packet over SONET/SDH (POS) port:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#forward policy MirrorPolicy in
```

## Related Commands

**drop**  
**forward policy out**  
**mirror destination**  
**redirect destination circuit**  
**redirect destination next-hop**

## forward policy out

**forward policy** *name* **out** [**acl-counters**]

**no forward policy** *name* **out** [**acl-counters**]

### Purpose

Attaches a forward policy that mirrors traffic to outgoing traffic on a circuit, port, or subscriber record.

### Command Mode

ATM DS-3 configuration  
ATM OC-configuration  
ATM PVC configuration  
dot1q PVC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
Frame Relay PVC configuration  
port configuration  
subscriber configuration

### Syntax Description

|                     |                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>         | Forward policy name.                                                                                                                        |
| <b>acl-counters</b> | Optional. Keeps track of the number of packets that are mirrored when a policy access control list (ACL) is attached to the forward policy. |

### Default

No policy is attached.

### Usage Guidelines

Use the **forward policy out** command to attach a forward policy that mirrors traffic to outgoing traffic on a circuit, port, or subscriber record.

**Note** You can apply a forward policy with redirect or drop functions only to incoming traffic, which requires that you use the **forward policy in** command.

Use the **no** form of this command to remove a forward policy from a circuit, port, or subscriber record.

### Examples

The following example attaches the forward policy, `MirrorPolicy`, to outgoing traffic on an ATM port:

```
[local]Redback(config)#port atm 13/1  
[local]Redback(config-atm-oc)#forward policy MirrorPolicy out
```

## Related Commands

**drop**  
**forward output**  
**forward policy**  
**forward policy in**  
**mirror destination**  
**redirect destination circuit**



## mirror destination

**mirror destination** *dest-name* { **all** | **dropped** | **forwarded** } [**header-only**] [**sampling** *interval*]

**no mirror destination**

### Purpose

Enables the mirroring of packets to an output destination.

### Command Mode

forward policy configuration  
policy ACL class configuration

### Syntax Description

|                                 |                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>dest-name</i>                | Output destination name for mirrored traffic.                                                                                               |
| <b>all</b>                      | Mirrors all traffic.                                                                                                                        |
| <b>dropped</b>                  | Mirrors only dropped packets. Packets dropped by IP checksums or by ACLs are not mirrored.                                                  |
| <b>forwarded</b>                | Mirrors only forwarded packets.                                                                                                             |
| <b>header-only</b>              | Optional. Mirrors only packet headers.                                                                                                      |
| <b>sampling</b> <i>interval</i> | Optional. Sampling interval. Periodically (as opposed to continuously) mirrors traffic. The sampling interval is specified in milliseconds. |

### Default

Packets are not mirrored.

### Usage Guidelines

Use the **mirror destination** command to enable the mirroring of packets to an output destination.

Mirrored output can be bound only to a major circuit, such as an Ethernet, Gigabit Ethernet, or Packet over SONET/SDH (POS) circuit. Mirrored output can not be obtained on virtual containers (VCs) or 802.1Q virtual LANs (VLANs); however, it can be obtained on Generic Routing Encapsulation (GRE) circuits.

Use the **no** form of this command to disable the mirroring of packets to an output destination.

### Examples

The following example configures a policy, `MirrorPolicy`, which mirrors dropped packets every 3 seconds (3000 milliseconds) to the output destination, `DroppedTraffic`:

```
[local]Redback#config
[local]Redback(config)#forward policy MirrorPolicy
[local]Redback(config-policy-frwd)#mirror destination DroppedTraffic dropped sampling 3000
```

## Related Commands

**forward output**  
**forward policy in**  
**forward policy out**

## redirect destination circuit

**redirect destination circuit** *dest-name*

**no redirect destination**

### Purpose

Redirects packets to an output destination.

### Command Mode

forward policy configuration

policy ACL class configuration

### Syntax Description

|                  |                                            |
|------------------|--------------------------------------------|
| <i>dest-name</i> | Output destination for redirected traffic. |
|------------------|--------------------------------------------|

### Default

Packets are not redirected.

### Usage Guidelines

Use the **redirect destination circuit** command to redirect packets to an output destination.

Use the **forward output** command (in ATM PVC, Frame Relay PVC, GRE tunnel, or port configuration mode) to configure the output destination.

Use the **no** form of this command to disable the redirecting of packets.

### Examples

The following example redirects traffic to the output destination circuit, OD15:

```
[local]Redback#config
[local]Redback(config)#forward policy RedirectPolicy
[local]Redback(config-policy-frwd)#redirect destination circuit OD15
```

### Related Commands

**forward output**

**forward policy in**

**redirect destination local**

**redirect destination next-hop**

## redirect destination next-hop

**redirect destination next-hop** {*ip-addr...* | **default**}

**no redirect destination**

### Purpose

Redirects packets to the specified IP address or to the packets' default destination IP address per the routing table.

### Command Mode

forward policy configuration  
policy ACL class configuration

### Syntax Description

|                   |                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr...</i> | One to eight next-hop IP addresses in order of priority. Each entry in the list is an IP address in the form <i>A.B.C.D</i> .                                                                               |
| <b>default</b>    | Specifies that the packet's destination IP address should be used to forward the packet according to the routing table. When the <b>default</b> keyword is active, the packet is routed and not redirected. |

### Default

Packets are not redirected.

### Usage Guidelines

Use the **redirect destination next-hop** command to redirect packets to the specified IP address or to the packets' default destination IP address per the routing table.

If an address is unreachable, then the next lower priority address is tried. From time to time, the system will try to return to the highest priority entry available. The **default** keyword can be used in the next-hop list instead of an IP address to indicate that the destination IP address from the packet should be used when all higher priority next hops are unreachable. The **default** keyword can be first in the list, which means redirecting packets only when the normal route is unreachable.

**Note** To modify the list of next hop entries, you must re-enter the entire **redirect destination next-hop** command.

Use the **no** form of this command to disable the redirecting of packets.

## Examples

The following example redirects traffic to the next-hop IP address, 10.1.1.1. If that address is unreachable, the SmartEdge OS redirects traffic to the next-hop IP address, 10.1.2.1. If both addresses are unreachable, traffic is routed normally.

```
[local]Redback#config  
[local]Redback(config)#forward policy RedirectPolicy  
[local]Redback(config-policy-frwd)#redirect destination next-hop 10.1.1.1 10.1.2.1 default
```

The following example routes traffic normally. If the route is unavailable, traffic is redirected to the next-hop IP address, 10.1.1.1:

```
[local]Redback#config  
[local]Redback(config)#forward policy RedirectPolicy  
[local]Redback(config-policy-frwd)#redirect destination next-hop default 10.1.1.1
```

The following example redirects traffic to the next-hop IP address, 192.1.1.1. If that address is unreachable, the SmartEdge OS attempts to redirect traffic to the next-hop IP address, 10.1.1.1. If both addresses are unreachable, traffic is dropped.

```
[local]Redback#config  
[local]Redback(config)#forward policy RedirectPolicy  
[local]Redback(config-policy-frwd)#redirect destination next-hop 192.1.1.1 10.1.1.1
```

## Related Commands

- forward output**
- forward policy in**
- redirect destination circuit**
- redirect destination local**



# NAT Policy Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS Network Address Translation (NAT) policy features.

For information about the tasks and commands used to monitor, troubleshoot, and administer NAT policies, see the “NAT Policy Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

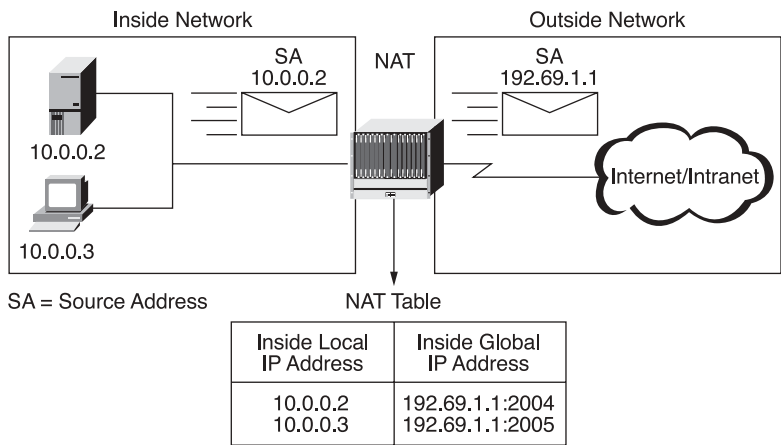
Through NAT, hosts using unregistered IP addresses on an internal, private network can connect to hosts on the Internet, and conversely. NAT translates the private (not globally unique) addresses in the internal network into public IP addresses before packets are forwarded onto another network. Network Address and Port Translation (NAPT) translates a private network and its Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port on the internal network into a public address and its TCP/UDP ports. By using port multiplexing, NAPT enables multiple hosts on a private network to simultaneously access remote networks through a single IP address.

NAT policies can contain a combination of static and dynamic translation actions as well as drop and ignore actions, and can be applied to all packets traveling across a circuit, or to a particular class of packets using policy access control list (ACL). The default NAT policy action is drop.

**Note** NAT policies are not supported for subscriber sessions that use the Layer 2 Tunneling Protocol (L2TP) and that are terminated at the SmartEdge router when it is acting as an L2TP network server (LNS). If you inadvertently apply a NAT policy to such a subscriber, the session comes up because the policy has no effect on it.

Figure 10-1 illustrates how NAT translates private source IP addresses to public addresses.

**Figure 10-1 NAT Translation**



0799

The SmartEdge OS implementation of NAT supports traditional NAT. In a traditional NAT, sessions are unidirectional, outbound from the private network. Sessions in the opposite direction may be allowed on an exception basis, using static address maps for preselected hosts. It is assumed that NAT policies are applied on private interfaces only because applying them on public interfaces would profoundly affect performance.

**Note** In this chapter, the terms, incoming and outgoing, refer to the direction of the packets passing through the interface. The terms, outbound and inbound, refer to the direction of the packet flow from the private network to the public network, and from the public network to the private network, respectively.

The SmartEdge OS implementation of NAT is described in the following sections:

- Static Translation
- Dynamic Translation
- Policy ACLs
- NAT DMZ
- Summary

## Static Translation

With static translation, the private IP addresses and TCP or UDP ports and the NAT addresses and the ports to which they are translated are fixed numbers.

**Note** When just the IP address is translated, static NAT is referred to as basic static NAT. Static NAT includes both basic static NAT and static NAPT.



## Dynamic Translation

With dynamic translation, the SmartEdge OS translates the private IP addresses and TCP or UDP ports to the NAT addresses and ports. At runtime, the SmartEdge OS selects the NAT addresses and ports from a pool of global IP addresses (referred to as a NAT pool). With dynamic translation, you can also modify the period after which translations time out.

NAPT also supports dynamic translation of subsets of TCP/UDP ports, referred to as port blocks. The port number space of the TCP/UDP ports is divided into 16 port blocks, numbered 0 to 15; each port block consists of 4,096 port numbers. Port block granularity allows the sharing of a single IP address between NAT pools, and thus between NAT policies and traffic cards, with each pool having the IP address with a unique subset of TCP/UDP port blocks assigned to it.

**Note** When just the IP address is translated, dynamic NAT is referred to as basic dynamic NAT. Dynamic NAT includes both basic dynamic NAT and dynamic NAPT.

## Policy ACLs

Policy access control lists (ACLs) configure classes of packets; you can apply an IP ACL to a NAT policy so that distinct actions can be applied to packets traveling across the same circuit.

When you include the **drop**, **ignore**, **pool**, and **timeout** commands (in NAT policy configuration mode) in a NAT policy, the specified action is applied to all packets traveling across the interface or subscriber circuit or, if an ACL is referenced, to packets that do not belong to the classes specified by the ACL. These classes are referred to as belonging to the default class.

When you include the **drop**, **ignore**, **pool**, and **timeout** commands (in policy ACL class configuration mode) in a policy ACL, the specified action is applied only to packets belonging to classes specified by the ACL.

**Note** The **pool** and **timeout** commands apply only to dynamic NAT.

Each policy ACL supports up to eight unique classes. You can classify a packet according to its IP precedence value, protocol number, IP source and destination address, Internet Control Management Protocol (ICMP) attributes, Internet Group Management Protocol (IGMP) attributes, Transmission Control Protocol (TCP) attributes, and User Datagram Protocol (UDP) attributes. For more information about policy ACLs, see Chapter 8, “ACL Configuration.”

## NAT DMZ

The SmartEdge OS also provides support for the demilitarized zone (DMZ) feature in NAT policies. You can configure a DMZ rule in a NAT policy to translate traffic returning to the SmartEdge router that does not satisfy any of the conditions for static or dynamic NAT translations that you have specified in that NAT policy. The basic NAT translation specified by the DMZ rule changes the destination IP address of the packet to a fixed private IP address of a DMZ host server without changing the TCP/UDP port number.

Three types of applications might require a DMZ host server:

- You use your own tools to do extensive logging and analysis of the packets that would be dropped by the NAT policy.
- You do not know the exact TCP/UDP port numbers, or there are too many ports, that need to be opened by static NAPT rules to allow access to applications.

- You need a workaround for applications that do not work with NAPT, because they use protocols other than UDP or TCP, or require IP packet fragmentation.

The following differences apply to a private network with a DMZ host server:

- A DMZ rule in a NAT policy does not affect non-DMZ hosts on the internal network that use static or dynamic NAPT, except that returning traffic for dynamic UDP sessions are now subject to source IP address verification.
- Non-DMZ hosts can use basic static or basic dynamic NAT, although such configurations might not seem practical.
- The DMZ host server cannot use basic static NAT basic dynamic NAT, and dynamic NAPT, but can still use static NAPT.

## Summary

The order in which the conditions in a NAT policy are checked to determine the action for a packet is as follows:

1. The conditions set by the policy static translations.
2. The conditions set by the policy ACL.
3. If the conditions in step 1 and step 2 are not satisfied, the action for the packet is determined by the default class action, if the policy ACL exists, or by the NAT policy action.

For more information about NAT, see RFC 3022, *Traditional IP Network Address Translator (NAT)* and RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure NAT policies, perform the tasks described in the following sections:

- Configure a NAT Policy with Static Translations
- Configure a NAT Policy with a DMZ Host Server
- Configure a NAT Policy with Dynamic Translations
- Apply a Policy ACL to a NAT Policy

## Configure a NAT Policy with Static Translations

To configure a NAT policy with static translations, perform the tasks described in Table 10-1.

**Table 10-1 Configure a NAT Policy with Traditional Static Translations**

| #  | Task                                                                                                                                                                                                                                | Root Command                                          | Notes                                                                                                                                                                                                                                                                              |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Configure a NAT policy name and access NAT policy configuration mode.                                                                                                                                                               | <b>nat policy</b>                                     | Enter this command in context configuration mode.                                                                                                                                                                                                                                  |
| 2. | Translate the source IP address for incoming packets on the interface or the subscriber circuit to which the NAT policy will be attached in the private network.                                                                    | <b>ip static in</b>                                   | Enter this command in NAT policy configuration mode.<br>The destination IP address of incoming packets is translated in the reverse direction.<br>Use the optional <b>tcp</b> or <b>udp</b> keyword to translate the source address and source port number of the TCP/UDP packets. |
| 3. | Translate the source IP address for outgoing packets on the interface or the subscriber circuit to which the NAT policy will be attached in the private network.                                                                    | <b>ip static out</b>                                  | Enter this command in NAT policy configuration mode.<br>The destination IP address of incoming packets is translated in the reverse direction.                                                                                                                                     |
| 4. | Translate the destination IP address for those inbound packets (on the interface or subscriber circuit to which the NAT policy will be attached) that do not satisfy any condition for static or dynamic translation in the policy. | <b>ip dmz</b>                                         | Enter this command in NAT policy configuration mode.<br>The source IP address is translated in the outbound direction.                                                                                                                                                             |
| 5. | Optional. Apply a policy ACL.                                                                                                                                                                                                       | See the “Apply a Policy ACL to a NAT Policy” section. |                                                                                                                                                                                                                                                                                    |
| 6. | Attach the policy to an interface or subscriber, using one of the following tasks:                                                                                                                                                  |                                                       |                                                                                                                                                                                                                                                                                    |
|    | • To an interface.                                                                                                                                                                                                                  | <b>ip nat</b>                                         | Enter this command in interface configuration mode.                                                                                                                                                                                                                                |
|    | • To a subscriber record, named profile, or default profile.                                                                                                                                                                        | <b>nat policy-name</b>                                | Enter this command in subscriber configuration mode.                                                                                                                                                                                                                               |

**Note** For information about configuring interfaces and subscribers, see the “Interface Configuration” chapter and the “Subscriber Configuration” chapter, respectively, in the *Basic System Configuration Guide* for the SmartEdge OS.

## Configure a NAT Policy with a DMZ Host Server

To configure a NAT policy with a DMZ host server, perform the tasks described in Table 10-2.

**Table 10-2 Configure a NAT Policy with a DMZ Host Server**

| #  | Task                                                                                                                                                                                                                    | Root Command      | Notes                                                                                                                                          |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Configure a NAT policy name and access NAT policy configuration mode.                                                                                                                                                   | <b>nat policy</b> | Enter this command in context configuration mode.                                                                                              |
| 2. | Translate the destination IP address for those outgoing packets (on the interface or subscriber circuit to which the NAT policy will be attached) that do not satisfy any of the static or dynamic rules in the policy. | <b>ip dmz</b>     | Enter this command in NAT policy configuration mode.<br>The destination IP address of incoming packets is translated in the reverse direction. |

**Table 10-2 Configure a NAT Policy with a DMZ Host Server** (*continued*)

| #  | Task                                                                               | Root Command           | Notes                                                |
|----|------------------------------------------------------------------------------------|------------------------|------------------------------------------------------|
| 3. | Attach the policy to an interface or subscriber, using one of the following tasks: |                        |                                                      |
|    | • To an interface.                                                                 | <b>ip nat</b>          | Enter this command in interface configuration mode.  |
|    | • To a subscriber record, named profile, or default profile.                       | <b>nat policy-name</b> | Enter this command in subscriber configuration mode. |

## Configure a NAT Policy with Dynamic Translations

To configure a NAT policy with dynamic translations, perform the tasks described in Table 10-3; enter all commands in NAT policy configuration mode, unless otherwise noted.

**Table 10-3 Configure a NAT Policy with Dynamic Translations**

| #  | Task                                                                                                                     | Root Command                                          | Notes                                                                                                                                                                                                                                                                      |
|----|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select a NAT pool and access NAT pool configuration mode.                                                      | <b>ip nat pool</b>                                    | Enter this command in context configuration mode.<br>Use the <b>napt</b> keyword to indicate that the addresses associated with the pool will be used for NAPT policies.<br>Use the <b>multibind</b> keyword to enable the NAT pool to be applied to multibind interfaces. |
| 2. | Configure the IP address, range of IP addresses, or the IP address with a range of TCP/UDP port blocks for the NAT pool. | <b>address</b>                                        | Enter this command in NAT pool configuration mode.<br>Enter this command multiple times to configure several IP addresses, address ranges, and IP addresses with port blocks for the NAT pool.                                                                             |
| 3. | Create or select a policy and access NAT policy configuration mode.                                                      | <b>nat policy</b>                                     | Enter this command in context configuration mode.                                                                                                                                                                                                                          |
| 4. | Specify the action to take on packets not associated with a class with one of the following tasks:                       |                                                       | Any of these actions is applied to packets not associated with a class if a policy ACL is applied to this NAT policy.                                                                                                                                                      |
|    | • Translate packets using the pool of IP addresses (created in step 1).                                                  | <b>pool</b>                                           |                                                                                                                                                                                                                                                                            |
|    | • Drop packets.                                                                                                          | <b>drop</b>                                           | Dropped packets are not affected by the policy.                                                                                                                                                                                                                            |
|    | • Ignore packets.                                                                                                        | <b>ignore</b>                                         | Ignored packets are not affected by the policy.                                                                                                                                                                                                                            |
| 5. | Optional. Modify the period after which translations time out.                                                           | <b>timeout</b>                                        | Enter this command only if you have specified the <b>pool</b> command (in step 4). This timeout is used for packets not associated with a class, if a policy ACL is applied to this NAT policy.                                                                            |
| 6. | Optional. Apply a policy ACL to this policy.                                                                             | See the “Apply a Policy ACL to a NAT Policy” section. |                                                                                                                                                                                                                                                                            |
| 7. | Attach the NAT or NATP policy to an interface or subscriber, using one of the following tasks:                           |                                                       |                                                                                                                                                                                                                                                                            |
|    | • To an interface.                                                                                                       | <b>ip nat</b>                                         | Enter this command in interface configuration mode.                                                                                                                                                                                                                        |
|    | • To a subscriber record, named profile, or default profile.                                                             | <b>nat policy-name</b>                                | Enter this command in subscriber configuration mode.                                                                                                                                                                                                                       |

## Apply a Policy ACL to a NAT Policy

To apply a policy ACL to packets associated with a dynamic NAT policy and complete the configuration of the policy, perform the tasks described in Table 10-4; enter all commands in policy ACL class configuration mode, unless otherwise noted.

**Table 10-4 Apply a Policy ACL to a NAT Policy**

| #  | Task                                                                                             | Root Command        | Notes                                                                                                                                                             |
|----|--------------------------------------------------------------------------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Apply a policy ACL to a dynamic NAT policy and access policy ACL configuration mode.             | <b>access-group</b> | Enter this command in NAT policy configuration mode.                                                                                                              |
| 2. | Specify a class and access policy ACL class configuration mode.                                  | <b>class</b>        | Enter this command in policy ACL configuration mode.<br><br>The class name must match the name of a class specified in a <b>permit</b> command in the policy ACL. |
| 3. | Specify the action to take on packets associated with the class with one of the following tasks: |                     | Enter any of these commands in policy ACL class configuration mode.                                                                                               |
|    | • Translate packets using the pool of IP addresses.                                              | <b>pool</b>         |                                                                                                                                                                   |
|    | • Drop packets associated with the class.                                                        | <b>drop</b>         | Dropped packets are not affected by the policy.                                                                                                                   |
|    | • Ignore packets associated with the class.                                                      | <b>ignore</b>       | Ignored packets are not affected by the policy.                                                                                                                   |
| 4. | Optional. Modify the period after which translations time out.                                   | <b>timeout</b>      | Enter this command only if you have specified the <b>pool</b> command (in step 3). Enter this command in policy ACL class configuration mode.                     |

## Configuration Examples

This section provides configuration examples for:

- NAT Policy with Static Translation
- NAT Policy with Static NAPT Translation
- NAT Policy with Static Translation and a DMZ Host Server
- NAT Policy with Dynamic Translation and an Ignore Action
- NAT Policy with Dynamic NAPT Translation and a Drop Action
- NAT Policy with Static and Dynamic Translations

### NAT Policy with Static Translation

The following example configures a NAT policy with static translations:

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in source 10.1.1.3 100.1.1.3
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos2
[local]Redback(config-if)#ip nat p2
```

## NAT Policy with Static NAPT Translation

The following example configures a static NAPT policy:

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in tcp source 10.1.1.3 80 100.1.1.3 8080
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos2
[local]Redback(config-if)#ip nat p2
```

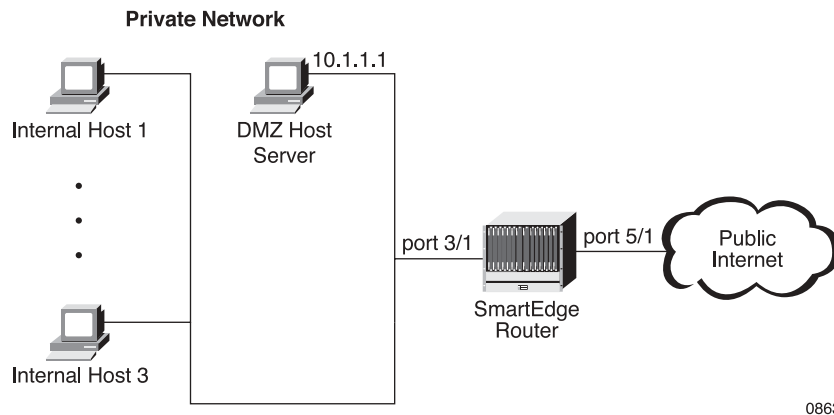
## NAT Policy with Static Translation and a DMZ Host Server

The following example configures a NAT policy with static translation, two internal hosts, and a DMZ host server:

```
!Configure context, NAT policy, and interface for private network
[local]Redback(config)#context local
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip dmz source 10.1.1.1 100.1.1.1 context local
[local]Redback(config-policy-nat)#ip static in source 10.1.1.2 100.1.1.2
[local]Redback(config-policy-nat)#ip static in source 10.1.1.3 100.1.1.3
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface if-private
[local]Redback(config-if)#ip address 10.1.1.1/24
[local]Redback(config-if)#ip nat p2
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
!Configure context, NAT policy, and interface for public network
[local]Redback(config)#context public
[local]Redback(config-ctx)#interface if-public
[local]Redback(config-if)#ip address 100.1.1.1/24
!Configure an Ethernet port for the private network
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#bind interface if-private local
[local]Redback(config-port)#no shutdown
!Configure an Ethernet port for the public network
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#bind interface if-public public
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#exit
[local]Redback(config)#
```

Figure 10-2 illustrates the network configuration for the example.

Figure 10-2 Private Network with NAT DMZ Host Server



0863

## NAT Policy with Dynamic Translation and an Ignore Action

The following example creates a policy ACL and applies it to a NAT policy with dynamic translations in which all packets except those classified as CLASS3 are ignored (that is, the NAT policy is not applied to them). All source IP addresses for incoming packets classified as CLASS3 are translated using IP addresses from the pool\_dyn pool.

```
!Create the NAT pool
[local]Redback(config-ctx)#ip nat pool pool_dyn
[local]Redback(config-nat-pool)#address 11.11.11.0/24
[local]Redback(config-nat-pool)#exit
!Create the policy ACL
[local]Redback(config-ctx)#policy access-list NAT-ACL
[local]Redback(config-access-list)#seq 10 permit ip 10.10.10.0 0.0.0.255 class CLASS3
[local]Redback(config-access-list)#exit
!Create the NAT policy and apply the policy ACL
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-nat-pool)#ignore
[local]Redback(config-nat-pool)#access-group NAT-ACL
[local]Redback(config-policy-acl)#class CLASS3
[local]Redback(config-policy-acl-class)#pool pool_dyn local
```

## NAT Policy with Dynamic NAPT Translation and a Drop Action

The following example configures a NAPT policy with dynamic translations in which all packets, except those classified as CLASS3, are dropped. Source IP addresses and their TCP/UDP ports for packets classified as CLASS3 are translated using the IP address and its TCP/UDP port blocks 1 to 15 from the pool\_dyn\_napt pool.

```
[local]Redback(config-ctx)#ip nat pool pool_dyn_napt napt
[local]Redback(config-nat-pool)#address 11.11.11.1/32 port-block 1 to 15
[local]Redback(config-nat-pool)#exit
```

```
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-policy-nat)#drop
[local]Redback(config-policy-nat)#access-group NAT_ACL
[local]Redback(config-policy-acl)#class CLASS3
[local]Redback(config-policy-acl-class)#pool pool_dyn_napt local
```

## NAT Policy with Static and Dynamic Translations

The following example configures a NAT policy that uses a combination of static and dynamic, basic NAT and NAPT translations and applies a policy ACL:

```
[local]Redback(config-ctx)#ip nat pool pool_dyn
[local]Redback(config-nat-pool)#address 100.1.2.0/24
[local]Redback(config-nat-pool)#exit
[local]Redback(config-ctx)#ip nat pool pool_dyn_napt napt
[local]Redback(config-nat-pool)#address 100.1.1.2/32 port-block 1
[local]Redback(config-nat-pool)#exit
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-policy-nat)#pool pool_dyn local
[local]Redback(config-policy-nat)#access-group NAT_ACL
[local]Redback(config-policy-acl)#class CLASS3
[local]Redback(config-policy-acl-class)#pool pool_dyn_napt local
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#exit
[local]Redback(config-policy-nat)#ip static in tcp source 10.1.1.2 80 100.1.1.2 8080
[local]Redback(config-policy-nat)#ip static in source 10.1.1.3 100.1.1.3
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure NAT policies. The commands are presented in alphabetical order.

|                    |                        |
|--------------------|------------------------|
| <b>address</b>     | <b>ip static in</b>    |
| <b>drop</b>        | <b>ip static out</b>   |
| <b>ignore</b>      | <b>nat policy</b>      |
| <b>ip dmz</b>      | <b>nat policy-name</b> |
| <b>ip nat</b>      | <b>pool</b>            |
| <b>ip nat pool</b> | <b>timeout</b>         |



## address

```
address {ip-addr netmask | ip-addr/prefix-length | start-ip-addr to end-ip-addr | ip-addr/32  
           port-block start-port-block [to end-port-block]}  
no address {ip-addr netmask | ip-addr/prefix-length | start-ip-addr to end-ip-addr}
```

### Purpose

Assigns an IP address, a range of IP addresses, or an IP address with one or more blocks of Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports to the Network Address Translation (NAT) pool.

### Command Mode

NAT pool configuration

### Syntax Description

|                                           |                                                                                                                                                                                                |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr netmask</i>                    | IP address and subnet mask.                                                                                                                                                                    |
| <i>ip-addr/prefix-length</i>              | IP address and prefix length.                                                                                                                                                                  |
| <i>start-ip-addr to end-ip-addr</i>       | Starting IP address to ending IP address.                                                                                                                                                      |
| <i>ip-addr/32</i>                         | IP address and prefix length when specifying one or more blocks of TCP/UDP port numbers.                                                                                                       |
| <b>port-block</b> <i>start-port-block</i> | Starting port block number. The range of values is 0 to 15.                                                                                                                                    |
| <b>to</b> <i>end-port-block</i>           | Optional. Ending port-block number. If not entered, assigns only the TCP/UDP port numbers in the port block specified by the <i>start-port-block</i> argument. The range of values is 1 to 15. |

### Default

All TCP/UDP port numbers for the IP address are assigned to the NAT pool.

### Usage Guidelines

Use the **address** command to assign the IP address and subnet mask, a range of IP addresses, or an IP address with a range of TCP/UDP ports that will be included in the NAT pool. The TCP/UDP port number space is divided into 16 blocks. Each block contains 4,096 sequential numbers. Blocks are numbered from 0 to 15. If you specify one or more blocks of TCP/UDP ports, you must specify 32 as the prefix length.

You can enter this command multiple times to assign multiple IP addresses, ranges of IP addresses, and an IP address with TCP/UDP port blocks to a NAT pool.

Use the **no** form of this command to remove IP addresses from the NAT pool. If you enter the **no** form with an IP address that was configured with the **port-block** keyword, the IP address and all its configured port blocks are removed from the NAT pool.

### Examples

The following example configures the NAT pool, NAT-1, and fills the pool with the IP address, 171.71.71.1, with all its TCP/UDP ports and the IP address, 171.71.72.2, with port blocks 1 to 3:

```
[local]Redback(config)#context ISP  
[local]Redback(config-ctx)#ip nat pool NAT-1 napt  
[local]Redback(config-nat-pool)#address 171.71.71.1/32  
[local]Redback(config-nat-pool)#address 171.71.72.2/32 port-block 1 to 3
```

### Related Commands

```
ip nat pool  
pool
```

# drop

**drop**

## Purpose

Drops all packets or classes of packets associated with the Network Address Translation (NAT) policy.

## Command Mode

NAT policy configuration  
policy ACL class configuration

## Syntax Description

This command has no keywords or arguments.

## Default

If no action is configured for the NAT policy, by default, packets are dropped.

## Usage Guidelines

Use the **drop** command to drop all packets or classes of packets associated with the NAT policy.

## Examples

The following example configures the NAT-1 policy and applies the NAT-ACL-1 ACL to it. Packets that are classified as NAT-CLASS-1 will be dropped. All other packets, except those explicitly defined by the static rule, will be ignored.

```
[local]Redback(config)#context CUSTOMER
[local]Redback(config-ctx)#nat policy NAT-1
[local]Redback(config-policy-nat)#ignore
[local]Redback(config-policy-nat)#ip static in source 10.0.0.1 171.71.71.1
[local]Redback(config-policy-nat)#access-group NAT-ACL-1
[local]Redback(config-policy-acl)#class NAT-CLASS-1
[local]Redback(config-policy-acl-class)#drop
```

## Related Commands

**ignore**  
**pool**  
**timeout**

# ignore

**ignore**

## Purpose

Removes the application of the Network Address Translation (NAT) policy to all packets, or classes of packets, traveling across circuits attached to the interface or subscriber to which the NAT policy is applied.

## Command Mode

NAT policy configuration  
policy ACL class configuration

## Syntax Description

This command has no keywords or arguments.

## Default

If no action is configured for the NAT policy, by default, packets are dropped.

## Usage Guidelines

Use the **ignore** command to remove the application of the NAT policy to all packets, or classes of packets, traveling across circuits attached to the interface or subscriber to which the NAT policy is applied.

## Examples

The following example configures the NAT - 2 policy and applies the NAT - ACL - 2 access control list (ACL) to it. Packets that are classified as NAT - CLASS - 2 will be ignored; the policy will not be applied to these packets. All other packets, except those defined in the static rule, will be dropped.

```
[local]Redback(config)#context CUSTOMER
[local]Redback(config-ctx)#nat policy NAT-2
[local]Redback(config-policy-nat)#ip static in source 10.0.0.1 171.71.71.1
[local]Redback(config-policy-nat)#access-group NAT-ACL-2
[local]Redback(config-policy-acl)#class NAT-CLASS-2
[local]Redback(config-policy-acl-class)#ignore
```

## Related Commands

**drop**  
**pool**  
**timeout**

## ip dmz

**ip dmz source** *ip-addr nat-addr context ctx-name*

**no ip dmz source** *ip-addr nat-addr context ctx-name*

### Purpose

Configures the source and Network Address Translation (NAT) IP addresses for a demilitarized zone (DMZ) host server.

### Command Mode

NAT policy configuration

### Syntax Description

|                                |                                                                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>source</b> <i>ip-addr</i>   | Original source IP address for the DMZ host server on the private network.                                                                                                  |
| <i>nat-addr</i>                | NAT address. The IP address of the DMZ host server on the public network to which the source IP address is mapped.                                                          |
| <b>context</b> <i>ctx-name</i> | Name of the context in which the NAT address of the DMZ host server is defined for the interface that is used to forward packets after the source IP address is translated. |

### Default

No DMZ host server is configured.

### Usage Guidelines

Use the **ip dmz** command to configure a DMZ host server.

Use the **no** form of this command to remove the DMZ host server from the configuration.

### Examples

The following example configures a DMZ host server with an internal network address, 10.1.1.1, and an external network address, 201.1.1.1, which are defined in the `local` context:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#nat policy policy1
[local]Redback(config-policy-nat)#ip dmz source 10.1.1.1 201.1.1.1 context local
```

### Related Commands

None

# ip nat

**ip nat** *pol-name*

**no ip nat** *pol-name*

## Purpose

Attaches a Network Address Translation (NAT) policy to packets received or transmitted on any circuit bound to the specified interface.

## Command Mode

interface configuration

## Syntax Description

*pol-name* NAT policy name.

## Default

None

## Usage Guidelines

Use the **ip nat** command to attach a NAT policy to packets received or transmitted on any circuit bound to the specified interface.

Use the **no** form of this command to remove the NAT policy from the interface.

## Examples

The following example translates an IP source address for the p1 NAT policy and applies the policy to packets traveling across the pos1 interface:

```
[local]Redback(config-ctx)#nat policy p1
[local]Redback(config-policy-nat)#ip static in source 10.1.2.3 32.32.32.32
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos1
[local]Redback(config-if)#ip nat p1
```

## Related Commands

**nat policy**

**nat policy-name**

## ip nat pool

```
ip nat pool pool-name [napt [multibind]]  
no ip nat pool pool-name [napt [multibind]]
```

### Purpose

Configures a Network Address Translation (NAT) pool name and enters NAT pool configuration mode.

### Command Mode

context configuration

### Syntax Description

|                  |                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| <i>pool-name</i> | NAT pool name.                                                                                                     |
| <b>napt</b>      | Optional. Enables support for translation of Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports. |
| <b>multibind</b> | Optional. Enables the NAT pool to be applied to multibind interfaces.                                              |

### Default

None

### Usage Guidelines

Use the **ip nat pool** command to configure a NAT pool name and to enter NAT pool configuration mode.

Use the **no** form of this command to remove a NAT pool.

### Examples

The following example configures the NAT pool, NAT-POOL-BASIC, with 14 IP addresses (171.71.71.4 to 171.71.71.7 and 171.71.71.101 to 171.71.71.110):

```
[local]Redback(config-ctx)#ip nat pool NAT-POOL-BASIC  
[local]Redback(config-nat-pool)#address 171.71.71.4 255.255.255.252  
[local]Redback(config-nat-pool)#address 171.71.71.101 to 171.71.71.110
```

### Related Commands

**address**  
**pool**

## ip static in

**ip static in** [**tcp** | **udp**] **source** *ip-addr* [*port*] *nat-addr* [*nat-port*] [**context** *ctx-name*]

**no ip static in** [**tcp** | **udp**] **source** *ip-addr* [*port*] *nat-addr* [*nat-port*] [**context** *ctx-name*]

### Purpose

Translates the source IP address in the private network, and optionally, Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports, of incoming packets on the interface to which the Network Address Translation (NAT) policy is attached. In the reverse direction, translates the destination IP address, and optionally, TCP/UDP ports, of outgoing packets on the interface.

### Command Mode

NAT policy configuration

### Syntax Description

|                                |                                                                                                                                                                                                            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tcp</b>                     | Optional. Indicates a TCP port.                                                                                                                                                                            |
| <b>udp</b>                     | Optional. Indicates a UDP port.                                                                                                                                                                            |
| <b>source</b>                  | Indicates the source information.                                                                                                                                                                          |
| <i>ip-addr</i>                 | Original source IP address.                                                                                                                                                                                |
| <i>port</i>                    | Optional. Original TCP or UDP source port number. The range of values is 1 to 65,535. Required when using the <b>tcp</b> or <b>udp</b> keyword.                                                            |
| <i>nat-addr</i>                | NAT address. The IP address to which the source IP address is mapped in the address translation table.                                                                                                     |
| <i>nat-port</i>                | Optional. TCP or UDP port number to which the source port number is mapped in the address translation table. The range of values is 1 to 65,535. Required when using the <b>tcp</b> or <b>udp</b> keyword. |
| <b>context</b> <i>ctx-name</i> | Optional. Context name. Required for intercontext forwarding of packets. Interfaces in the specified context are used to forward packets after addresses are translated.                                   |

### Default

If no action is configured for the NAT policy, by default, packets are dropped.

### Usage Guidelines

Use the **ip static in** command to translate the source IP address in the private network, and optionally, TCP/UDP ports, of incoming packets on the interface to which the NAT policy is attached. In the reverse direction, this command translates the destination IP address, and optionally, TCP/UDP ports, of outgoing packets on the interface.



Incoming packets with a source IP address that matches the *ip-addr* argument use the IP address specified with the *nat-addr* argument as their source IP address instead. In the opposite direction, outgoing packets with a destination IP address that matches the *nat-addr* argument use the *ip-addr* argument as the destination IP address.

If the *nat-addr* argument overlaps an IP address in a NAT pool, the static translation takes precedence.

Use the **no** form of this command to disable the translation of the source IP address and TCP/UDP ports.

## Examples

The following example translates the source IP address of packets received on the interface, *customer1*, to 2.2.2.2 when the original source address of the packets is 1.1.1.1. At the same time, the destination address of packets sent out the interface are translated to 1.1.1.1 when the original destination address of the packets is 2.2.2.2.

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in source 1.1.1.1 2.2.2.2
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface customer1
[local]Redback(config-if)#ip address 1.1.1.254/24
[local]Redback(config-if)#ip nat p2
```

## Related Commands

**ip static out**

## ip static out

**ip static out source** *ip-addr nat-addr*

**no ip static out source** *ip-addr nat-addr*

### Purpose

Translates the source IP address in the private network of outgoing packets on the interface to which the Network Address Translation (NAT) policy is applied, and in the reverse direction, translates the destination IP address of incoming packets on the interface.

### Command Mode

NAT policy configuration

### Syntax Description

|                 |                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------|
| <b>source</b>   | Indicates the source information.                                                                      |
| <i>ip-addr</i>  | Original source IP address.                                                                            |
| <i>nat-addr</i> | NAT address. The IP address to which the source IP address is mapped in the address translation table. |

### Default

If no action is configured for the NAT policy, packets are dropped.

### Usage Guidelines

Use the **ip static out** command to translate the source IP address in the private network of outgoing packets on the interface to which the NAT policy is applied, and in the reverse direction, to translate the destination IP address of incoming packets on the interface.

Outgoing packets with a source IP address that match the *ip-addr* argument use the IP address specified with the *nat-addr* argument as their source IP address instead. In the opposite direction, incoming packets with a destination IP address that matches the *nat-addr* argument use the *ip-addr* argument as the destination IP address.

Use the **no** form of this command to disable the translation of the IP address.

## Examples

The following example translates the IP source address of packets sent out the interface, pos1, to 10.30.40.50 when the original source address of the packets is 64.64.64.64. At the same time, the destination address of packets coming into the interface are translated to 64.64.64.64 when the destination address of the packets is 10.30.40.50.

```
[local]Redback(config-ctx)#nat policy p1
[local]Redback(config-policy-nat)#ip static out source 64.64.64.64 10.30.40.50
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos1
[local]Redback(config-if)#ip nat p1
```

## Related Commands

**ip static in**

## nat policy

**nat policy** *pol-name*

**no nat policy** *pol-name*

### Purpose

Configures a Network Address Translation (NAT) policy name and enters NAT policy configuration mode.

### Command Mode

context configuration

### Syntax Description

*pol-name* NAT policy name.

### Default

None

### Usage Guidelines

Use the **nat policy** command to configure a NAT policy name and to enter NAT policy configuration mode.

Use the **no** form of this command to remove the NAT policy.

### Examples

The following example translates source addresses for NAT policy, p2, which is applied to packets received on the pos2 interface:

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in source 34.34.34.34 35.35.35.35
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos2
[local]Redback(config-if)#ip nat p2
```

### Related Commands

**drop**  
**ignore**  
**ip nat**  
**ip static in**  
**ip static out**  
**nat policy-name**  
**pool**  
**timeout**

## nat policy-name

**nat policy-name** *pol-name*

**no nat policy-name** *pol-name*

### Purpose

Attaches the specified Network Address Translation (NAT) policy name to the subscriber's circuit.

### Command Mode

subscriber configuration

### Syntax Description

*pol-name*                      NAT policy name.

### Default

None

### Usage Guidelines

Use the **nat policy-name** command to attach the specified NAT policy to the subscriber's circuit.

Use the **no** form of this command to remove the NAT policy from the subscriber's circuit.

### Examples

The following example attaches the NAT policy, `nat-pol-1`, to the circuit attached to the `nat-sub` subscriber's circuit:

```
[local]Redback(config-ctx)#subscriber name nat-sub  
[local]Redback(config-sub)#nat policy-name nat-pol-1
```

### Related Commands

**drop**  
**ignore**  
**ip nat**  
**ip static in**  
**ip static out**  
**nat policy**  
**pool**  
**timeout**

# pool

**pool** *nat-pool-name* *ctx-name*

## Purpose

Configures the Network Address Translation (NAT) policy or class of packets to use the specified pool of IP addresses for packet translation.

## Command Mode

NAT policy configuration  
policy ACL class configuration

## Syntax Description

|                      |                                                          |
|----------------------|----------------------------------------------------------|
| <i>nat-pool-name</i> | NAT pool name.                                           |
| <i>ctx-name</i>      | Name of the context in which the NAT pool is configured. |

## Default

If no action is configured for the NAT policy, by default, packets are dropped.

## Usage Guidelines

Use the **pool** command to configure the NAT policy or class of packets to use the specified pool of IP addresses for packet translation.

## Examples

The following example configures the NAT policy, NAT-POLICY, to use the pool, NAT-POOL-DEFAULT, configured in the ISP context, and configures packets classified as NAT-CLASS-BASIC to use the pool, NAT-POOL-BASIC, configured in the ISP context:

```
[local]Redback(config-ctx)#nat policy NAT-POLICY
[local]Redback(config-policy-nat)#pool NAT-POOL-DEFAULT ISP
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-acl)#class NAT-CLASS-BASIC
[local]Redback(config-policy-acl-class)#pool NAT-POOL-BASIC ISP
```

## Related Commands

**address**  
**drop**  
**ignore**  
**ip nat pool**  
**timeout**

## timeout

**timeout** {**basic** *seconds* | **fin-reset** *seconds* | **icmp** *seconds* | **syn** *seconds* | **tcp** *seconds* | **udp** *seconds*}

**no timeout** {**basic** | **fin-reset** | **icmp** | **syn** | **tcp** | **udp**}

### Purpose

Modifies the period after which Network Address Translation (NAT) translations time out after there has been no activity.

### Command Mode

NAT policy configuration  
policy ACL class configuration

### Syntax Description

|                                 |                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>basic</b> <i>seconds</i>     | <p>Period, in seconds, after which basic NAT translations time out. The range of values is 4 to 262,143; the default value is 3600 (1 hour).</p> <p>This construct is only supported for basic NAT translations (not using NAPT).</p>                            |
| <b>fin-reset</b> <i>seconds</i> | <p>Period, in seconds, after which NAT translations for Transmission Control Protocol (TCP) FINISH and RESET packets time out. The range of values is 4 to 65,535; the default value is 240.</p> <p>This construct is only supported by policies using NAPT.</p> |
| <b>icmp</b> <i>seconds</i>      | <p>Period, in seconds, after which NAT translations for Internet Control Message Protocol (ICMP) packets time out. The range of values is 4 to 65,535; the default value is 60.</p> <p>This construct is only supported by policies using NAPT.</p>              |
| <b>syn</b> <i>seconds</i>       | <p>Period, in seconds, after which NAT translations for TCP SYN packets time out. The range of values is 4 to 65,535; the default value is 128.</p> <p>This construct is only supported by policies using NAPT.</p>                                              |
| <b>tcp</b> <i>seconds</i>       | <p>Period, in seconds, after which NAT translations for established TCP connections time out. The range of values is 4 to 262,143. The default value is 86,400 (24 hours).</p> <p>This construct is only supported by policies using NAPT.</p>                   |
| <b>udp</b> <i>seconds</i>       | <p>Period, in seconds, after which NAT translations for User Datagram Protocol (UDP) packets time out. The range of values is 4 to 65,535; the default value is 120.</p> <p>This construct is only supported by policies using NAPT.</p>                         |

### Default

See the “Syntax Description” section for default values.

### Usage Guidelines

Use the **timeout** command to modify the period after which NAT translations time out after there has been no activity. Timeout applies only if there is relevant translation.

Use the **no** form of this command to reset the timeout to its default value.

### Examples

The following example configures basic NAT translations to time out after there has been no activity for 7200 seconds (2 hours):

```
[local]Redback(config-ctx)#ip nat pool NAT-POOL
[local]Redback(config-nat-pool)#address 171.71.71.0/24
[local]Redback(config-nat-pool)#exit
[local]Redback(config-ctx)#nat policy NAT-1
[local]Redback(config-policy-nat)#pool NAT-POOL local
[local]Redback(config-policy-nat)#timeout basic 7200
```

### Related Commands

**drop**  
**ignore**  
**pool**



# Service Policy Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS service policy features.

For information about the tasks and commands used to monitor, troubleshoot, and administer forward policies, see the “Service Policy Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter includes the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

Service policies determine the context, or contexts that Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE) subscribers can access by verifying the domain or context name associate with subscriber records.

A service policy can be attached to any PPP- or PPPoE-encapsulated circuit using the **bind authentication** command (in ATM PVC, dot1q PVC, port, and protocol configuration mode); for more information, see the “Bindings Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

When the SmartEdge router is configured as a Layer 2 Tunneling Protocol (L2TP) network server (LNS), a service policy can be attached to subscriber sessions on the L2TP tunnel with the **session-auth** command (in L2TP peer configuration mode); for more information, see the “L2TP Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure service policies, perform the tasks described in the following sections:

- Configure a Service Policy
- Attach a Service Policy to Subscriber Sessions

### Configure a Service Policy

To configure a service policy, perform the tasks described in Table 11-1.

**Table 11-1** Configure a Service Policy

| #  | Task                                                                          | Root Command          | Notes                                                                                                                                                                                                                         |
|----|-------------------------------------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Configure a service policy name and access service policy configuration mode. | <b>service-policy</b> | Enter this command in global configuration mode.                                                                                                                                                                              |
| 2. | Configure the domain or context to which subscribers are allowed access.      | <b>allow</b>          | Enter this command in service policy configuration mode.<br>To specify more than one context or domain, use this command multiple times. Any context names that are not specified through this command are implicitly denied. |

### Attach a Service Policy to Subscriber Sessions

To attach a service policy to subscriber sessions, perform the appropriate task described in Table 11-2.

**Table 11-2** Attach a Service Policy to Subscriber Sessions

| Task                                                                             | Root Command               | Notes                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attach a service policy to PPP- and PPPoE-encapsulated subscriber sessions.      | <b>bind authentication</b> | Enter this command in ATM PVC, dot1q PVC, port, and protocol configuration modes.<br>This command is described in the “Bindings Configuration” chapter in the <i>Ports, Circuits, and Tunnels Configuration Guide</i> for the SmartEdge OS. |
| Attach a service policy to PPP-encapsulated subscriber sessions on L2TP tunnels. | <b>session-auth</b>        | Enter this command in L2TP peer configuration mode.<br>This command is described in the “L2TP Configuration” chapter in the <i>Ports, Circuits, and Tunnels Configuration Guide</i> for the SmartEdge OS.                                   |

## Configuration Examples

The following example configures the service policy, `local-only`, which allows subscribers access to the `local` context only. The service policy is applied to subscriber sessions using the specified Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC):

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#allow context name local
[local]Redback(config-policy-svc)#exit
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#atm pvc 3 5 profile atm1 encapsulation ppp
[local]Redback(config-atm-pvc)#bind authentication pap service-policy local-only
```

The following example restricts all subscribers that originate their session on ATM PVC 0 32 to be tunneled only to the `corp1` remote peer:

```
[local]Redback(config)#service-policy Corp-One-Permit
[local]Redback(config-policy-svc)#allow corp1.com
[local]Redback(config-policy-svc)#exit
[local]Redback(config)#context corporations
[local]Redback(config-ctx)#aaa authentication subscriber none
[local]Redback(config-ctx)#domain corp1.com
[local]Redback(config-ctx)#domain corp2.com
[local]Redback(config-ctx)#domain corp3.com
[local]Redback(config-ctx)#l2tp-peer name corp1 media udp-ip remote dns corp1.com local
10.1.1.1
[local]Redback(config-l2tp)#domain corp1.com
[local]Redback(config-l2tp)#exit
[local]Redback(config-ctx)#l2tp-peer name corp2 media udp-ip remote dns corp2.com local
10.1.1.2
[local]Redback(config-l2tp)#domain corp2.com
[local]Redback(config-l2tp)#exit
[local]Redback(config-ctx)#l2tp-peer name corp3 media udp-ip remote dns corp3.com local
10.1.1.3
[local]Redback(config-l2tp)#domain corp3.com
[local]Redback(config-l2tp)#exit
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#tunnel domain
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 5/1
[local]Redback(config-atm)#atm pvc 0 32 profile atm-pro-1 encapsulation pppoe
[local]Redback(config-atm-pvc)#bind authentication service-policy Corp-One-Permit
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure service policies. The commands are presented in alphabetical order.

**allow**  
**service-policy**

# allow

**allow** {**context name** *ctx-name* | **domain name** *name*}

**no allow** {**context name** *ctx-name* | **domain name** *name*}

## Purpose

Allows access to the specified context or domain for subscriber sessions that are attached to the service policy.

## Command Mode

service policy configuration

## Syntax Description

|                                     |                                                   |
|-------------------------------------|---------------------------------------------------|
| <b>context name</b> <i>ctx-name</i> | Context to which subscriber sessions are allowed. |
| <b>domain name</b> <i>name</i>      | Domain to which subscriber sessions are allowed.  |

## Default

None

## Usage Guidelines

Use the **allow** command to allow access to the specified context or domain for subscriber sessions that are attached to the service policy.

Any context or domain names that are not specified through this command are implicitly denied.

Use the **no** form of this command to remove the specified context.

## Examples

The following example configures a service policy, `local-only`, and configures it to allow subscribers access to the `local` context:

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#allow context name local
```

## Related Commands

`service-policy`

## service-policy

**service-policy name** *svc-pol-name*

**no service-policy name** *svc-pol-name*

### Purpose

Configures a service policy name and enters service policy configuration mode.

### Command Mode

global configuration

### Syntax Description

**name** *svc-pol-name*      Service policy name.

### Default

None

### Usage Guidelines

Use the **service-policy** command to configure a service policy name, and to enter service policy configuration mode.

Use the **no** form of this command to remove a service policy.

### Examples

The following example configures a service policy, `local-only`, and allows subscribers access to the `local` context only:

```
[local]Redback(config)#service-policy name local-only  
[local]Redback(config-policy-svc)#allow context name local
```

### Related Commands

**allow**

# Quality of Service Policies

---

This part describes the tasks and commands used to configure quality of service (QoS) policies and ports, channels, circuits, and applications for QoS functions. It consists of the following chapters:

- Chapter 12, “QoS Rate- and Class-Limiting Configuration”
- Chapter 13, “QoS Scheduling Configuration”
- Chapter 14, “QoS Circuit Configuration”





# QoS Rate- and Class-Limiting Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS quality of service (QoS) features.

For information about other QoS configuration tasks and commands, see the following chapters:

- Chapter 13, “QoS Scheduling Configuration”—Scheduling features (scheduling policies)
- Chapter 14, “QoS Circuit Configuration”—Port, channel, and circuit configuration for all QoS policies and features

For information about the tasks and commands used to monitor, troubleshoot, and administer QoS, see the “QoS Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

**Note** In this chapter, the term, first-generation Asynchronous Transfer Mode (ATM) OC traffic card, refers to a 2-port ATM OC-3c/STM-1c or ATM OC-12c/STM-4c traffic card; similarly, the term, second-generation ATM OC traffic card, refers to a 4-port ATM OC-3c/STM-1c or Enhanced ATM OC-12c/STM-4c traffic card.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

The Internet provides only best-effort service, offering no guarantees on when or whether a packet is delivered to the receiver. However, the SmartEdge OS offers QoS differentiation based on the subscriber record, the traffic type, and the application. QoS policies create and enforce levels of service and bandwidth rates, and prioritize how packets are admitted into scheduled from egress queues. The SmartEdge OS classifies, marks, and rate-limits incoming packets as described in these sections:

- Priority Groups
- Policy Access Control Lists

- QoS Policing and Metering Policies
- Summary

## Priority Groups

Incoming packets can be classified by assignment to a priority group. A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The actual queue number depends upon the queue map used and the number of queues configured on the circuit. The type of service (ToS) value and the IP Differentiated Services Code Point (DSCP) bits are not changed when assigned to a priority group.

## Policy Access Control Lists

A classification filter is configured by a policy access control list (ACL). Each policy ACL supports up to eight unique classes. Packets can be classified according to IP precedence value, protocol number, IP source and destination address, Internet Control Management Protocol (ICMP) attributes, Internet Group Management Protocol (IGMP) attributes, Transmission Control Protocol (TCP) attributes, and User Datagram Protocol (UDP) attributes.

A policy ACL can be applied to incoming or outgoing packets on a port, circuit, or for a subscriber record. A policy ACL is applied to incoming packets through a QoS policing policy and to outgoing packets through a QoS metering policy. For details about policy ACLs, see Chapter 8, “ACL Configuration.”

## QoS Policing and Metering Policies

A QoS policing policy can classify, mark, rate-limit, or perform all actions on incoming packets; a QoS metering policy performs the same operations for outgoing packets. You can apply both types of policies at one of two levels or at both levels, simultaneously. Either type of policy can apply to all packets on a particular circuit; this application is referred to as a circuit-based action. Alternatively, a policy can apply to only a particular class of packets traveling across the circuit; the class is configured using a policy ACL and the application is referred to as a class-based action. These actions (classification, marking, and rate-limiting) and the types of application are described in the following sections:

- Circuit-Based Marking
- Circuit-Based Rate-Limiting
- Class-Based Marking
- Class-Based Rate-Limiting
- Circuit-Based and Class-Based Rate-Limiting
- Single Rate Three-Color Markers

## Circuit-Based Marking

When a QoS policy is applied to a circuit without a policy ACL, all packets traveling over the circuit are affected by the QoS policy.

The value of packets traveling over the circuit can be modified by the SmartEdge OS and sent out from the router with the new value through either the **mark dscp** or **mark precedence** command in policing policy configuration mode (for incoming packets) or in metering policy configuration mode (for outgoing packets).

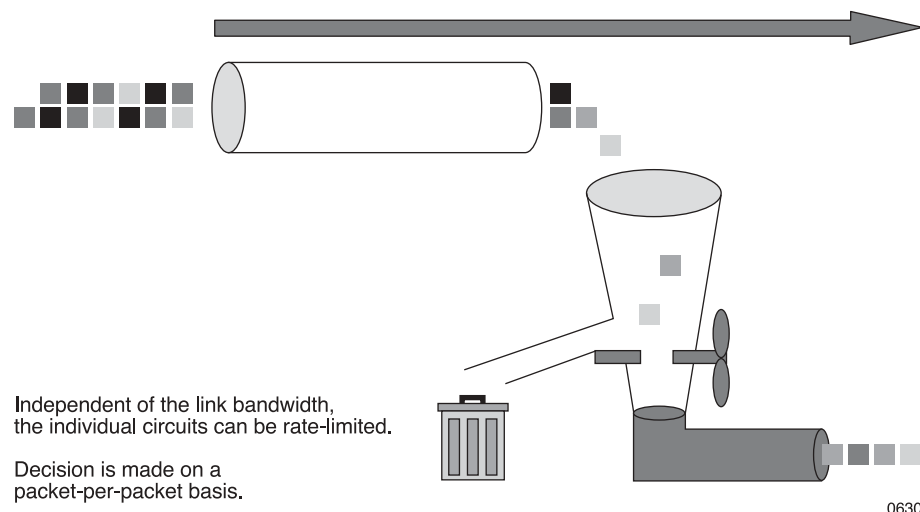
Or, packets can be prioritized by the SmartEdge OS for internal flow of traffic through the router only using the **mark priority** command in policing policy configuration mode (for incoming packets) or in metering policy configuration mode (for outgoing packets). In this case, when packets are sent out from the router, they retain their original value.

## Circuit-Based Rate-Limiting

When a QoS policy is applied to a circuit without a policy ACL, all packets traveling over the circuit are affected by the QoS policy.

By default, inbound packets that conform to the policing or metering rate are admitted with no additional action taken, while packets that exceed the rate are dropped. To modify the action taken by the SmartEdge OS, use the **conform** and **exceed** commands in policy rate configuration mode; see Figure 12-1.

**Figure 12-1 Circuit-Based Rate-Limiting**



## Class-Based Marking

When a QoS policy is applied to a circuit in conjunction with a policy ACL, only particular classes of packets traveling over the circuit are affected by the QoS policy. To configure up to eight classes to prioritize packets differently, use the **class** command (in policy ACL configuration mode). For details about policy ACLs, see Chapter 8, “ACL Configuration.”

The prioritization for particular classes of packets can be modified and sent out the router with the new value using the **mark dscp** or **mark precedence** command (in policy ACL class configuration mode).

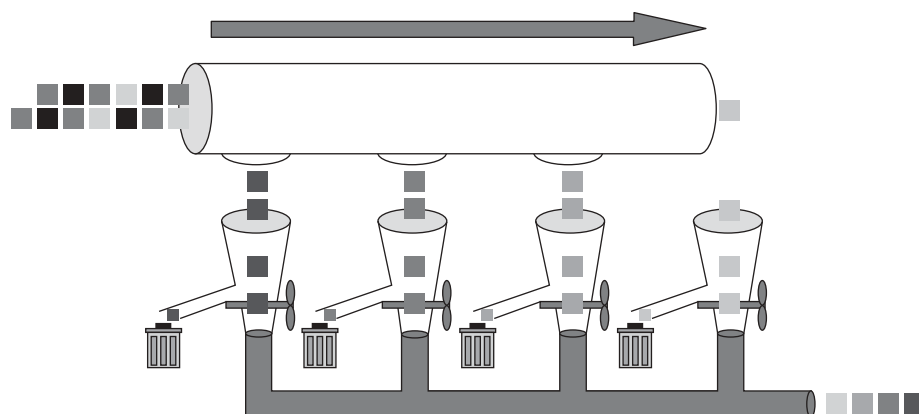
Classes of packets can also be prioritized for only internal flow of traffic through the router using the **mark priority** command (in policy ACL class configuration mode), so that when packets are sent out from the router, they retain their original value.

## Class-Based Rate-Limiting

When a QoS policy is applied to a circuit in conjunction with a policy ACL, only particular classes of packets traveling over the circuit are affected by the QoS policy.

By default, inbound packets that conform to the QoS policy rate are admitted with no additional action taken, while packets that exceed the rate are dropped. You can modify the default behavior for classes of packets using the **conform** and **exceed** commands in policy class rate configuration mode; see Figure 12-2.

**Figure 12-2 Class-Based Rate-Limiting**



Independent of the link bandwidth, the traffic can be rate-limited on a traffic class basis.

Decision is made on a packet-per-packet basis within each traffic class.

0631

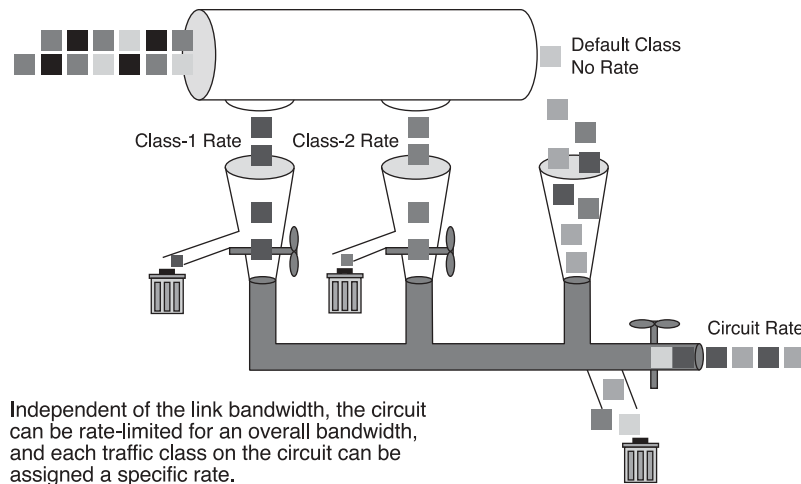
## Circuit-Based and Class-Based Rate-Limiting

A circuit can be rate-limited for an overall bandwidth, while each traffic class on the circuit is assigned a specific rate. Class-based rate limiting is applied to the packets first; see Figure 12-3. Then the circuit rate limit is applied to all packets, regardless of class and including packets that do not belong to any class (the default class).

If a class-based traffic rate is less than the circuit rate, that class-based traffic is guaranteed through the policing or metering policy. However, class-based traffic cannot borrow bandwidth from other classes.

The default class is allowed to borrow bandwidth, up to the circuit rate, if it is configured without a rate; however, if the class-based rate is equal to the circuit rate, the class-based traffic can severely limit default class traffic to the point where no default traffic can be transmitted or received.

**Figure 12-3 Circuit-Based and Class-Based Rate-Limiting**



0632

## Single Rate Three-Color Markers

The single rate three-color marker implementation meters traffic and assigns a color to packets for rate limiting purposes according to the following three configurable traffic thresholds:

- The traffic rate
- The burst tolerance
- The excess burst tolerance

The traffic rate, burst tolerance, and excess burst tolerance are configurable thresholds that you can use to specify how packets are dropped or marked. Depending on which thresholds are exceeded, packets are classified, using one of the following colors:

- **Green**—Packets that do not exceed the traffic rate or the burst tolerance. To configure the rate limiting action taken for these packets, use one of the **conform** commands in policy class rate configuration or policy rate configuration mode.
- **Yellow**—Packets that exceed the burst tolerance, but do not exceed the excess burst tolerance. To configure the rate limiting action taken for these packets, use one of the **exceed** commands in policy class rate configuration or policy rate configuration mode.
- **Red**—Packets that exceed the excess burst tolerance. To configure the rate limiting action taken for these packets, use one of the **violate** commands in policy class rate configuration or policy rate configuration mode.

The SmartEdge OS implementation of a single rate three-color marker conforms to RFC 2697, *A Single Rate Three Color Marker*.

### Summary

the high-level QoS flow through the SmartEdge router is as follows:

1. As the packet enters the SmartEdge router, the packet goes through a classification filter configured by a policy ACL.
2. After packets are classified, they can be marked as follows:
  - a. Rate limits can be set on the incoming port, circuit, or subscriber record that can cause the packet to be dropped.
  - b. If is not dropped due to rate-limiting, the packet can be assigned to a priority group without changing the packet's QoS bits, or it can be marked by changing its IP DSCP value or IP precedence value, or Multiprotocol Label Switching (MPLS) experimental (EXP) bits can be appended to it.
3. At this point, the SmartEdge OS transports the packet to the appropriate outbound traffic card.
4. Incoming queues on outbound traffic cards have associated scheduling parameters such as rates, depths, and relative weights. The traffic card's scheduler draws packets from the incoming queues based on weight, rate, or strict priority:
  - a. A packet can be dropped when queues back up over a configured discard threshold or because of a random early detection (RED) parameter setting.
  - b. If a packet is not dropped, it is scheduled into an output queue based on its priority group or its scheduling policy.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure a metering or policing policy, complete the tasks described in the following sections:

- Policy Configuration Guidelines
- Configure a Metering Policy
- Configure a Policing Policy
- Apply a Policy ACL

### Policy Configuration Guidelines

The following guidelines apply to the configuration of QoS metering and policing policies:

- You can either mark or establish a rate for packets on a single circuit, port, or subscriber record; these conditions are mutually exclusive.
- Only one marking instruction can be in effect at a time. Any succeeding command supersedes the previous instruction.

## Configure a Metering Policy

To configure a metering policy, perform the tasks described in Table 12-1; enter all commands in metering policy configuration mode, unless otherwise noted.

**Table 12-1 Configure a Metering Policy**

| #  | Task                                                                                                                                                                                                                                                                                                                                                                                        | Root Command                                                                                                                                  | Notes                                                                                                                     |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select a metering policy and access metering policy configuration mode.                                                                                                                                                                                                                                                                                                           | <b>qos policy metering</b>                                                                                                                    | Enter this command in global configuration mode.                                                                          |
| 2. | Optional. Mark outgoing packets associated with the policy with one of the following tasks: <ul style="list-style-type: none"> <li>Assign a DSCP priority.</li> <li>Assign a drop precedence value.</li> <li>Assign a priority group number.</li> </ul>                                                                                                                                     | <b>mark dscp</b><br><b>mark precedence</b><br><b>mark priority</b>                                                                            | Only one marking instruction can be in effect at any time.                                                                |
| 3. | Set the policy rate for outgoing packets and access policy rate configuration mode.                                                                                                                                                                                                                                                                                                         | <b>rate</b>                                                                                                                                   |                                                                                                                           |
| 4. | Optional. Specify the treatment of outgoing packets that conform to a set rate with one of the following tasks: <ul style="list-style-type: none"> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul>                              | <b>conform no-action</b><br><b>conform mark dscp</b><br><b>conform mark precedence</b><br><b>conform mark priority</b>                        | Enter these commands in policy rate configuration mode.<br><br>Only one marking instruction can be in effect at any time. |
| 5. | Optional. Specify the treatment of outgoing packets that exceed a set rate with one of the following tasks: <ul style="list-style-type: none"> <li>Drop outgoing packets.</li> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul>  | <b>exceed drop</b><br><b>exceed no-action</b><br><b>exceed mark dscp</b><br><b>exceed mark precedence</b><br><b>exceed mark priority</b>      | Enter these commands in policy rate configuration mode.<br><br>Only one marking instruction can be in effect at any time. |
| 6. | Optional. Specify the treatment of outgoing packets that violate a set rate with one of the following tasks: <ul style="list-style-type: none"> <li>Drop outgoing packets.</li> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul> | <b>violate drop</b><br><b>violate no-action</b><br><b>violate mark dscp</b><br><b>violate mark precedence</b><br><b>violate mark priority</b> | Enter these commands in policy rate configuration mode.<br><br>Only one marking instruction can be in effect at any time. |
| 7. | Optional. Apply a policy ACL to this policy.                                                                                                                                                                                                                                                                                                                                                | See the "Apply a Policy ACL" section.                                                                                                         |                                                                                                                           |

## Configure a Policing Policy

To configure a policing policy, perform the tasks described in Table 12-2; enter all commands in policing policy configuration mode, unless otherwise noted.

**Table 12-2 Configure a Policing Policy**

| #  | Task                                                                                                                                                                                                                                                                                                                                                                                       | Root Command                                                                                                                                  | Notes                                                                                                                     |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select a policing policy and access policing policy configuration mode.                                                                                                                                                                                                                                                                                                          | <b>qos policy policing</b>                                                                                                                    | Enter this command in global configuration mode.                                                                          |
| 2. | Optional. Mark incoming packets associated with the policy with one of the following tasks: <ul style="list-style-type: none"> <li>Assign a DSCP priority.</li> <li>Assign a drop precedence value.</li> <li>Assign a priority group number.</li> </ul>                                                                                                                                    | <b>mark dscp</b><br><b>mark precedence</b><br><b>mark priority</b>                                                                            | Only one marking instruction can be in effect at any time.                                                                |
| 3. | Set the policy rate for incoming packets and access policy rate configuration mode.                                                                                                                                                                                                                                                                                                        | <b>rate</b>                                                                                                                                   |                                                                                                                           |
| 4. | Optional. Specify the treatment of incoming packets that conform to a set rate with one of the following tasks: <ul style="list-style-type: none"> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul>                             | <b>conform no-action</b><br><b>conform mark dscp</b><br><b>conform mark precedence</b><br><b>conform mark priority</b>                        | Enter these commands in policy rate configuration mode.<br><br>Only one marking instruction can be in effect at any time. |
| 5. | Optional. Specify the treatment of incoming packets that exceed a set rate with one of the following tasks: <ul style="list-style-type: none"> <li>Drop inbound packets.</li> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul>  | <b>exceed drop</b><br><b>exceed no-action</b><br><b>exceed mark dscp</b><br><b>exceed mark precedence</b><br><b>exceed mark priority</b>      | Enter these commands in policy rate configuration mode.<br><br>Only one marking instruction can be in effect at any time. |
| 6. | Optional. Specify the treatment of incoming packets that violate a set rate with one of the following tasks: <ul style="list-style-type: none"> <li>Drop inbound packets.</li> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul> | <b>violate drop</b><br><b>violate no-action</b><br><b>violate mark dscp</b><br><b>violate mark precedence</b><br><b>violate mark priority</b> | Enter these commands in policy rate configuration mode.<br><br>Only one marking instruction can be in effect at any time. |
| 7. | Optional. Apply a policy ACL to this policy.                                                                                                                                                                                                                                                                                                                                               | See the "Apply a Policy ACL" section.                                                                                                         |                                                                                                                           |



## Apply a Policy ACL

To apply a policy ACL to packets associated with a QoS metering or policing policy and complete the configuration of the policy, perform the tasks described in Table 12-3.

**Table 12-3 Apply a Policy ACL**

| #  | Task                                                                                                                                                                                                                                                                                                                                                                                | Root Command                                                                                                                                                  | Notes                                                                                                                                                         |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Apply a policy ACL to a QoS metering policy or a QoS policing policy, and access policy ACL configuration mode.                                                                                                                                                                                                                                                                     | <b>access-group</b>                                                                                                                                           | Enter this command in policing policy or metering policy configuration mode.                                                                                  |
| 2. | Specify a class and access policy ACL class configuration mode.                                                                                                                                                                                                                                                                                                                     | <b>class</b>                                                                                                                                                  | Enter this command in policy ACL configuration mode.<br>The class name must match the name of a class specified in a <b>permit</b> command in the policy ACL. |
| 3. | Optional. Specify the rate for this class, using one of the following tasks: <ul style="list-style-type: none"> <li>Set the rate and burst tolerance and access policy class rate configuration mode.</li> <li>Assign a percentage of the overall policy rate to this class of traffic and access policy class rate configuration mode.</li> </ul>                                  | <b>rate</b><br><br><b>rate percentage</b>                                                                                                                     | Enter these commands in policy ACL class configuration mode.                                                                                                  |
| 4. | Optional. Specify the treatment of packets that conform to the rate, using one of the following tasks: <ul style="list-style-type: none"> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul>                               | <b>conform no-action</b><br><br><b>conform mark dscp</b><br><br><b>conform mark precedence</b><br><br><b>conform mark priority</b>                            | Enter these commands in policy class rate configuration mode.<br><br>Only one marking instruction can be in effect at any time.                               |
| 5. | Optional. Specify the treatment of packets that exceed a set rate, using one of the following tasks: <ul style="list-style-type: none"> <li>Drop inbound packets.</li> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Assign a drop precedence value to packets.</li> <li>Assign a priority group number to packets.</li> </ul>  | <b>exceed drop</b><br><br><b>exceed no-action</b><br><br><b>exceed mark dscp</b><br><br><b>exceed mark precedence</b><br><br><b>exceed mark priority</b>      | Enter these commands in policy class rate configuration mode.                                                                                                 |
| 6. | Optional. Specify the treatment of packets that violate a set rate, using one of the following tasks: <ul style="list-style-type: none"> <li>Drop inbound packets.</li> <li>Specify that no action is taken on packets.</li> <li>Mark packets with a DSCP class.</li> <li>Mark packets with a drop precedence value.</li> <li>Mark packets with a priority group number.</li> </ul> | <b>violate drop</b><br><br><b>violate no-action</b><br><br><b>violate mark dscp</b><br><br><b>violate mark precedence</b><br><br><b>violate mark priority</b> | Enter these commands in policy class rate configuration mode.                                                                                                 |

## Configuration Examples

---

Examples of rate limiting and class-based marking, using policing policy configurations, are described in the following sections:

- Circuit-Based Marking
- Circuit-Based Rate-Limiting
- Class-Based and Circuit-Based Rate Limiting

### Circuit-Based Marking

The following example simply marks all packets on the circuit to which the policy, `circuit`, is applied with a DSCP value of `ef`, which indicates a high priority through expedited forwarding. Packets are not required to conform to a specific traffic rate.

```
[local]Redback(config)#qos policy circuit policing
[local]Redback(config-policy-policing)#mark dscp ef
```

### Circuit-Based Rate-Limiting

The following example configures the QoS policy, `circuit`. Packets conforming to 10000 kbps are marked with a DSCP value of `ef`, which indicates a high priority through expedited forwarding. Packets that exceed the rate are dropped by default. The `counters` keyword in the `rate` command records the number of packets conforming to the rate limit and the number of packets exceeding the rate limit.

```
[local]Redback(config)#qos policy circuit policing
[local]Redback(config-policy-policing)#rate 10000 burst 1000 counters
[local]Redback(config-policy-rate)#conform mark dscp ef
```

### Class-Based and Circuit-Based Rate Limiting

The following example creates a policy ACL, `qosmet`, in the `local` context and attaches it to the QoS metering policy, `meter`. The ACL classifies packets into three classes: `priority`, `immediate`, `flash`, and a default class, `default`. The QoS policy assigns a different rate to the `priority`, `immediate`, and `flash` classes; packets classified as `default` are marked with priority 7.

```
[local]Redback(config-ctx)#policy access-list qosmet
[local]Redback(config-access-list)#sequence 10 permit ip precedence priority
class class-1
[local]Redback(config-access-list)#sequence 20 permit ip precedence immediate
class class-2
[local]Redback(config-access-list)#sequence 30 permit ip precedence flash class class-3
[local]Redback(config-access-list)#sequence 40 permit ip any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit

[local]Redback(config)#qos policy meter metering
[local]Redback(config-policy-metering)#rate 1000 burst 50000 excess-burst 200000
counters
```

```
[local]Redback(config-policy-metering)#access-group qosmet local
[local]Redback(config-policy-acl)#class class-1
[local]Redback(config-policy-acl-class)#rate 1000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-acl-class)#exit

[local]Redback(config-policy-acl)#class class-2
[local]Redback(config-policy-acl-class)#rate 2000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-acl-class)#exit

[local]Redback(config-policy-acl)#class class-3
[local]Redback(config-policy-acl-class)#rate 3000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-acl-class)#exit

[local]Redback(config-policy-acl)#class default
[local]Redback(config-policy-acl-class)#mark priority 7
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#exit
[local]Redback(config-policy-policing)#exit
```

The following example creates a policy ACL, qos-class, in the local context and attaches it to the QoS metering policy, sub-rate. The ACL defines three classes: tcp, voip, and default.

```
[local]Redback(config-ctx)#policy access-list qos-class
[local]Redback(config-access-list)#sequence 10 permit ip precedence tcp any any
class tcp
[local]Redback(config-access-list)#sequence 20 permit ip precedence ip any any dscp
equ cs6 class voip
[local]Redback(config-access-list)#sequence 30 permit ip any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit

[local]Redback(config)#qos policy sub-rate metering
[local]Redback(config-policy-metering)#rate 2000 burst 100000 excess-burst 200000
counters
[local]Redback(config-policy-metering)#access-group qos-class local
[local]Redback(config-policy-acl)#class tcp
[local]Redback(config-policy-acl-class)#rate 1000 burst 50000 excess-burst 100000
conform mark priority 3
[local]Redback(config-policy-acl)#class voip
[local]Redback(config-policy-acl-class)#rate 200 burst 20000 excess-burst 40000 conform
mark priority 0
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-acl-class)#exit

[local]Redback(config-policy-acl)#class default
[local]Redback(config-policy-acl-class)#mark priority 7
```

The following example configures the QoS policing policy, combined, which combines circuit-based rate-limiting and class-based rate-limiting and marking:

```
[local]Redback(config)#qos policy combined policing
[local]Redback(config-policy-policing)#rate 10000 burst 5000
[local]Redback(config-policy-rate)#conform mark precedence 2
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#access-group qos
[local]Redback(config-policy-acl)#class web
[local]Redback(config-policy-acl-class)#rate 5000 burst 1000
[local]Redback(config-policy-class-rate)#conform mark dscp AF11
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class voip
[local]Redback(config-policy-acl-class)#mark dscp ef
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class default
[local]Redback(config-policy-acl-class)#mark dscp df
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure QoS policies. The commands are presented in alphabetical order.

**conform mark dscp**  
**conform mark precedence**  
**conform mark priority**  
**conform no-action**  
**exceed drop**  
**exceed mark dscp**  
**exceed mark precedence**  
**exceed mark priority**  
**exceed no-action**  
**mark dscp**  
**mark precedence**

**mark priority**  
**qos policy metering**  
**qos policy policing**  
**rate**  
**rate percentage**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate mark priority**  
**violate no-action**

## conform mark dscp

**conform mark dscp** *dscp-class*

{**no** | **default**} **conform mark dscp**

### Purpose

Marks inbound packets that conform to the configured quality of service (QoS) rate with a Differentiated Services Code Point (DSCP) value.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*dscp-class*

Priority with which packets conforming to the rate are marked. Values can be:

- An integer from **0** to **63**.
- One of the keywords listed in Table 12-4.

### Default

No action is taken on packets that conform to the configured rate.

### Usage Guidelines

Use the **conform mark dscp** command to mark inbound packets that conform to the configured rate with a DSCP value.

You can configure the rate using the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode). Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark dscp** command, specifying a new value for the *dscp-class* argument, which supersedes the one previously configured.

Table 12-4 lists the keywords for the *dscp-class* argument.

**Table 12-4 DSCP Class Keywords**

| DSCP Class                                            | Keyword     | DSCP Class                                       | Keyword                         |
|-------------------------------------------------------|-------------|--------------------------------------------------|---------------------------------|
| Assured Forwarding (AF) Class 1/<br>Drop precedence 1 | <b>af11</b> | Class Selector 0<br>(same as default forwarding) | <b>cs0</b> (same as <b>df</b> ) |
| AF Class 1/Drop precedence 2                          | <b>af12</b> | Class Selector 1                                 | <b>cs1</b>                      |
| AF Class 1/Drop precedence 3                          | <b>af13</b> | Class Selector 2                                 | <b>cs2</b>                      |
| AF Class 2/Drop precedence 1                          | <b>af21</b> | Class Selector 3                                 | <b>cs3</b>                      |
| AF Class 2/Drop precedence 2                          | <b>af22</b> | Class Selector 4                                 | <b>cs4</b>                      |
| AF Class 3/Drop precedence 3                          | <b>af23</b> | Class Selector 5                                 | <b>cs5</b>                      |

**Table 12-4 DSCP Class Keywords** (*continued*)

| DSCP Class                   | Keyword     | DSCP Class                                       | Keyword                         |
|------------------------------|-------------|--------------------------------------------------|---------------------------------|
| AF Class 3/Drop precedence 1 | <b>af31</b> | Class Selector 6                                 | <b>cs6</b>                      |
| AF Class 3/Drop precedence 2 | <b>af32</b> | Class Selector 7                                 | <b>cs7</b>                      |
| AF Class 3/Drop precedence 3 | <b>af33</b> | Default Forwarding<br>(same as Class Selector 0) | <b>df</b> (same as <b>cs0</b> ) |
| AF Class 4/Drop precedence 1 | <b>af41</b> | Expedited Forwarding                             | <b>ef</b>                       |
| AF Class 4/Drop precedence 2 | <b>af42</b> |                                                  |                                 |
| AF Class 4/Drop precedence 3 | <b>af43</b> |                                                  |                                 |

For more information about DSCP values, see RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.



**Caution** Risk of packet reordering. Packets can be reordered into a different major DSCP class. To reduce the risk, ensure that the marking of conforming packets and exceeding packets differ only within a major DSCP class. Major DSCP classes are identified by the Class Selector code, and include CS0=DF, CS1=AF11, AF12, AF13, CS2=AF21, AF22, AF23, CS3=AF31, AF32, AF33, CS4=AF41, AF42, AF43, and CS5=EF. For example, if you mark conforming packets with AF11 and you want to avoid reordering, mark exceeding packets with AF11, AF12, or AF13 only.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of not taking any action on packets that conform to the configured rate.

## Examples

The following example configures the policing policy, **protection1**, to mark all packets that conform to the configured rate with a DSCP value representing a high priority of expedited forwarding (**ef**) and, by default using the **conform mark** command, to drop all packets that exceed the rate configured for the policing policy:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark dscp ef
```

## Related Commands

**conform mark precedence**  
**conform mark priority**  
**conform no-action**  
**exceed drop**  
**exceed mark dscp**  
**exceed mark precedence**  
**exceed mark priority**

**exceed no-action**  
**rate**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate mark priority**  
**violate no-action**

## conform mark precedence

**conform mark precedence** *prec-value*

{**no** | **default**} **conform mark precedence**

### Purpose

Marks inbound packets that conform to the configured quality of service (QoS) rate with a drop precedence value corresponding to the assured forwarding (AF) class of the packet.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*prec-value*

Drop precedence value. The range of values is 1 to 3.

### Default

No action is taken on packets that conform to the configured rate.

### Usage Guidelines

Use the **conform mark precedence** command to mark inbound packets that conform to the configured rate with a drop precedence value corresponding to the AF class of the packet.

You can configure rate using the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

In general, the level of forwarding assurance of an IP packet is based on: (1) the resources allocated to the AF class to which the packet belongs, (2) the current load of the AF class, and, in case of congestion within the class, (3) the drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF Differentiated Services Code Point (DSCP) class. Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 12-5 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

**Table 12-5 Drop Precedence Values**

| DSCP Value of an Incoming Packet | Packet is Tagged with a Drop Precedence Value | DSCP Value of the Outgoing Packet |
|----------------------------------|-----------------------------------------------|-----------------------------------|
| AF11, AF12, AF13                 | 1                                             | AF11                              |
| AF21, AF22, AF23                 |                                               | AF21                              |
| AF31, AF32, AF33                 |                                               | AF31                              |
| AF41, AF42, AF43                 |                                               | AF41                              |



**Table 12-5 Drop Precedence Values** (*continued*)

| DSCP Value of an Incoming Packet | Packet is Tagged with a Drop Precedence Value | DSCP Value of the Outgoing Packet |
|----------------------------------|-----------------------------------------------|-----------------------------------|
| AF11, AF12, AF13                 | 2                                             | AF12                              |
| AF21, AF22, AF23                 |                                               | AF22                              |
| AF31, AF32, AF33                 |                                               | AF32                              |
| AF41, AF42, AF43                 |                                               | AF42                              |
| AF11, AF12, AF13                 | 3                                             | AF13                              |
| AF21, AF22, AF23                 |                                               | AF23                              |
| AF31, AF32, AF33                 |                                               | AF33                              |
| AF41, AF42, AF43                 |                                               | AF43                              |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark precedence** command, specifying a new value for the *prec-value* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of not taking any action on packets that conform to the configured rate.

## Examples

The following example configures the policing policy, `protection1`, to mark all packets that conform to the configured rate with a drop precedence value of 1 and drops all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark precedence 1
```

## Related Commands

|                               |                                |
|-------------------------------|--------------------------------|
| <b>conform mark dscp</b>      | <b>exceed no-action</b>        |
| <b>conform mark priority</b>  | <b>rate</b>                    |
| <b>conform no-action</b>      | <b>violate drop</b>            |
| <b>exceed drop</b>            | <b>violate mark dscp</b>       |
| <b>exceed mark dscp</b>       | <b>violate mark precedence</b> |
| <b>exceed mark precedence</b> | <b>violate mark priority</b>   |
| <b>exceed mark priority</b>   | <b>violate no-action</b>       |

## conform mark priority

**conform mark priority** *group-num*

{**no** | **default**} **conform mark priority**

### Purpose

Marks inbound packets that conform to the configured quality of service (QoS) rate with a priority group number.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*group-num*

Priority group number. The range of values is 0 to 7.

### Default

No action is taken on packets that conform to the configured rate. Default mapping of priority groups to queues are listed in Table 12-6 in the “Usage Guidelines” section.

### Usage Guidelines

Use the **conform mark priority** command to mark inbound packets that conform to the configured rate with a priority group number.

To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not being changed by this command. The actual queue number depends upon the number of queues configured on the circuit; see the **num-queues** command.

The SmartEdge OS assigns factory preset, or default, mapping of a priority group to a particular queue, according to the number of queues configured on a circuit; see Table 12-6.

**Table 12-6 Default Mapping of Priority Groups to Queues**

| Priority Group | 8 Queues | 4 Queues | 2 Queues | 1 Queue |
|----------------|----------|----------|----------|---------|
| 0              | queue 0  | queue 0  | queue 0  | queue 0 |
| 1              | queue 1  | queue 1  | queue 1  | queue 0 |
| 2              | queue 2  | queue 1  | queue 1  | queue 0 |
| 3              | queue 3  | queue 2  | queue 1  | queue 0 |
| 4              | queue 4  | queue 2  | queue 1  | queue 0 |
| 5              | queue 5  | queue 2  | queue 1  | queue 0 |
| 6              | queue 6  | queue 2  | queue 1  | queue 0 |
| 7              | queue 7  | queue 3  | queue 1  | queue 0 |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark priority** command, specifying a new value for the *group-num* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to specify the default behavior.

## Examples

The following example configures the policy to mark all packets that conform to the configured rate with priority group number 3 and drops all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark priority 3
```

## Related Commands

|                                |                                |
|--------------------------------|--------------------------------|
| <b>conform mark dscp</b>       | <b>exceed no-action</b>        |
| <b>conform mark precedence</b> | <b>rate</b>                    |
| <b>conform no-action</b>       | <b>violate drop</b>            |
| <b>exceed drop</b>             | <b>violate mark dscp</b>       |
| <b>exceed mark dscp</b>        | <b>violate mark precedence</b> |
| <b>exceed mark precedence</b>  | <b>violate mark priority</b>   |
| <b>exceed mark priority</b>    | <b>violate no-action</b>       |

## conform no-action

**conform no-action**

**{no | default} conform no-action**

### Purpose

Specifies that no marking is made on packets that conform to the configured quality of service (QoS) rate.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

This command has no keywords or arguments.

### Default

No marking is taken on packets that conform to the configured rate.

### Usage Guidelines

Use the **conform no-action** command to specify that no marking is taken on packets that conform to the configured rate.

To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

Use the **no** or **default** form of this command to specify that no marking is made.

### Examples

The following example configures the policy to mark all packets that conform to the configured rate with no action:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform no-action
```

### Related Commands

**conform mark dscp**  
**conform mark precedence**  
**conform mark priority**  
**exceed drop**  
**exceed mark dscp**  
**exceed mark precedence**  
**exceed mark priority**

**exceed no-action**  
**rate**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate mark priority**  
**violate no-action**

## exceed drop

**exceed drop** [*qos-priority group-num*]

{**no** | **default**} **exceed drop** [*qos-priority group-num*]

### Purpose

Specifies how packets are dropped when the traffic rate exceeds the quality of service (QoS) rate and burst tolerance.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

**qos-priority group-num** Optional. Priority group number. This option is available only if the QoS rate is configured with an excess burst tolerance. The range of values for the *group-num* argument is 0 to 7.

### Default

If the excess burst tolerance is not configured, all packets exceeding the QoS burst tolerance are dropped. If the excess burst tolerance is configured, packets exceeding the QoS burst tolerance are dropped randomly.

### Usage Guidelines

Use the **exceed drop** command to specify how packets are dropped when the traffic rate exceeds the QoS rate and burst tolerance. Use this command as part of a policing policy for incoming packets and as part of a metering policy for outgoing packets.

You can configure the traffic rate, burst tolerance, and excess burst tolerance with the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode). The following conditions determine how packets are dropped:

- If the excess burst tolerance is not configured, all packets exceeding the configured burst tolerance are dropped.
- If the excess burst tolerance is configured, and the traffic rate does not exceed the excess burst tolerance, packets are dropped according to one of the following conditions:
  - If the **qos-priority group-num** construct is not configured, packets are dropped randomly.
  - If the **qos-priority group-num** construct is configured, only packets with a QoS priority less than the specified *group-num* argument are dropped. All other packets are not dropped.

**Note** Use the **violate drop** commands (in policy class rate and policy rate configuration modes) to specify how packets are dropped when the traffic rate exceeds the configured excess burst tolerance.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to specify the default condition.

## Examples

The following example drops packets that exceed the traffic rate and burst tolerance:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
```

## Related Commands

**conform mark dscp**  
**conform mark precedence**  
**conform mark priority**  
**conform no-action**  
**exceed mark dscp**  
**exceed mark precedence**  
**exceed mark priority**

**exceed no-action**  
**rate**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate mark priority**  
**violate no-action**

## exceed mark dscp

**exceed mark dscp** *dscp-class*

{**no** | **default**} **exceed mark dscp**

### Purpose

Marks packets that exceed the configured quality of service (QoS) rate and burst tolerance with a Differentiated Services Code Point (DSCP) value.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*dscp-class*                      Priority with which packets exceeding the rate are marked. Values can be:

- An integer from **0** to **63**.
- One of the keywords listed in Table 12-7.

### Default

Packets exceeding the policing rate are dropped.

### Usage Guidelines

Use the **exceed mark dscp** command to mark packets that exceed the configured rate with a DSCP value.

To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode). Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **exceed mark dscp** command, specifying a new value for the *dscp-class* argument, which supersedes the one previously configured.

Table 12-7 lists the keywords for the *dscp-class* argument.

**Table 12-7 DSCP Class Keywords**

| DSCP Class                                         | Keyword     | DSCP Class                                    | Keyword                         |
|----------------------------------------------------|-------------|-----------------------------------------------|---------------------------------|
| Assured Forwarding (AF) Class 1 /Drop precedence 1 | <b>af11</b> | Class Selector 0 (same as default forwarding) | <b>cs0</b> (same as <b>df</b> ) |
| AF Class 1/Drop precedence 2                       | <b>af12</b> | Class Selector 1                              | <b>cs1</b>                      |
| AF Class 1/Drop precedence 3                       | <b>af13</b> | Class Selector 2                              | <b>cs2</b>                      |
| AF Class 2/Drop precedence 1                       | <b>af21</b> | Class Selector 3                              | <b>cs3</b>                      |
| AF Class 2/Drop precedence 2                       | <b>af22</b> | Class Selector 4                              | <b>cs4</b>                      |
| AF Class 3/Drop precedence 3                       | <b>af23</b> | Class Selector 5                              | <b>cs5</b>                      |
| AF Class 3/Drop precedence 1                       | <b>af31</b> | Class Selector 6                              | <b>cs6</b>                      |

**Table 12-7 DSCP Class Keywords** (*continued*)

| DSCP Class                   | Keyword     | DSCP Class                                       | Keyword                         |
|------------------------------|-------------|--------------------------------------------------|---------------------------------|
| AF Class 3/Drop precedence 2 | <b>af32</b> | Class Selector 7                                 | <b>cs7</b>                      |
| AF Class 3/Drop precedence 3 | <b>af33</b> | Default Forwarding<br>(same as Class Selector 0) | <b>df</b> (same as <b>cs0</b> ) |
| AF Class 4/Drop precedence 1 | <b>af41</b> | Expedited Forwarding                             | <b>ef</b>                       |
| AF Class 4/Drop precedence 2 | <b>af42</b> |                                                  |                                 |
| AF Class 4/Drop precedence 3 | <b>af43</b> |                                                  |                                 |

**Note** RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, defines the Class Selector code points.



**Caution** Risk of packet reordering. To reduce the risk, ensure that the marking of conforming packets and exceeding packets differ only within a major DSCP class. Major DSCP classes are identified by the Class Selector code, and include CS0=DF, CS1=AF11, AF12, AF13, CS2=AF21, AF22, AF23, CS3=AF31, AF32, AF33, CS4=AF41, AF42, AF43, and CS5=EF. For example, if you mark conforming packets with AF11 and you want to avoid reordering, mark exceeding packets with AF11, AF12, or AF13 only.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

## Examples

The following example configures the policy to mark all packets that conform to the configured rate with a DSCP value representing a high priority and drops all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark dscp ef
```

## Related Commands

conform mark dscp  
conform mark precedence  
conform mark priority  
conform no-action  
exceed drop  
exceed mark precedence  
exceed mark priority

exceed no-action  
rate  
violate drop  
violate mark dscp  
violate mark precedence  
violate mark priority  
violate no-action



## exceed mark precedence

**exceed mark precedence** *prec-value*

{**no** | **default**} **exceed mark precedence**

### Purpose

Marks packets that exceed the configured quality of service (QoS) rate with a drop precedence value corresponding to the assured forwarding (AF) class of the packet.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*prec-value*

Drop precedence bits value. The range of values is 1 to 3.

### Default

Packets exceeding the policy rate are dropped.

### Usage Guidelines

Use the **exceed mark precedence** command to mark packets that exceed the configured rate with a drop precedence value corresponding to the AF class of the packet.

To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

In general, the level of forwarding assurance of an IP packet is based on: (1) the resources allocated to the AF class to which the packet belongs, (2) the current load of the AF class, and, in case of congestion within the class, (3) the drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 12-8 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

**Table 12-8 Drop Precedence Values**

| DSCP Value of an Incoming Packet | Packet is Tagged with a Drop Precedence Value | DSCP Value of the Outgoing Packet |
|----------------------------------|-----------------------------------------------|-----------------------------------|
| AF11, AF12, AF13                 | 1                                             | AF11                              |
| AF21, AF22, AF23                 |                                               | AF21                              |
| AF31, AF32, AF33                 |                                               | AF31                              |
| AF41, AF42, AF43                 |                                               | AF41                              |

**Table 12-8 Drop Precedence Values** (*continued*)

| DSCP Value of an Incoming Packet | Packet is Tagged with a Drop Precedence Value | DSCP Value of the Outgoing Packet |
|----------------------------------|-----------------------------------------------|-----------------------------------|
| AF11, AF12, AF13                 | 2                                             | AF12                              |
| AF21, AF22, AF23                 |                                               | AF22                              |
| AF31, AF32, AF33                 |                                               | AF32                              |
| AF41, AF42, AF43                 |                                               | AF42                              |
| AF11, AF12, AF13                 | 3                                             | AF13                              |
| AF21, AF22, AF23                 |                                               | AF23                              |
| AF31, AF32, AF33                 |                                               | AF33                              |
| AF41, AF42, AF43                 |                                               | AF43                              |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **exceed mark precedence** command, specifying a new value for the *prec-value* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

## Examples

The following example configures the policy to mark all packets that conform to the configured rate with an IP precedence value of 3 and uses the **conform mark** command, which by default, drops all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark precedence 3
```

## Related Commands

**conform mark dscp**  
**conform mark precedence**  
**conform mark priority**  
**conform no-action**  
**exceed drop**  
**exceed mark dscp**  
**exceed mark priority**

**exceed no-action**  
**rate**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate mark priority**  
**violate no-action**

## exceed mark priority

**exceed mark priority** *group-num*

{ **no** | **default** } **exceed mark priority**

### Purpose

Marks packets that exceed the quality of service (QoS) rate and burst tolerance with a priority group number.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*group-num*                      Priority group number. The range of values is 0 to 7.

### Default

Packets exceeding the rate are dropped.

### Usage Guidelines

Use the **exceed mark priority** command to mark packets that exceed the rate with a priority group number. To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not being changed by this command. The actual queue number depends upon the number of queues configured on the circuit; see the **num-queues** command. The SmartEdge OS assigns factory preset, or default, mapping of a priority group to a particular queue, according to the number of queues configured on a circuit; see Table 12-9.

**Table 12-9 Default Mapping of Priority Groups**

| Priority Group | 8 Queues | 4 Queues | 2 Queues | 1 Queue |
|----------------|----------|----------|----------|---------|
| 0              | Queue 0  | Queue 0  | Queue 0  | Queue 0 |
| 1              | Queue 1  | Queue 1  | Queue 1  | Queue 0 |
| 2              | Queue 2  | Queue 1  | Queue 1  | Queue 0 |
| 3              | Queue 3  | Queue 2  | Queue 1  | Queue 0 |
| 4              | Queue 4  | Queue 2  | Queue 1  | Queue 0 |
| 5              | Queue 5  | Queue 2  | Queue 1  | Queue 0 |
| 6              | Queue 6  | Queue 2  | Queue 1  | Queue 0 |
| 7              | Queue 7  | Queue 3  | Queue 1  | Queue 0 |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **exceed mark priority** command, specifying a new value for the *group-num* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

**Note** By default, the SmartEdge OS assigns a priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue priority map using the **qos queue-map** command (in global configuration mode).

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

## Examples

The following example configures the policy to mark all packets that conform to the configured rate with a priority group of 3 and uses the **conform mark** command, which by default, drops all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark priority 3
```

## Related Commands

**conform mark dscp**  
**conform mark precedence**  
**conform mark priority**  
**conform no-action**  
**exceed drop**  
**exceed mark dscp**  
**exceed mark precedence**

**exceed no-action**  
**rate**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate mark priority**  
**violate no-action**

## exceed no-action

**exceed no-action**

{no | default} **exceed no-action**

### Purpose

Specifies that no action is taken on packets that exceed the configured quality of service (QoS) rate and burst tolerance.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Packets exceeding the rate are dropped.

### Usage Guidelines

Use the **exceed no-action** command to specify that no action is taken on packets that exceed the rate.

To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

### Examples

The following example configures the policy to take no action on packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed no-action
```

**Related Commands**

- |                                |                                |
|--------------------------------|--------------------------------|
| <b>conform mark dscp</b>       | <b>exceed mark priority</b>    |
| <b>conform mark precedence</b> | <b>rate</b>                    |
| <b>conform mark priority</b>   | <b>violate drop</b>            |
| <b>conform no-action</b>       | <b>violate mark dscp</b>       |
| <b>exceed drop</b>             | <b>violate mark precedence</b> |
| <b>exceed mark dscp</b>        | <b>violate mark priority</b>   |
| <b>exceed mark precedence</b>  | <b>violate no-action</b>       |

## mark dscp

**mark dscp** *dscp-class*

**no mark dscp** *dscp-class*

### Purpose

Assigns a quality of service (QoS) Differentiated Services Code Point (DSCP) priority to packets.

### Command Mode

metering policy configuration  
policy ACL class configuration  
policing policy configuration

### Syntax Description

*dscp-class*                      Priority with which packets are marked. Values can be:

- Integer from **0** to **63**.
- One of the keywords listed in Table 12-10.

### Default

Packets are not assigned a DSCP priority.

### Usage Guidelines

Use the **mark dscp** command to assign a QoS DSCP priority to packets.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Table 12-10 lists the keywords for the *dscp-class* argument.

**Table 12-10 DSCP Class Keywords**

| DSCP Class                                            | Keyword     | DSCP Class                                       | Keyword                         |
|-------------------------------------------------------|-------------|--------------------------------------------------|---------------------------------|
| Assured Forwarding (AF) Class 1/<br>Drop precedence 1 | <b>af11</b> | Class Selector 0<br>(same as default forwarding) | <b>cs0</b> (same as <b>df</b> ) |
| AF Class 1/Drop precedence 2                          | <b>af12</b> | Class Selector 1                                 | <b>cs1</b>                      |
| AF Class 1/Drop precedence 3                          | <b>af13</b> | Class Selector 2                                 | <b>cs2</b>                      |
| AF Class 2/Drop precedence 1                          | <b>af21</b> | Class Selector 3                                 | <b>cs3</b>                      |
| AF Class 2/Drop precedence 2                          | <b>af22</b> | Class Selector 4                                 | <b>cs4</b>                      |

**Table 12-10 DSCP Class Keywords** (*continued*)

| DSCP Class                   | Keyword     | DSCP Class                                       | Keyword                         |
|------------------------------|-------------|--------------------------------------------------|---------------------------------|
| AF Class3/Drop precedence 3  | <b>af23</b> | Class Selector 5                                 | <b>cs5</b>                      |
| AF Class 3/Drop precedence 1 | <b>af31</b> | Class Selector 6                                 | <b>cs6</b>                      |
| AF Class 3/Drop precedence 2 | <b>af32</b> | Class Selector 7                                 | <b>cs7</b>                      |
| AF Class 3/Drop precedence 3 | <b>af33</b> | Default Forwarding<br>(same as Class Selector 0) | <b>df</b> (same as <b>cs0</b> ) |
| AF Class 4/Drop precedence 1 | <b>af41</b> | Expedited Forwarding                             | <b>ef</b>                       |
| AF Class 4/Drop precedence 2 | <b>af42</b> |                                                  |                                 |
| AF Class 4/Drop precedence 3 | <b>af43</b> |                                                  |                                 |

**Note** RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, defines the Class Selector code points.

Use the **no** form of this command to return to the default behavior where packets are assigned a DSCP priority.

## Examples

The following example configures the policy, `GE-in policing`, to mark all packets within the `VOIP` class as high-priority packets, while all packets within the `best-effort` class are marked as low-priority packets:

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl cont2
[local]Redback(config-policy-acl)#class VOIP
[local]Redback(config-policy-acl-class)#mark dscp ef
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class best-effort
[local]Redback(config-policy-acl-class)#mark dscp df
```

## Related Commands

**conform mark dscp**  
**exceed mark dscp**  
**mark precedence**



## mark precedence

**mark precedence** *prec-value*

**no mark precedence** *prec-value*

### Purpose

Assigns a quality of service (QoS) drop precedence value to packets corresponding to the assured forwarding (AF) class of the packets.

### Command Mode

metering policy configuration  
policy ACL class configuration  
policing policy configuration

### Syntax Description

*prec-value*                      Drop precedence value. The range of values is 1 to 3.

### Default

Packets are not marked with an explicit drop precedence value.

### Usage Guidelines

Use the **mark precedence** command to assign a QoS drop precedence value to packets.

In general, the level of forwarding assurance of an IP packet is based on: (1) the resources allocated to the AF class to which the packet belongs, (2) the current load of the AF class, and, in case of congestion within the class, (3) the drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the assured forwarding (AF) Differentiated Services Code Point (DSCP) class. Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded. (For more information see RFC 2597, *Assured Forwarding PHB Group*.)

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **mark precedence** command, specifying a new value for the *prec-value* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** form of this command to return to the default behavior where packets are not marked with a drop precedence value.

### Examples

The following example configures the policy, `GE-in policing`, to mark all packets within the `VOIP` class as preferred packets, while all packets within the `best-effort` class are marked as less-preferred packets:

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl cont2
[local]Redback(config-policy-acl)#class VOIP
[local]Redback(config-policy-acl-class)#mark precedence 1
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class best-effort
[local]Redback(config-policy-acl-class)#mark precedence 3
```

### Related Commands

**conform mark precedence**  
**exceed mark precedence**  
**mark dscp**

## mark priority

**mark priority** *group-num*

**no mark priority**

### Purpose

Marks packets that are associated with a quality of service (QoS) priority group number.

### Command Mode

metering policy configuration  
policy ACL class configuration  
policing policy configuration

### Syntax Description

*group-num*                      Priority group number. The range of values is 0 to 7.

### Default

Packets are not marked with a priority group number.

### Usage Guidelines

Use the **mark priority** command to mark packets with a QoS priority group number.

A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not being changed by this command. The actual queue number depends upon the number of queues configured on the circuit; see the **num-queues** command.

The SmartEdge OS assigns factory preset, or default, mapping of a priority group to a particular queue, according to the number of queues configured on a circuit; see Table 12-11.

**Table 12-11 Default Mapping of Priority Groups**

| Priority Group | 8 Queues | 4 Queues | 2 Queues | 1 Queue |
|----------------|----------|----------|----------|---------|
| 0              | Queue 0  | Queue 0  | Queue 0  | Queue 0 |
| 1              | Queue 1  | Queue 1  | Queue 1  | Queue 0 |
| 2              | Queue 2  | Queue 1  | Queue 1  | Queue 0 |
| 3              | Queue 3  | Queue 2  | Queue 1  | Queue 0 |
| 4              | Queue 4  | Queue 2  | Queue 1  | Queue 0 |
| 5              | Queue 5  | Queue 2  | Queue 1  | Queue 0 |
| 6              | Queue 6  | Queue 2  | Queue 1  | Queue 0 |
| 7              | Queue 7  | Queue 3  | Queue 1  | Queue 0 |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **mark priority** command, specifying a new value for the *group-num* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

**Note** By default, the SmartEdge OS assigns a priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue priority map through the **qos queue-map** command (in global configuration mode).

Use the **no** form of this command to return to the default behavior where packets are not marked with an explicit priority queuing value.

## Examples

The following example configures the policy, `GE-in policing`, to mark all packets within the `VOIP` class as high-priority packets, while all packets within the `best-effort` class are marked as low-priority packets:

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl cont2
[local]Redback(config-policy-acl)#class VOIP
[local]Redback(config-policy-acl-class)#mark priority 2
[local]Redback(config-policy-acl-class)#exit
[local]Redback(config-policy-acl)#class best-effort
[local]Redback(config-policy-acl-class)#mark priority 7
```

## Related Commands

**conform mark priority**  
**exceed mark priority**  
**qos queue-map**

## qos policy metering

**qos policy *pol-name* metering**

**no qos policy *pol-name* metering**

### Purpose

Creates or selects a quality of service (QoS) metering policy and enters metering policy configuration mode.

### Command Mode

global configuration

### Syntax Description

*pol-name*                      Name of the metering policy.

### Default

No metering policy is created.

### Usage Guidelines

Use the **qos policy metering** command to create or select a metering policy and enter metering policy configuration mode.

**Note** Link group support for QoS metering policies is limited to Multilink Point-to-Point Protocol (MP) and Multilink Frame Relay (MFR) bundles.

**Note** Virtual LAN (VLAN) bridge circuits and Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) circuits do not support policy access control lists (ACLs), classes, and actions within classes. Rate limiting is supported; however, the **conform dscp**, **mark dscp**, **exceed dscp**, and **mark precedence** commands (in metering policy configuration mode) are not allowed.

Use the **no** form of this command in global configuration mode to delete a metering policy.

### Examples

The following example creates the metering policy, `example2`, and attaches it to an Ethernet port:

```
[local]Redback(config)#qos policy example2 metering
[local]Redback(config-policy-metering)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-metering)#exit
```

### Related Commands

**qos policy policing**

## qos policy policing

**qos policy** *pol-name* **policing**

**no qos policy** *pol-name* **policing**

### Purpose

Creates or selects a quality of service (QoS) policing policy and enters policing policy configuration mode.

### Command Mode

global configuration

### Syntax Description

*pol-name*            Name of the policing policy to be attached.

### Default

No policing policy is created.

### Usage Guidelines

Use the **qos policy policing** command to create or select a policing policy and enter policing policy configuration mode.

**Note** Link group support for QoS policing policies is limited to Multilink Point-to-Point Protocol (MP) and Multilink Frame Relay (MFR) bundles.

**Note** Virtual LAN (VLAN) bridge circuits and Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) circuits do not support policy access control lists (ACLs), classes, and actions within classes. Rate limiting is supported; however, the **conform dscp**, **mark dscp**, **exceed dscp**, and **mark precedence** commands (in policing policy configuration mode) are not allowed.

Use the **no** form of this command to delete a policing policy.

### Examples

The following example creates the `example2` policing policy:

```
[local]Redback(config)#qos policy example2 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
```

The following example creates the **WholePort** policing policy for an Ethernet port and the **OneVC** policing policy for an 802.1Q PVC on that port. When the **OneVC** policy is attached to the PVC, it supersedes the **WholePort** policy attached to the port for that PVC; for all the other PVCs on the port, the policy attached to the port takes effect.

```
[local]Redback(config)#qos policy OneVC policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark dscp ef
[local]Redback(config-policy-rate)#exceed mark dscp df
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#qos policy WholePort policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
```

## Related Commands

**qos policy metering**

## rate

**rate** [**informational**] *kbps* **burst** *bytes* [**excess-burst** *bytes* [**counters**] | **counters**]

**no rate**

### Purpose

Sets the rate, burst tolerance, and excess burst tolerance for traffic on the circuit, port, or subscriber record to which the quality of service (QoS) policy is attached, or for a policy ACL class of traffic for that policy.

### Command Mode

metering policy configuration  
 policing policy configuration  
 policy ACL class configuration

### Syntax Description

|                                  |                                                                                                                                                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>informational</b>             | Optional. Specifies the rate to be used by the system only to calculate a percentage rate for a policy ACL class when you specify the class rate as a percentage. The effect is that the overall circuit is not rate limited. |
| <i>kbps</i>                      | Rate in kilobits per second. The range of values is 5 to 1,000,000.                                                                                                                                                           |
| <b>burst</b> <i>bytes</i>        | Burst tolerance in bytes. The range of values is 1 to 12,000,000.                                                                                                                                                             |
| <b>excess-burst</b> <i>bytes</i> | Optional. Excess burst tolerance in bytes. The range of values is 1 to 12,000,000.                                                                                                                                            |
| <b>counters</b>                  | Optional. Logs statistics related to packets that conform to or exceed the rate.                                                                                                                                              |

### Default

Rate is calculated based on the default values for the *kbps* and *bytes* arguments.

### Usage Guidelines

Use the **rate** command to set the rate, burst tolerance, and excess-burst for traffic on the port, circuit, or subscriber record to which the QoS policy is attached, or for a policy ACL class of traffic for that policy. If entered in metering or policing policy configuration mode, this command accesses policy rate configuration mode; if entered in policy ACL class configuration mode, this command accesses policy class rate configuration mode.

Use the **informational** keyword to specify that the policy rate will not be used to enforce an overall circuit rate limit, but will be used only to calculate the class rate if you specify the rate for an ACL class as a percentage of the policy rate, using the **rate percentage** command (in policy ACL class configuration mode). This keyword is not available in policy ACL class configuration mode.

Use the **excess-burst** *bytes* construct to optionally configure the excess burst tolerance. The burst tolerance and excess burst tolerance are thresholds that can be used to determine the traffic rate at which packets can be dropped or marked.



For more information about dropping or marking packets when the traffic rate exceeds the burst tolerance, but does not exceed the excess burst tolerance, see the **exceed** commands. For more information about dropping or marking packets when the traffic rate exceeds the excess burst tolerance, see the **violate** commands.

Use the **no** form of this command to specify the default traffic rate and burst tolerance.

**Note** The maximum rate set by the **qos rate** command (in port configuration mode) is the rate at which the port, 802.1Q tunnel, or 802.1Q PVC operates; any priority queuing (PQ), enhanced deficit round-robin (EDRR), or priority weighted-fair queuing (PWFQ) queue or circuit with a PQ, EDRR, or PWFQ policy is limited by the rate specified by that command for the circuit. Also, the sum of all traffic on the port carried by the queues belonging to the circuits or subscribers is limited to the rate specified by that command.

## Examples

The following example marks all traffic conforming to the configured policy rate with expedited forwarding (ef) and marks traffic that exceeds the policy rate with default forwarding (df):

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#rate 6000000 burst 10000 counters
[local]Redback(config-policy-rate)#conform mark dscp ef
[local]Redback(config-policy-rate)#exceed mark dscp df
```

By including the **counters** keyword in the **rate** command, you can use the **show circuit counters** command (in any mode) with the **detail** keyword to display the number of packets that conform to the rate and the number of packets that exceed the rate.

## Related Commands

|                                |                                |
|--------------------------------|--------------------------------|
| <b>conform mark dscp</b>       | <b>qos rate</b>                |
| <b>conform mark precedence</b> | <b>rate percentage</b>         |
| <b>conform mark priority</b>   | <b>violate drop</b>            |
| <b>exceed drop</b>             | <b>violate mark dscp</b>       |
| <b>exceed mark dscp</b>        | <b>violate mark precedence</b> |
| <b>exceed mark precedence</b>  | <b>violate mark priority</b>   |
| <b>exceed mark priority</b>    | <b>violate no-action</b>       |
| <b>exceed no-action</b>        |                                |

## rate percentage

**rate percentage** *percent-rate* [**counters**]

**no rate percentage**

### Purpose

Assigns a percentage of the overall policy rate to this class of traffic on the circuit, port, or subscriber record to which the quality of service (QoS) policy is attached and accesses policy class rate configuration mode.

### Command Mode

policy ACL class configuration

### Syntax Description

|                     |                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------|
| <i>percent-rate</i> | Relative class rate, as a percentage of the policy rate, for this class. The range of values is 1 to 100. |
| <b>counters</b>     | Optional. Logs statistics related to packets that conform to or exceed the rate.                          |

### Default

No rate percentage is specified for this class.

### Usage Guidelines

Use the **rate percentage** command to assign a percentage (a relative class rate) of the overall policy rate to this class of traffic on the circuit, port, or subscriber record to which the QoS policy is attached, and access policy class rate configuration mode. The percentage applies to the policy rate, burst, and excess burst values.

Use the **no** form of this command to remove the rate percentage from this class configuration.

**Note** The maximum rate set by the **qos rate** command (in port configuration mode) is the rate at which the port, 802.1Q tunnel, or 802.1Q permanent virtual circuit (PVC) operates; any priority queuing (PQ), enhanced deficit round-robin (EDRR), or priority weighted-fair queuing (PWFQ) queue or circuit with a PQ, EDRR, or PWFQ policy is limited by the rate specified by that command for the circuit. Also, the sum of all traffic on the port carried by the queues belonging to the circuits or subscribers is limited to the rate specified by that command.

## Examples

The following example assigns 25 percent of the policy rate to the **realtime** class:

```
[local]Redback(config)#qos policy rate-incoming policing
[local]Redback(config-policy-policing)#rate informational 6000000 burst 10000 counters
[local]Redback(config-policy-policing)#access-group Class local
[local]Redback(config-policy-policy-acl)#class realtime
[local]Redback(config-policy-policy-acl-class)#rate percentage 25
```

By including the **counters** keyword in the **rate percentage** command, you can use the **show circuit counters** command (in any mode) with the **detail** keyword to display the number of packets that conform to the rate percentage and the number of packets that exceed that rate percentage.

## Related Commands

|                                |                                |
|--------------------------------|--------------------------------|
| <b>conform mark dscp</b>       | <b>qos rate</b>                |
| <b>conform mark precedence</b> | <b>rate</b>                    |
| <b>conform mark priority</b>   | <b>violate drop</b>            |
| <b>exceed drop</b>             | <b>violate mark dscp</b>       |
| <b>exceed mark dscp</b>        | <b>violate mark precedence</b> |
| <b>exceed mark precedence</b>  | <b>violate mark priority</b>   |
| <b>exceed mark priority</b>    | <b>violate no-action</b>       |
| <b>exceed no-action</b>        |                                |

## violate drop

**violate drop**

{no | default} **violate drop**

### Purpose

Drops packets that exceed the configured excess burst tolerance.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Packets exceeding the configured excess burst tolerance are dropped.

### Usage Guidelines

Use the **violate drop** command to drop packets that exceed the configured excess burst tolerance. Use this command as part of a policing policy for incoming packets and as part of a metering policy for outgoing packets.

To configure the excess burst tolerance, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode). The following conditions determine how packets are dropped:

- If the excess burst tolerance is not configured, all packets exceeding the configured burst tolerance are dropped.
- If the excess burst tolerance is configured, all packets that exceed the excess burst tolerance are dropped.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

**Note** Use the **exceed drop** commands (in policy class rate and policy rate configuration modes) to specify how packets are dropped when the traffic rate does not exceed the configured excess burst tolerance.

Use the **no** or **default** form of this command to drop packets that exceed the configured excess-burst tolerance.

## Examples

The following example drops packets that exceed the excess burst tolerance:

```
[local]Redback(config)#qos policy protection1 policing  
[local]Redback(config-policy-policing)#rate 10000 burst 100000 excess-burst 120000  
[local]Redback(config-policy-rate)#violate drop
```

## Related Commands

|                                |                                |
|--------------------------------|--------------------------------|
| <b>conform mark dscp</b>       | <b>exceed mark priority</b>    |
| <b>conform mark precedence</b> | <b>exceed no-action</b>        |
| <b>conform mark priority</b>   | <b>rate</b>                    |
| <b>conform no-action</b>       | <b>violate mark dscp</b>       |
| <b>exceed drop</b>             | <b>violate mark precedence</b> |
| <b>exceed mark dscp</b>        | <b>violate mark priority</b>   |
| <b>exceed mark precedence</b>  | <b>violate no-action</b>       |

# violate mark dscp

**violate mark dscp** *dscp-class*

{**no** | **default**} **violate mark dscp**

## Purpose

Marks packets that exceed the configured excess burst tolerance with a Differentiated Services Code Point (DSCP) value.

## Command Mode

policy class rate configuration

policy rate configuration

## Syntax Description

- dscp-class*                      Priority with which packets exceeding the rate are marked. Values can be:
- An integer from **0** to **63**.
  - One of the keywords listed in Table 12-12.

## Default

Packets exceeding the configured excess burst tolerance are dropped.

## Usage Guidelines

Use the **violate mark dscp** command to mark packets that exceed the configured excess burst tolerance with a DSCP value.

To configure the excess burst tolerance, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode). Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **violate mark dscp** command, specifying a new value for the *dscp-class* argument, which supersedes the one previously configured.

Table 12-12 lists the keywords for the *dscp-class* argument.

**Table 12-12 DSCP Class Keywords**

| DSCP Class                                         | Keyword     | DSCP Class                                    | Keyword                         |
|----------------------------------------------------|-------------|-----------------------------------------------|---------------------------------|
| Assured Forwarding (AF) Class 1 /Drop precedence 1 | <b>af11</b> | Class Selector 0 (same as default forwarding) | <b>cs0</b> (same as <b>df</b> ) |
| AF Class 1/Drop precedence 2                       | <b>af12</b> | Class Selector 1                              | <b>cs1</b>                      |
| AF Class 1/Drop precedence 3                       | <b>af13</b> | Class Selector 2                              | <b>cs2</b>                      |
| AF Class 2/Drop precedence 1                       | <b>af21</b> | Class Selector 3                              | <b>cs3</b>                      |
| AF Class 2/Drop precedence 2                       | <b>af22</b> | Class Selector 4                              | <b>cs4</b>                      |
| AF Class3/Drop precedence 3                        | <b>af23</b> | Class Selector 5                              | <b>cs5</b>                      |

**Table 12-12 DSCP Class Keywords** (*continued*)

| DSCP Class                   | Keyword     | DSCP Class                                       | Keyword                         |
|------------------------------|-------------|--------------------------------------------------|---------------------------------|
| AF Class 3/Drop precedence 1 | <b>af31</b> | Class Selector 6                                 | <b>cs6</b>                      |
| AF Class 3/Drop precedence 2 | <b>af32</b> | Class Selector 7                                 | <b>cs7</b>                      |
| AF Class 3/Drop precedence 3 | <b>af33</b> | Default Forwarding<br>(same as Class Selector 0) | <b>df</b> (same as <b>cs0</b> ) |
| AF Class 4/Drop precedence 1 | <b>af41</b> | Expedited Forwarding                             | <b>ef</b>                       |
| AF Class 4/Drop precedence 2 | <b>af42</b> |                                                  |                                 |
| AF Class 4/Drop precedence 3 | <b>af43</b> |                                                  |                                 |

**Note** RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, defines the Class Selector code points.



**Caution** Risk of packet reordering. To reduce the risk, ensure that the marking of conforming packets and exceeding packets differ only within a major DSCP class. Major DSCP classes are identified by the Class Selector code, and include CS0=DF, CS1=AF11, AF12, AF13, CS2=AF21, AF22, AF23, CS3=AF31, AF32, AF33, CS4=AF41, AF42, AF43, and CS5=EF. For example, if you mark conforming packets with AF11 and you want to avoid reordering, mark exceeding packets with AF11, AF12, or AF13 only.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the excess burst tolerance.

## Examples

The following example configures the policy to mark all packets that exceed the excess burst tolerance with a DSCP value representing a high priority:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000 excess-burst 120000
[local]Redback(config-policy-rate)#violate mark dscp ef
```

### Related Commands

conform mark dscp  
conform mark precedence  
conform mark priority  
conform no-action  
exceed drop  
exceed mark dscp  
exceed mark precedence

exceed mark priority  
exceed no-action  
rate  
violate drop  
violate mark precedence  
violate mark priority  
violate no-action



## violate mark precedence

**violate mark precedence** *prec-value*

{**no** | **default**} **violate mark precedence**

### Purpose

Marks packets that exceed the configured excess burst tolerance with a drop precedence value corresponding to the assured forwarding (AF) class of the packet.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*prec-value*

Drop precedence bits value. The range of values is 1 to 3.

### Default

Packets exceeding the excess burst tolerance are dropped.

### Usage Guidelines

Use the **violate mark precedence** command to mark packets that exceed the configured excess burst tolerance with a drop precedence value corresponding to the AF class of the packet.

To configure the excess burst tolerance, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

In general, the level of forwarding assurance of an IP packet is based on: (1) the resources allocated to the AF class to which the packet belongs, (2) the current load of the AF class, and, in case of congestion within the class, (3) the drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 12-13 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

**Table 12-13 Drop Precedence Values**

| DSCP Value of an Incoming Packet | Packet is Tagged with a Drop Precedence Value | DSCP Value of the Outgoing Packet |
|----------------------------------|-----------------------------------------------|-----------------------------------|
| AF11, AF12, AF13                 | 1                                             | AF11                              |
| AF21, AF22, AF23                 |                                               | AF21                              |
| AF31, AF32, AF33                 |                                               | AF31                              |
| AF41, AF42, AF43                 |                                               | AF41                              |

**Table 12-13 Drop Precedence Values** (*continued*)

| DSCP Value of an Incoming Packet | Packet is Tagged with a Drop Precedence Value | DSCP Value of the Outgoing Packet |
|----------------------------------|-----------------------------------------------|-----------------------------------|
| AF11, AF12, AF13                 | 2                                             | AF12                              |
| AF21, AF22, AF23                 |                                               | AF22                              |
| AF31, AF32, AF33                 |                                               | AF32                              |
| AF41, AF42, AF43                 |                                               | AF42                              |
| AF11, AF12, AF13                 | 3                                             | AF13                              |
| AF21, AF22, AF23                 |                                               | AF23                              |
| AF31, AF32, AF33                 |                                               | AF33                              |
| AF41, AF42, AF43                 |                                               | AF43                              |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **violate mark precedence** command, specifying a new value for the *prec-value* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the excess burst tolerance.

## Examples

The following example configures the policy to mark all packets that exceed the configured burst tolerance with an IP precedence value of 3:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000 excess-burst 120000
[local]Redback(config-policy-rate)#violate mark precedence 3
```

## Related Commands

|                                |                              |
|--------------------------------|------------------------------|
| <b>conform mark dscp</b>       | <b>exceed mark priority</b>  |
| <b>conform mark precedence</b> | <b>exceed no-action</b>      |
| <b>conform mark priority</b>   | <b>rate</b>                  |
| <b>conform no-action</b>       | <b>violate drop</b>          |
| <b>exceed drop</b>             | <b>violate mark dscp</b>     |
| <b>exceed mark dscp</b>        | <b>violate mark priority</b> |
| <b>exceed mark precedence</b>  | <b>violate no-action</b>     |

## violate mark priority

**violate mark priority** *group-num*

{**no** | **default**} **violate mark priority**

### Purpose

Marks packets that exceed the excess burst tolerance with a priority group number.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

*group-num*                      Priority group number. The range of values is 0 to 7.

### Default

Packets exceeding the excess burst tolerance are dropped.

### Usage Guidelines

Use the **violate mark priority** command to mark packets that exceed the excess burst tolerance with a priority group number. To configure the excess burst tolerance, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not being changed by this command. The actual queue number depends upon the number of queues configured on the circuit; see the **num-queues** command. The SmartEdge OS assigns factory preset, or default, mapping of a priority group to a particular queue, according to the number of queues configured on a circuit; see Table 12-14.

**Table 12-14 Default Mapping of Priority Groups**

| Priority Group | 8 Queues | 4 Queues | 2 Queues | 1 Queue |
|----------------|----------|----------|----------|---------|
| 0              | Queue 0  | Queue 0  | Queue 0  | Queue 0 |
| 1              | Queue 1  | Queue 1  | Queue 1  | Queue 0 |
| 2              | Queue 2  | Queue 1  | Queue 1  | Queue 0 |
| 3              | Queue 3  | Queue 2  | Queue 1  | Queue 0 |
| 4              | Queue 4  | Queue 2  | Queue 1  | Queue 0 |
| 5              | Queue 5  | Queue 2  | Queue 1  | Queue 0 |
| 6              | Queue 6  | Queue 2  | Queue 1  | Queue 0 |
| 7              | Queue 7  | Queue 3  | Queue 1  | Queue 0 |

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **violate mark priority** command, specifying a new value for the *group-num* argument, which supersedes the one previously configured.



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

**Note** By default, the SmartEdge OS assigns a priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue priority map through the **qos queue-map** command (in global configuration mode).

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the excess burst tolerance.

## Examples

The following example configures the policy to mark all packets that exceed the configured burst tolerance with a priority group of 3:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000 excess-burst 120000
[local]Redback(config-policy-rate)#violate mark priority 3
```

## Related Commands

**conform mark dscp**  
**conform mark precedence**  
**conform mark priority**  
**conform no-action**  
**exceed drop**  
**exceed mark dscp**  
**exceed mark precedence**

**exceed mark priority**  
**exceed no-action**  
**rate**  
**violate drop**  
**violate mark dscp**  
**violate mark precedence**  
**violate no-action**

## violate no-action

**violate no-action**

{no | default} **violate no-action**

### Purpose

Specifies that no action is taken on packets that exceed the configured excess burst tolerance.

### Command Mode

policy class rate configuration

policy rate configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Packets exceeding the excess burst tolerance are dropped.

### Usage Guidelines

Use the **violate no-action** command to specify that no action is taken on packets that exceed the excess burst tolerance.

To configure the excess burst tolerance, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).



**Caution** Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines:

- Circuit-based marking overrides class-based marking.
- Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the excess burst tolerance.

### Examples

The following example configures the policy to take no action on packets that exceed the configured excess burst tolerance:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000 excess-burst 120000
[local]Redback(config-policy-rate)#violate no-action
```

### Related Commands

conform mark dscp  
conform mark precedence  
conform mark priority  
conform no-action  
exceed drop  
exceed mark dscp  
exceed mark precedence

exceed mark priority  
exceed no-action  
rate  
violate drop  
violate mark dscp  
violate mark precedence  
violate mark priority

# QoS Scheduling Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS quality of service (QoS) scheduling policy features.

For information about other QoS configuration tasks and commands, see the following chapters:

- Chapter 12, “QoS Rate- and Class-Limiting Configuration”—Rate- and class-limiting features (metering and policing policies)
- Chapter 14, “QoS Circuit Configuration”—Port, channel, and circuit configuration for all QoS policies and features

For information about the tasks and commands used to monitor, troubleshoot, and administer QoS, see the “QoS Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

**Note** In this chapter, the term, first-generation Asynchronous Transfer Mode (ATM) OC traffic card, refers to a 2-port ATM OC-3c/STM-1c or ATM OC-12c/STM-4c traffic card; similarly, the term, second-generation ATM OC traffic card, refers to a 4-port ATM OC-3c/STM-1c or Enhanced ATM OC-12c/STM-4c traffic card.

The term, traffic-managed circuit, refers to a circuit or port on a Gigabit Ethernet 3 (GE3) or Gigabit Ethernet 1020 (GE1020) traffic card.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

QoS scheduling policies create and enforce levels of service and bandwidth rates, and prioritize how packets are scheduled into egress queues. Incoming queues on outbound traffic cards have associated scheduling parameters such as rates, depths, and relative weights. The traffic card's scheduler draws packets from the incoming queues based on weight, rate, or strict priority:

- A packet can be dropped when queues back up over a configured discard threshold or because of an parameter setting.
- If a packet is not dropped, it is scheduled into an output queue based on its priority group or its scheduling policy.

After classification, marking, and rate-limiting occurs on an incoming packet, the packet is placed into an output queue for servicing by an egress traffic card's scheduler. The SmartEdge OS supports up to eight queues per circuit. Queues are serviced according to a queue map scheme, a QoS scheduling policy, or both, as described in the following sections:

- Queue Maps
- Priority Queuing Policies
- Enhanced Deficit Round-Robin Policies
- Asynchronous Transfer Mode Weighted Fair Queuing Policies
- Priority Weighted Fair Queuing Policies
- Congestion Management and Avoidance

## Queue Maps

By default, the SmartEdge OS assigns a priority group number to an egress queue, according to the number of queues configured on a circuit; see Table 13-1.

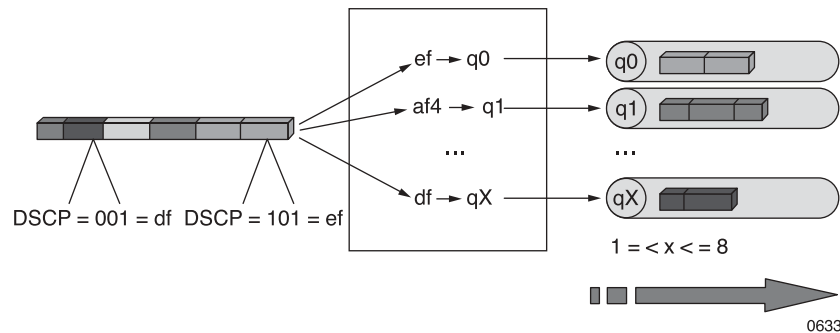
**Table 13-1 Default Mapping of Packets into Queues Using Priority Groups**

| Priority Group | DSCP Value                      | IP Prec | MPLS EXP | 802.1p | 8 Queues | 4 Queues | 2 Queues | 1 Queue |
|----------------|---------------------------------|---------|----------|--------|----------|----------|----------|---------|
| 0              | Network control                 | 7       | 7        | 7      | Queue 0  | Queue 0  | Queue 0  | Queue 0 |
| 1              | Reserved                        | 6       | 6        | 6      | Queue 1  | Queue 1  | Queue 1  | Queue 0 |
| 2              | Expedited Forwarding (EF)       | 5       | 5        | 5      | Queue 2  | Queue 1  | Queue 1  | Queue 0 |
| 3              | Assured Forwarding (AF) level 4 | 4       | 4        | 4      | Queue 3  | Queue 2  | Queue 1  | Queue 0 |
| 4              | AF level 3                      | 3       | 3        | 3      | Queue 4  | Queue 2  | Queue 1  | Queue 0 |
| 5              | AF level 2                      | 2       | 2        | 2      | Queue 5  | Queue 2  | Queue 1  | Queue 0 |
| 6              | AF level 1                      | 1       | 1        | 1      | Queue 6  | Queue 2  | Queue 1  | Queue 0 |
| 7              | Default Forwarding (DF)         | 0       | 0        | 0      | Queue 7  | Queue 3  | Queue 1  | Queue 0 |



You can configure a customized queue map and assign it to any scheduling policy. The map overrides the default mapping of packets into the egress queues of the policy to which it is assigned; see Figure 13-1. When the scheduling policy is attached to a circuit, it overrides the default queue map. You can configure up to three customized queue maps.

**Figure 13-1 Queue Map**



## Priority Queuing Policies

When a priority queuing (PQ) policy is enabled on a circuit, its output queues are serviced in strict priority order; that is, packets waiting in the highest-priority queue (queue 0) are serviced until that queue is empty, then packets waiting in the second-highest priority queue are serviced (queue 1), and so on. Under congestion, a PQ policy allows the highest priority traffic to get through, at the expense of lower-priority traffic.

With a PQ policy, the potential exists for a high volume of high-priority traffic to completely starve low-priority traffic. To prevent such starvation, the SmartEdge OS allows a rate limit to be configured on each queue, which limits the amount of bandwidth available to a high priority queue. With careful tuning of the rate limits, you can prevent the lower priority queues from being starved.

**Note** PQ policies are not supported on ATM DS-3 and second-generation ATM OC traffic cards.

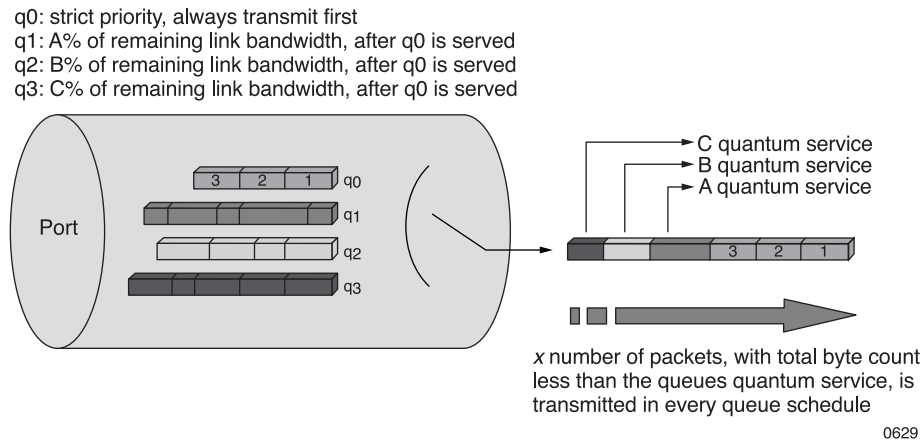
## Enhanced Deficit Round-Robin Policies

Enhanced deficit round-robin (EDRR) policies can operate in one of three modes: normal, strict, or alternate. In normal mode, queue 0 is treated like all other queues on a circuit. Each queue receives its share of the circuit's bandwidth according to the weight assigned to the queue. In strict mode, queue 0 always has priority over all other queues configured on a circuit. In alternate mode, the servicing of queues alternates between queue 0 and the remaining queues. Queue 0 is served, then the next queue is served. Queue 0 is served again, and the next queue in turn is served, and so on. For example, if there are four queues configured, the order of servicing will be q0, q1, q0, q2, q0, q3, q0, q1, and so on. With strict mode, queue 0 can starve other queues if there are always packets waiting in queue 0. To prevent such starvation, the SmartEdge OS supports alternating mode so that, in every other round, either queue 0 or one of the other queues on the circuit is served, in alternating fashion.

With EDRR policies, each queue has an associated quantum value and a deficit counter. The quantum value is derived from the configured weight of the queue. A quantum value is the average number of bytes served in each round; the deficit counter is initialized to the quantum value. Packets in a queue are served as long as the deficit counter is greater than zero. Each packet served decreases the deficit counter by a value equal to its length in bytes. At each new round, each nonempty queue's deficit counter is incremented by its quantum value; see Figure 13-2.

**Note** EDRR policies are not supported on ATM DS-3 and second-generation ATM OC traffic cards.

**Figure 13-2 EDRR Strict Mode Scheduling**



## Asynchronous Transfer Mode Weighted Fair Queuing Policies

Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policies ensure that queues do not starve for bandwidth and that traffic obtains predictable service. These policies operate in one of two modes: alternate and strict. In either mode, the ATM segmentation and reassembly (SAR) uses a class-based WFQ algorithm to perform QoS priority packet scheduling. In strict mode, queue 0 is serviced immediately and the other queues are serviced in a round-robin fashion according to their configured weights. In alternate mode, the servicing of queues alternates between queue 0 and the remaining queues, according to their configured weights. Queue 0 is served, then the next queue is served. Queue 0 is served again, and the next queue in turn is served, and so on. For example, if there are four queues configured, the order of servicing will be q0, q1, q0, q2, q0, q3, q0, q1, and so on.

**Note** ATMWFQ policies are not supported on first-generation ATM OC traffic cards.

## Priority Weighted Fair Queuing Policies

Priority weighted fair queuing (PWFQ) policies use a priority- and a weight-based algorithm to implement hierarchical QoS-aware scheduling. Each queue in the policy includes both a priority and a relative weight, which control how each queue is serviced. Inside the PWFQ policy, priority takes precedence, and for queues placed at the same priority, the individual configured weight defines how the queue is used in the scheduling decision.

Hierarchical scheduling provides the means to perform scheduling at the port, 802.1Q tunnel, and 802.1Q permanent virtual circuit (PVC) levels, using PWFQ policies. It also provides the means to perform QoS shaping for subscriber sessions using PWFQ policies attached to hierarchical nodes and node groups, so that four levels of scheduling are possible (hierarchical node, 802.1Q PVC, 802.1Q tunnel, port levels). Scheduling modes include:

- **Strict**—Each queue is assigned a unique priority and is serviced according to its priority. The relative weight does not affect the scheduling.
- **Normal**—All queues are assigned the same priority. Each queue is serviced in round-robin order, according to the assigned relative weight, which is a percentage of the available bandwidth.
- **Strict + Normal**—Strict and normal modes are combined. Multiple queues can be assigned the same priority (forming a priority group); the queues in each group are serviced in round-robin order with each queue receiving the percentage of the group's bandwidth assigned to it by the relative weight.

**Note** PWFQ policies and hierarchical scheduling and shaping are supported only for GE3 and GE1020 traffic cards.

## Congestion Management and Avoidance

The SmartEdge OS employs the following congestion avoidance features when processing packets using the different queuing and scheduling policies:

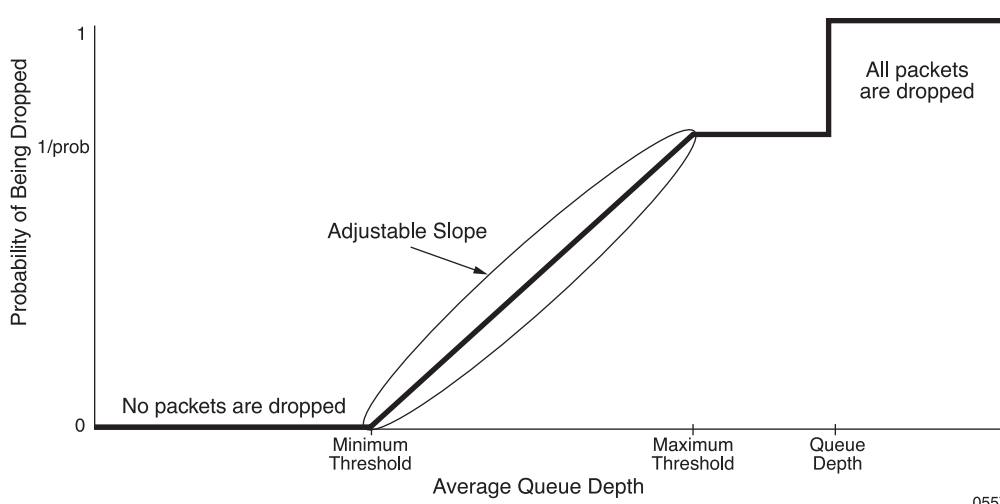
- Random Early Detection
- Early Packet Discard
- Multidrop Precedence
- Congestion Avoidance Maps
- Queue Depth
- Queue Rates

### Random Early Detection

With scheduling policies, you can configure random early detection (RED) parameters to manage buffer congestion by signaling to sources of traffic that the network is on the verge of entering a congested state, rather than waiting until the network is actually congested. The technique is to drop packets with a probability that varies as a function of how many packets are waiting in a queue at any particular time, and the minimum and maximum average queue depth.

When a queue is nearly empty, the probability of dropping a packet is small. As the queue's average depth increases, the likelihood of dropping packets becomes greater; see Figure 13-3.

**Note** For ATM DS-3 and second-generation ATM OC traffic cards, the queue depth value is equal to the value configured for the maximum threshold.

**Figure 13-3 Probability of Being Dropped as a Function of Queue Depth**

## Early Packet Discard

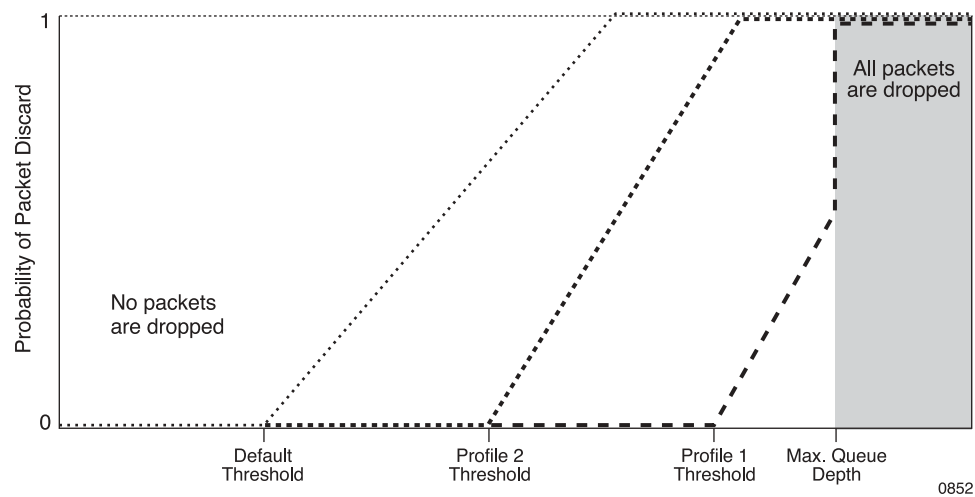
With ATMWFQ policies, you can also configure early packet discard (EPD), a congestion avoidance mechanism that starts dropping packets after queues reach the EPD threshold. When queue buffers are nearly full (reaching the EPD threshold), the system is signaled that it may become congested. Any packets trying to enter queues, after the EPD threshold has been met, are dropped.

## Multidrop Precedence

With ATMWFQ and PWFQ policies, you can configure different congestion behaviors that depend on the DSCP values of the packets in a queue; this feature is referred to as multidrop precedence. Multidrop precedence supports up to three profiles for each queue, and each profile defines a different congestion behavior for one or more DSCP values. Each profile is also characterized by its RED parameter values. The DSCP value in the packet is used to select the profile that governs its congestion avoidance behavior.

Figure 13-4 shows how the three profiles can be defined with different minimum and maximum thresholds. Multidrop profiles are available only for ATMWFQ and PWFQ policies and are configured using congestion avoidance maps.

Figure 13-4 Multidrop Profiles



## Congestion Avoidance Maps

A congestion avoidance map specifies how congestion avoidance is managed for a set of queues. Each map supports eight queues.

**Note** Congestion avoidance maps are supported only for ATMWFQ and PWFQ policies.

For each queue, you define up to three profiles, each of which describes the congestion behavior for one or more DSCP values. The map specifies RED parameters for every queue. One of the profiles, the default profile, specifies the default congestion behavior for every DSCP value.

When you define either of the other profiles for a queue, the system removes the DSCP values that you specify from the default profile. If a congestion map is not assigned to an ATMWFQ or PWFQ policy, packets are dropped only when the maximum queue depth is exceeded.

## Queue Depth

With EDRR, PQ, and PWFQ policies, you can modify the number of packets allowed per queue on a circuit. Queue depth is configured for PWFQ policies with the congestion avoidance map that you assign to the policy and for EDRR and PQ policies with the **queue depth** command (in EDRR and PQ policy configuration mode). See Table 13-11 for default and maximum queue depth values for various port types.

## Queue Rates

With PQ and EDRR policies, you can configure a rate limit. In PQ policies, the rate is controlled on each individual queue through the **queue rate** command (in PQ policy configuration mode). In EDRR policies, the rate is a combined traffic rate for all queues in the policy, and is configured through the **rate** command (in EDRR policy configuration mode). A reasonable guideline for burst tolerance is to allow one to two seconds of burst time on the defined queue rate.

# Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure scheduling policies, perform the tasks described in the following sections:

- Configure a Queue Map
- Configure a Congestion Avoidance Map
- Configure an ATMWFQ Policy
- Configure an EDRR Policy
- Configure a PQ Policy
- Configure a PWFQ Policy

## Configure a Queue Map

The SmartEdge OS assigns a factory preset, or default, mapping of priority groups to queues, according to the number of queues configured. You can customize this mapping for the circuits to which any QoS scheduling policy is attached. To configure a queue map, perform the tasks in Table 13-2.

**Table 13-2** Configure a Queue Map

| #  | Task                                                                                                  | Root Command          | Notes                                                |
|----|-------------------------------------------------------------------------------------------------------|-----------------------|------------------------------------------------------|
| 1. | Create or select a queue map and access queue map configuration mode.                                 | <b>qos queue-map</b>  | Enter this command in global configuration mode.     |
| 2. | Specify the number of queues for the queue map and access num-queues configuration mode. <sup>1</sup> | <b>num-queues</b>     | Enter this command in queue map configuration mode.  |
| 3. | Customize the mapping of priority groups to queues.                                                   | <b>queue priority</b> | Enter this command in num-queues configuration mode. |

1. For information about the correlation between the number of ATMWFQ queues configured on a particular traffic card type and the corresponding number of PVCs allowed (per port and per traffic card), see the “Circuit Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

## Configure a Congestion Avoidance Map

By default, the SmartEdge OS drops packets at the end of the queue when the number of packets exceeds the configured maximum depth of the queue. A congestion avoidance map, when attached to an ATMWFQ or PWFQ scheduling policy, provides congestion management behavior for each queue defined by the policy.

To configure a congestion avoidance map, perform the tasks described in Table 13-3; enter all commands in congestion map configuration mode, unless otherwise noted.

**Table 13-3 Configure a Congestion Avoidance Map**

| #  | Task                                                                                      | Root Command                        | Notes                                                                                                                           |
|----|-------------------------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create or select a congestion avoidance map and access congestion map configuration mode. | <b>qos congestion-avoidance-map</b> | Enter this command in global configuration mode.                                                                                |
| 2. | Set the RED parameters for each queue in the map.                                         | <b>queue red</b>                    | Perform this task for each queue in the map.                                                                                    |
| 3. | Set the exponential-weight for each queue in the map.                                     | <b>queue exponential-weight</b>     | Enter this command for each queue in the map.                                                                                   |
| 4. | Specify the depth of a queue.                                                             | <b>queue depth</b>                  | This command applies only to congestion avoidance maps for PWFQ policies only.<br>Enter this command for each queue in the map. |

## Configure an ATMWFQ Policy

You can configure an ATMWFQ policy with either RED or EPD parameters. To configure an ATMWFQ policy with RED parameters, using a congestion avoidance map, perform the tasks described in Table 13-4; enter all commands in ATMWFQ policy configuration mode, unless otherwise noted.

**Table 13-4 Configure an ATMWFQ Policy with RED Parameters**

| #  | Task                                                                   | Root Command             | Notes                                            |
|----|------------------------------------------------------------------------|--------------------------|--------------------------------------------------|
| 1. | Create the policy name and access ATMWFQ policy configuration mode.    | <b>qos policy atmwfq</b> | Enter this command in global configuration mode. |
| 2. | Optional. Configure the policy with any or all of the following tasks: |                          |                                                  |
|    | Assign a queue map to the policy.                                      | <b>queue-map</b>         |                                                  |
|    | Specify the number of queues for the policy. <sup>1</sup>              | <b>num-queues</b>        | By default, the number of queues is 4.           |
|    | Assign a congestion avoidance map to the policy.                       | <b>congestion-map</b>    | By default, no congestion map is assigned.       |
|    | Define the algorithm for queue 0.                                      | <b>queue 0 mode</b>      | By default, the queue mode is alternate.         |
|    | Specify the traffic weight for each queue.                             | <b>queue weight</b>      | By default, the weight is 2.                     |

1. For information about the correlation between the number of queues and the number of VCs, see the "Circuit Configuration" chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

To configure an ATMWFQ policy with EPD parameters, perform the tasks described in Table 13-5; enter all commands in ATMWFQ policy configuration mode, unless otherwise noted.

**Table 13-5 Configure an ATM WFQ Policy with EPD Parameters**

| #  | Task                                                                | Root Command                | Notes                                            |
|----|---------------------------------------------------------------------|-----------------------------|--------------------------------------------------|
| 1. | Create the policy name and access ATMWFQ policy configuration mode. | <b>qos policy atmwfq</b>    | Enter this command in global configuration mode. |
| 2. | Configure the policy with any or all of the following tasks:        |                             |                                                  |
|    | Assign a queue map to the policy.                                   | <b>queue-map</b>            |                                                  |
|    | Specify the number of queues for the policy. <sup>1</sup>           | <b>num-queues</b>           | By default, the number of queues is 4.           |
|    | Modify congestion parameters for each queue.                        | <b>queue congestion epd</b> |                                                  |
|    | Define the algorithm for queue 0.                                   | <b>queue 0 mode</b>         | By default, the queue mode is alternate.         |
|    | Specify the traffic weight for each queue.                          | <b>queue weight</b>         | By default, the weight is 2.                     |

1. For information about the correlation between the number of queues and the number of VCs, see the "Circuit Configuration" chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

## Configure an EDRR Policy

To configure an EDRR policy, perform the tasks described in Table 13-6; enter all commands in EDRR policy configuration mode, unless otherwise noted.

**Table 13-6 Configure an EDRR Policy**

| #  | Task                                                                   | Root Command           | Notes                                            |
|----|------------------------------------------------------------------------|------------------------|--------------------------------------------------|
| 1. | Create the policy name and access EDRR policy configuration mode.      | <b>qos policy edrr</b> | Enter this command in global configuration mode. |
| 2. | Optional. Configure the policy with any or all of the following tasks: |                        |                                                  |
|    | Assign a queue map to the policy.                                      | <b>queue-map</b>       |                                                  |
|    | Specify the number of queues for the policy.                           | <b>num-queues</b>      | By default, the number of queues is 8.           |
|    | Specify the depth of a queue.                                          | <b>queue depth</b>     | You can enter this command for each queue.       |
|    | Set RED parameters per queue.                                          | <b>queue red</b>       | By default, RED is disabled.                     |
|    | Specify the traffic weight per queue.                                  | <b>queue weight</b>    | By default, the traffic weight is 0.             |
|    | Set a rate limit for the policy.                                       | <b>rate</b>            | By default, there is no rate limit.              |



## Configure a PQ Policy

To configure a PQ policy, perform the tasks described in Table 13-7; enter all commands in PQ policy configuration mode, unless otherwise noted.

**Table 13-7 Configure a PQ Policy**

| #  | Task                                                                   | Root Command         | Notes                                                 |
|----|------------------------------------------------------------------------|----------------------|-------------------------------------------------------|
| 1. | Create or select the policy and access PQ policy configuration mode.   | <b>qos policy pq</b> | Enter this command in global configuration mode.      |
| 2. | Optional. Configure the policy with any or all of the following tasks: |                      | Enter these commands in PQ policy configuration mode. |
|    | Assign a queue map to the policy.                                      | <b>queue-map</b>     |                                                       |
|    | Specify the number of queues for the policy.                           | <b>num-queues</b>    | By default, the number of queues is 8.                |
|    | Specify the depth of a queue.                                          | <b>queue depth</b>   | You can enter this command for each queue.            |
|    | Set a rate limit per queue.                                            | <b>queue rate</b>    | By default, there is no rate limit.                   |
|    | Set RED parameters per queue.                                          | <b>queue red</b>     | By default, RED is disabled.                          |

## Configure a PWFQ Policy

To configure a PWFQ policy, perform the tasks described in Table 13-8; enter all commands in PWFQ policy configuration mode, unless otherwise noted.

**Table 13-8 Configure a PWFQ Policy**

| #  | Task                                                                   | Root Command                | Notes                                                                                                                                                                     |
|----|------------------------------------------------------------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Create the policy name and access PWFQ policy configuration mode.      | <b>qos policy pwfq</b>      | Enter this command in global configuration mode.                                                                                                                          |
| 2. | Optional. Configure the policy with any or all of the following tasks: |                             |                                                                                                                                                                           |
|    | Assign a queue map to the policy.                                      | <b>queue-map</b>            |                                                                                                                                                                           |
|    | Specify the number of queues for the policy.                           | <b>num-queues</b>           | By default, the number of queues is 8.                                                                                                                                    |
|    | Assign a congestion avoidance map to the policy.                       | <b>congestion-map</b>       |                                                                                                                                                                           |
| 3. | Assign a priority and relative weight to each queue.                   | <b>queue priority</b>       | Enter this command for each queue that you specified with the <b>num-queues</b> command.                                                                                  |
| 4. | Set the maximum and minimum rates for the policy.                      | <b>rate</b>                 | You must enter this command to specify the maximum rate; the minimum rate is optional. You cannot set a minimum rate if you also assign a relative weight to this policy. |
| 5. | Assign a relative weight to this policy.                               | <b>weight</b>               | You cannot assign a relative weight if you also set a minimum rate for this policy.                                                                                       |
| 6. | Set the rate for each priority group.                                  | <b>queue priority-group</b> | Enter this command for each priority group.                                                                                                                               |

## Configuration Examples

---

The following sections provide examples of QoS scheduling configurations:

- Queue Maps
- Congestion Avoidance Map for Multidrop Profiles
- ATMWFQ Policies
- EDRR Policy
- PQ Policies
- PWFQ Policies

### Queue Maps

The following example creates three queue maps and assigns a custom mapping of priority groups to queues, based on the number of queues configured:

```
[local]Redback(config)#qos queue-map Custom2
[local]Redback(config-queue-map)#num-queues 2
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1 2 3 4 5 6 7
[local]Redback(config-num-queues)#exit
```

```
[local]Redback(config)#qos queue-map Custom4
[local]Redback(config-queue-map)#num-queues 4
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1 2
[local]Redback(config-num-queues)#queue 2 priority 3 4 5 6
[local]Redback(config-num-queues)#queue 3 priority 7
[local]Redback(config-num-queues)#exit
```

```
[local]Redback(config)#qos queue-map Custom8
[local]Redback(config-queue-map)#num-queues 8
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1
[local]Redback(config-num-queues)#queue 2 priority 2
[local]Redback(config-num-queues)#queue 3 priority 3
[local]Redback(config-num-queues)#queue 4 priority 4
[local]Redback(config-num-queues)#queue 5 priority 5
[local]Redback(config-num-queues)#queue 6 priority 6
[local]Redback(config-num-queues)#queue 7 priority 7
[local]Redback(config-num-queues)#exit
```

## Congestion Avoidance Map for Multidrop Profiles

The following example configures the congestion avoidance map, map-red4a, with two profiles for any ATMWFQ policy:

```
[local]Redback(config)#qos congestion-avoidance-map map-red4a atmwfq
[local]Redback(config-congestion-map)#queue 0 exponential-weight 40
[local]Redback(config-congestion-map)#queue 0 red default min-threshold 30
max-threshold 5200 probability 16
[local]Redback(config-congestion-map)#queue 0 red profile-1 dscp cs7 min-threshold 140
max-threshold 13000 probability 34
[local]Redback(config-congestion-map)#queue 0 red profile-2 dscp cs3 min-threshold 230
max-threshold 15600 probability 50
[local]Redback(config-congestion-map)#queue 3 exponential-weight 13
[local]Redback(config-congestion-map)#queue 3 red default max-threshold 5200
[local]Redback(config-congestion-map)#queue 3 red profile-1 dscp af21 min-threshold 100
max-threshold 14000 probability 450
```

## ATMWFQ Policies

The following example configures the ATMWFQ policy, example2, with the map-red4a congestion avoidance map:

```
[local]Redback(config)#qos policy example2 atmwfq
[local]Redback(config-policy-atmwfq)#num-queues 4
[local]Redback(config-policy-atmwfq)#congestion-map map-red4a
[local]Redback(config-policy-atmwfq)#queue 0 weight 10
[local]Redback(config-policy-atmwfq)#queue 1 weight 20
[local]Redback(config-policy-atmwfq)#queue 2 weight 30
[local]Redback(config-policy-atmwfq)#queue 3 weight 40
[local]Redback(config-policy-atmwfq)#qos 0 mode strict
[local]Redback(config-policy-atmwfq)#exit
```

The following example configures an ATMWFQ policy, example3, with EPD parameters:

```
[local]Redback(config)#qos policy example3 atmwfq
[local]Redback(config-policy-atmwfq)#num-queues 4
[local]Redback(config-policy-atmwfq)#queue 0 congestion epd max-threshold 5200
[local]Redback(config-policy-atmwfq)#queue 1 congestion epd max-threshold 5200
[local]Redback(config-policy-atmwfq)#queue 2 congestion epd max-threshold 5200
[local]Redback(config-policy-atmwfq)#qos 0 mode strict
[local]Redback(config-policy-atmwfq)#exit
```

## EDRR Policy

The following example configures the EDRR policy, example1, and gives queue number 3 30 percent of the bandwidth of the circuit:

```
[local]Redback(config)#qos policy example1 edrr
[local]Redback(config-policy-edrr)#queue 3 weight 30
[local]Redback(config-policy-edrr)#exit
```

## PQ Policies

The following sections provide examples of PQ policies:

- RED Parameters
- Rate-Limiting
- Backbone Application

### RED Parameters

The following example creates a PQ policy, `red`, and establishes RED parameters for each of the eight queues such that higher priority traffic has a lower probability of being dropped, and lower priority traffic has a higher probability of being dropped:

```
[local]Redback(config)#qos policy red pq
[local]Redback(config-policy-pq)#queue 0 red probability 10 weight 12 min-threshold
1900 max-threshold 5200
[local]Redback(config-policy-pq)#queue 1 red probability 9 weight 12 min-threshold 1850
max-threshold 5200
[local]Redback(config-policy-pq)#queue 2 red probability 8 weight 12 min-threshold 1800
max-threshold 5200
[local]Redback(config-policy-pq)#queue 3 red probability 7 weight 12 min-threshold 1750
max-threshold 5200
[local]Redback(config-policy-pq)#queue 4 red probability 6 weight 12 min-threshold 1700
max-threshold 5200
[local]Redback(config-policy-pq)#queue 5 red probability 5 weight 12 min-threshold 1650
max-threshold 5200
[local]Redback(config-policy-pq)#queue 6 red probability 4 weight 12 min-threshold 1600
max-threshold 5200
[local]Redback(config-policy-pq)#queue 7 red probability 1 weight 12 min-threshold 1550
max-threshold 5200
[local]Redback(config-policy-pq)#exit
```

### Rate-Limiting

The following example configures a PQ policy with 4 queues and divides the bandwidth between the queues according to an approximate 50:30:10:10 ratio during periods of congestion. This guarantees that even the lowest priority queue gets a share of bandwidth in the presence of congestion and strict priority queuing.

```
[local]Redback(config)#qos policy pos-qos pq
[local]Redback(config-policy-pq)#num-queues 4
[local]Redback(config-policy-pq)#queue 0 rate 310000 burst 40000
[local]Redback(config-policy-pq)#queue 1 rate 130000 burst 40000
[local]Redback(config-policy-pq)#queue 2 rate 62000 burst 40000
[local]Redback(config-policy-pq)#queue 3 rate 62000 burst 40000
[local]Redback(config-policy-pq)#exit
```

The following example uses rate-limiting to provide a customer with an access bandwidth that is less than the port speed; this is accomplished through the **no-exceed** keyword in the **queue 0 rate** command. The port is on an OC-12c/STM-14c traffic card and is configured to a maximum of 100 Mbps (instead of its port speed of 622 Mbps).

```
[local]Redback(config)#qos policy 100MbpsMaxBw pq
[local]Redback(config-policy-pq)#num-queues 1
[local]Redback(config-policy-pq)#queue 0 rate 100000 burst 12500 no-exceed
[local]Redback(config-policy-pq)#exit
```

The following example creates a policy, pos-rate, and rate-limits traffic in queue 0 to 300 Mbps when there is congestion on the port. When there is no congestion on the port, the limit is not imposed.

```
[local]Redback(config)#qos policy pos-rate pq
[local]Redback(config-policy-pq)#queue 0 rate 300000 burst 40000
[local]Redback(config-policy-pq)#exit
```

## Backbone Application

In the following example, the PQ policy has eight priority queues, with DSCP values mapping into those eight queues toward the backbone (an 2.5-Gbps OC-48 uplink). Strict rate limits, listed in Table 13-9, are placed on the amount of traffic allowed into the backbone for each DSCP value.

**Table 13-9 2.5-Gbps OC-48 Rate Limits**

| Queue Number | DSCP                             | Rate Limit |
|--------------|----------------------------------|------------|
| 0            | NA                               | None       |
| 1            | NA                               | None       |
| 2            | expedited forwarding (EF)        | 200 Mbps   |
| 3            | assured forwarding (AF), level 4 | 200 Mbps   |
| 4            | assured forwarding (AF), level 3 | 200 Mbps   |
| 5            | assured forwarding (AF), level 2 | 200 Mbps   |
| 6            | assured forwarding (AF), level 1 | 200 Mbps   |
| 7            | default forwarding (DF)          | None       |

The configuration is as follows:

```
[local]Redback(config)#qos policy Diffserv pq
[local]Redback(config-policy-pq)#num-queues 8
[local]Redback(config-policy-pq)#queue 2 rate 200000 burst 25000 no-exceed
[local]Redback(config-policy-pq)#queue 3 rate 200000 burst 25000 no-exceed
[local]Redback(config-policy-pq)#queue 4 rate 200000 burst 25000 no-exceed
[local]Redback(config-policy-pq)#queue 5 rate 200000 burst 25000 no-exceed
[local]Redback(config-policy-pq)#queue 6 rate 200000 burst 25000 no-exceed
```

## PWFQ Policies

The following examples provide configurations for types of priority scheduling:

- Strict Priority
- Normal Priority
- Strict + Normal Priority
- Strict + Normal Priority with Maximum Priority-Group Bandwidth
- Strict + Normal Priority with Maximum and Minimum Bandwidths

In these examples, all policies are configured with four queues, a queue map, `qmap1`, a congestion avoidance map, `map-red4p`, and a maximum bandwidth of 50 Mbits (50000) for the policy; each of the four queues in the policy is assigned a priority and a relative weight, which specifies percentage of the available bandwidth within its priority group.

### Strict Priority

The following example configures the `strict` PWFQ policy for strict priority scheduling. Each queue has a unique priority and the same relative weight.

```
[local]Redback(config)#qos policy strict pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue-map qmap1
[local]Redback(config-policy-pwfq)#congestion-map map-red4p
[local]Redback(config-policy-pwfq)#rate maximum 50000
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 100
[local]Redback(config-policy-pwfq)#queue 1 priority 1 weight 100
[local]Redback(config-policy-pwfq)#queue 2 priority 2 weight 100
[local]Redback(config-policy-pwfq)#queue 3 priority 3 weight 100
[local]Redback(config-policy-pwfq)#exit
```

### Normal Priority

The following example configures the `normal` PWFQ policy for normal priority scheduling. All queues have the same priority; scheduling is based on the relative weight assigned to each queue. In this example, queue 0 receives 50% of the available bandwidth (25 Mbits), queue 1 receives 30% (15 Mbits), queue 2 receives 20% (10 Mbits), and queue 3 receives 10% (5 Mbits).

```
[local]Redback(config)#qos policy normal pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue-map qmap1
[local]Redback(config-policy-pwfq)#congestion-map map-red4p
[local]Redback(config-policy-pwfq)#rate maximum 50000
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 50
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue 2 priority 0 weight 20
[local]Redback(config-policy-pwfq)#queue 3 priority 0 weight 10
[local]Redback(config-policy-pwfq)#exit
```

## Strict + Normal Priority

The following example configures the PWFQ policy, `pwfq4` with two priority groups, 0 and 1.

Queues 0 and 1 have the same priority (group 0) and will be serviced before queues 2 and 3 (assigned to group 1). Within each priority group the queues are serviced in round-robin order, according to their assigned relative weights. For example, queue 0 receives 70% and queue 1 receives 30% of the bandwidth available for the group. Queues 2 and 3 are serviced only when queues 0 and 1 are empty; queue 2 receives 60% and queue 3 receives 40% of the available bandwidth for the group.

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue-map qpmap1
[local]Redback(config-policy-pwfq)#congestion-map map-red4p
[local]Redback(config-policy-pwfq)#rate maximum 50000
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#exit
```

## Strict + Normal Priority with Maximum Priority-Group Bandwidth

The following example configures the `pwfq4` policy as before, but adds a maximum bandwidth limitation for each priority group. In this case, the combined traffic in group 0 is limited to 10 Mbits (10000), even when there is no traffic on the queues in priority group 1. Similarly, combined traffic on queues 2 and 3 is limited to 1 Mbit (1000), even when there is no traffic on queues 0 and 1.

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue-map qpmap1
[local]Redback(config-policy-pwfq)#congestion-map map-red4p
[local]Redback(config-policy-pwfq)#rate maximum 50000
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue priority-group 0 rate 10000
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#queue priority-group 1 rate 1000
[local]Redback(config-policy-pwfq)#exit
```

## Strict + Normal Priority with Maximum and Minimum Bandwidths

The following example configures the `pwfq4` policy as before, but adds a minimum bandwidth limitation of 10 Mbits (10000) for the policy. In this configuration, the minimum bandwidth is guaranteed to the policy only if the next higher level of scheduling (for example, for the scheduling policy applied towards an 802.1Q PVC) is in strict priority mode. If it is not, then the minimum bandwidth is ignored.

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue-map qpmap1
[local]Redback(config-policy-pwfq)#congestion-map map-red4p
[local]Redback(config-policy-pwfq)#rate maximum 50000
```

```
[local]Redback(config-policy-pwfq)#rate minimum 10000
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue priority-group 0 rate 10000
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#queue priority-group 1 rate 1000
[local]Redback(config-policy-pwfq)#exit
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure QoS policies. The commands are presented in alphabetical order.

|                                     |                                 |
|-------------------------------------|---------------------------------|
| <b>congestion-map</b>               | <b>queue exponential-weight</b> |
| <b>num-queues</b>                   | <b>queue-map</b>                |
| <b>qos congestion-avoidance-map</b> | <b>queue 0 mode</b>             |
| <b>qos policy atmwfq</b>            | <b>queue priority</b>           |
| <b>qos policy edrr</b>              | <b>queue priority-group</b>     |
| <b>qos policy pq</b>                | <b>queue rate</b>               |
| <b>qos policy pwfq</b>              | <b>queue red</b>                |
| <b>qos queue-map</b>                | <b>queue weight</b>             |
| <b>queue congestion epd</b>         | <b>rate</b>                     |
| <b>queue depth</b>                  | <b>weight</b>                   |



## congestion-map

**congestion-map** *map-name*

**no congestion-map** *map-name*

### Purpose

Assigns a congestion avoidance map to an Asynchronous Transfer Mode (ATM) weighted fair queuing (ATMWFQ) or priority weighted fair queuing (PWFQ) policy.

### Command Mode

ATMWFQ policy configuration

PWFQ policy configuration

### Syntax Description

|                 |                                |
|-----------------|--------------------------------|
| <i>map-name</i> | Congestion avoidance map name. |
|-----------------|--------------------------------|

### Default

No congestion avoidance map is assigned to any ATMWFQ or PWFQ policy; without a congestion avoidance map assigned, a PWFQ policy drops packets from the end of a queue only when the maximum queue depth is exceeded, the queue depth being that of the circuit to which the policy is attached. For an ATMWFQ policy, packets are dropped from the end of a queue according the congestion avoidance specified by the ATM profile assigned to the circuit.

### Usage Guidelines

Use the **congestion-map** command to assign a congestion avoidance map to an ATMWFQ or PWFQ policy.

To create a congestion avoidance map, enter the **qos congestion-avoidance-map** command (in global configuration mode).

Use the **no** form of this command to delete the congestion avoidance map from the policy.

### Examples

The following example assigns the congestion avoidance map, `map-red4p`, to the PWFQ policy, `pwfq4`:

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#congestion-map map-red4p
[local]Redback(config-policy-pwfq)#
```

### Related Commands

**qos congestion-avoidance-map**

## num-queues

In EDRR, PQ, and PWFQ policy configuration modes, the command syntax is:

**num-queues** {1 | 2 | 4 | 8}

{no | default} **num-queues**

In ATMWFQ policy and queue map configuration modes, the command syntax is:

**num-queues** {2 | 4 | 8}

{no | default} **num-queues**

### Purpose

In ATMWFQ, EDRR, PQ, or PWFQ policy configuration mode, specifies the number of queues for the policy.

In queue map configuration mode, specifies the number of queues for the QoS queue map, and enters num-queues configuration mode.

### Command Mode

ATMWFQ policy configuration  
EDRR policy configuration  
PQ policy configuration  
PWFQ policy configuration  
queue map configuration

### Syntax Description

In EDRR, PQ, and PWFQ policy configuration modes, the syntax description is:

- 1 Specifies that the policy has one queue.
- 2 Specifies that the policy has two queues.
- 4 Specifies that the policy has four queues.
- 8 Specifies that the policy has eight queues.

In ATMWFQ and queue map configuration modes, the syntax description is:

- 2 Specifies that the policy has two queues.
- 4 Specifies that the policy has four queues.
- 8 Specifies that the policy has eight queues.

### Default

For queue maps, EDRR, PQ, and PWFQ policies, the default number of queues is 8. For ATMWFQ policies, the default value is 4.

## Usage Guidelines

Use the **num-queues** command in ATMWFQ policy, EDRR policy, PQ policy, or PWFQ policy configuration mode to specify the number of queues to be used for the policy.

Use the **num-queues** command in queue map configuration mode to specify number of queues for the queue map, and to enter num-queues configuration mode.



**Caution** Risk of dropping packets. Modifying the parameters of an ATMWFQ policy will momentarily interrupt the traffic on all ATM PVCs using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

**Note** For information about the correlation between the number of queues configured on a particular traffic card type and the corresponding number of virtual circuits (VCs) allowed per port (and per traffic card), see the “Circuit Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

Use the **no** or **default** form of this command to specify the default number of queues.

## Examples

The following example configures the PQ policy, `firstout`, to have 4 queues:

```
[local]Redback(config)#qos policy firstout pq  
[local]Redback(config-policy-pq)#num-queues 4
```

## Related Commands

```
qos policy atmwfq  
qos policy edrr  
qos policy pq  
qos policy pwfq  
qos queue-map
```

## qos congestion-avoidance-map

**qos congestion-avoidance-map** *map-name pol-type*

**no qos congestion-avoidance-map** *map-name pol-type*

### Purpose

Creates a quality of service (QoS) congestion avoidance map and accesses congestion map configuration mode.

### Command Mode

global configuration

### Syntax Description

|                 |                                                                                                                                                                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>map-name</i> | Name of the congestion avoidance map.                                                                                                                                                                                                                                                                                 |
| <i>pol-type</i> | Policy type to which this congestion avoidance map will be assigned, according to one of the following keywords: <ul style="list-style-type: none"> <li><b>atmwfq</b>—Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy.</li> <li><b>pwfq</b>—Priority weighted fair queuing (PWFQ) policy.</li> </ul> |

### Default

None

### Usage Guidelines

Use the **qos congestion-avoidance-map** command to create a QoS congestion avoidance map and access congestion map configuration mode.

You can create up to 256 congestion avoidance maps.

Use the **queue red** command (in congestion map configuration mode) to configure the map. To assign a map to a policy, use the **congestion-map** command (in ATMWFQ or PWFQ policy configuration mode).

Use the **no** form of this command to delete the specified map from the configuration.

**Note** If you delete a congestion avoidance map that is assigned to a PWFQ policy, the queue depth reverts to the default; for ATMWFQ policies, queue depth remains as specified by the ATM profile assigned to the ATM permanent virtual circuit (PVC).

### Examples

The following example creates a congestion avoidance map, map-red4a:

```
[local]Redback(config)#qos congestion-avoidance-map map-red4a
[local]Redback(config-congestion-map)#
```

## Related Commands

`congestion-map`  
`queue exponential-weight`  
`queue red`

## qos policy atmwfq

**qos policy** *pol-name* **atmwfq**

**no qos policy** *pol-name* **atmwfq**

### Purpose

Creates or selects a quality of service (QoS) Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy and enters ATMWFQ policy configuration mode.

### Command Mode

global configuration

### Syntax Description

*pol-name*                      Name of the ATMWFQ policy to be created or selected.

### Default

No ATMWFQ policy is created.

### Usage Guidelines

Use the **qos policy atmwfq** command to create or select a QoS ATMWFQ policy and enter ATMWFQ policy configuration mode. An ATMWFQ policy defines QoS for outbound packets on the circuit to which the policy is attached. Up to eight queues per circuit can be serviced.

To attach an ATMWFQ policy to the circuit, use the **qos policy queuing** command (in ATM PVC configuration mode).

**Note** By default, the SmartEdge OS assigns a priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue map through the **qos queue-map** command (in global configuration mode).

**Note** An ATMWFQ policy is applicable to only ATM PVCs (not ports) on ATM DS-3 and second-generation ATM OC traffic cards. For first-generation ATM OC traffic cards, you can attach enhanced deficit round-robin (EDRR) or priority queuing (PQ) policies to both ATM ports and ATM PVCs. In addition, an ATMWFQ policy cannot be attached to a PVC that is shaped as UBR.



**Caution** Risk of dropping packets. Modifying the parameters of an ATMWFQ policy will momentarily interrupt the traffic on all ATM PVCs using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

Use the **no** form of this command to delete an ATMWFQ policy from the configuration.

## Examples

The following example creates the ATMWFQ policy, `example1`, configures 4 queues, and assigns a congestion map:

```
[local]Redback(config)#qos policy example1 atmwfq
[local]Redback(config-policy-atmwfq)#num-queues 4
[local]Redback(config-policy-atmwfq)#congestion-map red4
[local]Redback(config-policy-atmwfq)#exit
```

## Related Commands

`qos policy queuing`  
`qos queue-map`

## qos policy edrr

**qos policy** *pol-name* **edrr**

**no qos policy** *pol-name* **edrr**

### Purpose

Creates or selects a quality of service (QoS) enhanced deficit round-robin (EDRR) policy and enters EDRR policy configuration mode.

### Command Mode

global configuration

### Syntax Description

|                 |                                                    |
|-----------------|----------------------------------------------------|
| <i>pol-name</i> | Name of the EDRR policy to be created or selected. |
|-----------------|----------------------------------------------------|

### Default

No EDRR policy is configured.

### Usage Guidelines

Use the **qos policy edrr** command to create a QoS EDRR policy and enter EDRR policy configuration mode. An EDRR policy defines QoS for outgoing packets on the port or circuit to which the policy is attached. Up to eight queues per circuit can be serviced.

**Note** By default, the SmartEdge OS assigns a priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue map through the **qos queue-map** command (in global configuration mode).

To attach an EDRR policy, enter the **qos policy queuing** command (in the appropriate port or circuit configuration mode).

**Note** To attach an EDRR policy to a circuit, you must also attach the policy at the port level. The limit on attaching different EDRR policies a single traffic card is 15. EDRR is not supported on ATM DS-3 or second-generation ATM OC traffic cards.

Use the **no** form of this command to remove an EDRR policy from the configuration.

### Examples

The following example configures the EDRR policy, `example1`, and attaches the policy to an Ethernet port:

```
[local]Redback(config)#qos policy example1 edrr
[local]Redback(config-policy-edrr)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy queuing example1
```



## Related Commands

`qos mode`  
`qos policy queuing`  
`qos queue-map`

## qos policy pq

**qos policy** *pol-name* **pq**

**no qos policy** *pol-name* **pq**

### Purpose

Creates or selects a quality of service (QoS) priority queuing (PQ) policy and enters PQ policy configuration mode.

### Command Mode

global configuration

### Syntax Description

|                 |                                         |
|-----------------|-----------------------------------------|
| <i>pol-name</i> | Name of the PQ policy to be configured. |
|-----------------|-----------------------------------------|

### Default

No PQ policy is created.

### Usage Guidelines

Use the **qos policy pq** command to create a PQ policy and enter PQ policy configuration mode.

A PQ policy defines QoS for outgoing packets on the port or circuit to which the policy is attached. Up to eight queues per circuit can be serviced.

**Note** By default, the SmartEdge OS assigns a priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue map through the **qos queue-map** command (in global configuration mode).

To attach a PQ policy, use the **qos policy queuing** command (in the appropriate port or circuit configuration mode).

**Note** PQ is not supported on ATM DS-3 or second-generation ATM OC traffic cards.

Use the **no** form of this command to delete the named policy from the configuration.

### Examples

The following example creates the PQ policy, `example1`, and attaches the policy to an Ethernet port:

```
[local]Redback(config)#qos policy example1 pq
[local]Redback(config-policy-pq)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy queuing example1
```

The following example enables per-virtual LAN (VLAN) queuing on a Gigabit Ethernet port by defining a PQ policy with a single queue, and then attaching that policy to each VLAN on the port:

```
[local]Redback(config)#qos policy PerVcQueuing pq
[local]Redback(config-policy-pq)#num-queues 1
[local]Redback(config-policy-pq)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 100
[local]Redback(config-dot1q-pvc)#bind interface if_100 local
[local]Redback(config-dot1q-pvc)#qos policy queuing PerVcQueuing
```

## Related Commands

**qos policy queuing**  
**qos queue-map**

## qos policy pwfq

**qos policy** *pol-name* **pwfq**

**no qos policy** *pol-name* **pwfq**

### Purpose

Creates or selects quality of service (QoS) priority weighted fair queuing (PWFQ) policy and enters PWFQ policy configuration mode.

### Command Mode

global configuration

### Syntax Description

*pol-name*      Name of the policy to be created.

### Default

No PWFQ policy is created.

### Usage Guidelines

Use the **qos policy pwfq** command to create a QoS PWFQ policy and enter PWFQ policy configuration mode.

**Note** PWFQ policies are supported on traffic-managed circuits only.

Use the **no** form of this command to delete the named QoS PWFQ policy.

### Examples

The following example creates a QoS PWFQ policy, **ge3**, with two queues and attaches the policy to a Gigabit Ethernet 3 (GE3) port:

```
[local]Redback(config)#qos policy ge3 pwfq
[local]Redback(config-policy-pwfq)#num-queues 2
[local]Redback(config-policy-pwfq)#exit
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#qos policy queuing ge3
```

### Related Commands

**num-queues**

**qos policy queuing**

**qos rate**

## qos queue-map

**qos queue-map** *map-name*

**no qos queue-map** *map-name*

### Purpose

Creates a quality of service (QoS) queue map and enters queue map configuration mode.

### Command Mode

global configuration

### Syntax Description

*map-name* Queue map name.

### Default

The SmartEdge OS assigns priority groups to queues as listed in the “Usage Guidelines” section.

### Usage Guidelines

Use the **qos queue-map** command to create a QoS queue map and enter queue map configuration mode. You can create up to three customized queue maps.

By default, the SmartEdge OS maps priority groups, Differentiated Services Code Point (DSCP) classes, IP precedence values, Multiprotocol Label Switching (MPLS) experimental (EXP) bits, and Ethernet 802.1p bits to the specified number of queues as shown in Table 13-10.

**Table 13-10 Default Mapping of Packets into Queues Using Priority Groups**

| Priority Group | DSCP Value <sup>1</sup>         | IP Prec | MPLS EXP | 802.1p | 8 Queues | 4 Queues | 2 Queues | 1 Queue |
|----------------|---------------------------------|---------|----------|--------|----------|----------|----------|---------|
| 0              | Network control                 | 7       | 7        | 7      | Queue 0  | Queue 0  | Queue 0  | Queue 0 |
| 1              | Reserved                        | 6       | 6        | 6      | Queue 1  | Queue 1  | Queue 1  | Queue 0 |
| 2              | Expedited Forwarding (EF)       | 5       | 5        | 5      | Queue 2  | Queue 1  | Queue 1  | Queue 0 |
| 3              | Assured Forwarding (AF) level 4 | 4       | 4        | 4      | Queue 3  | Queue 2  | Queue 1  | Queue 0 |
| 4              | AF level 3                      | 3       | 3        | 3      | Queue 4  | Queue 2  | Queue 1  | Queue 0 |
| 5              | AF level 2                      | 2       | 2        | 2      | Queue 5  | Queue 2  | Queue 1  | Queue 0 |
| 6              | AF level 1                      | 1       | 1        | 1      | Queue 6  | Queue 2  | Queue 1  | Queue 0 |
| 7              | Default Forwarding (DF)         | 0       | 0        | 0      | Queue 7  | Queue 3  | Queue 1  | Queue 0 |

1. For more information about DSCP values, see RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* and RFC 2475, *An Architecture for Differentiated Services*.

Use the **num-queues** command (in queue map configuration mode) to specify the number of queues for the queue map, and then use the **queue priority** command (in num-queues configuration mode) to customize the mapping of one or more priority groups to each queue. Finally, use the **queue-map** command (in ATMWFQ policy, EDRR policy, PQ policy, or PWFQ policy configuration mode) to assign the queue map to a scheduling policy.

Use the **no** form of this command to remove the QoS queue map from the configuration.

## Examples

The following example configures the QoS queue map, qmap, and changes the default mapping of priority groups to queues when 4 queues are configured:

```
[local]Redback(config)#qos queue-map qmap
[local]Redback(config-queue-map)#num-queues 4
[local]Redback(config-num-queues)#queue 0 priority 0 1
[local]Redback(config-num-queues)#queue 1 priority 2 3 4 5
[local]Redback(config-num-queues)#queue 2 priority 6
[local]Redback(config-num-queues)#queue 3 priority 7
```

## Related Commands

**num-queues**  
**queue-map**  
**queue priority**

## queue congestion epd

**queue** *queue-num* **congestion epd threshold** *max*

{**no** | **default**} **queue** *queue-num* **congestion epd**

### Purpose

Configure early packet discard (EPD) parameters for this quality of service (QoS) Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy.

### Command Mode

ATMWFQ policy configuration

### Syntax Description

|                             |                                                                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>            | Queue number. The range of values is 0 to 7.                                                                                                                                                                      |
| <b>threshold</b> <i>max</i> | EPD threshold value. The number of packets (equivalent to six ATM cells) that can be in the queue before new incoming packets begin to be discarded. The range of values is 2 to 10,000; the default value is 26. |

### Default

Random early discard (RED) is enabled for ATM PVCs (on ATM DS-3 or second-generation ATM OC traffic cards only) that reference the ATMWFQ policy.

### Usage Guidelines

Use the **queue congestion epd** command to configure EPD parameters for the specified ATMWFQ policy.

With EPD, a threshold is set for the number of packets (equivalent to 6 ATM cells) that can be in the queue before any new incoming packets begin to be discarded. Incoming packets are broken into cells as they are being placed in the queue. If there is enough space in the queue to accept the first cell of a packet, the remaining cells in the packet are admitted. If not, the entire packet is dropped. When an entire packet is dropped, the queue is placed into EPD mode until enough packets have been sent out such that the number of packets in the queue is below the **threshold** *max* value.

Use the **no** or **default** form of this command to use the default EPD value.



**Caution** Risk of dropping packets. Modifying the parameters of an ATMWFQ policy will momentarily interrupt the traffic on all ATM PVCs using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

### Examples

The following example specifies the EPD threshold for the atmwfq-1 policy:

```
[local]Redback(config)#qos policy atmwfq-1 atmwfq
[local]Redback(config-policy-atmwfq)#queue congestion epd threshold 5200
```

## Related Commands

`qos policy atmwfq`



# queue depth

**queue** *queue-num* **depth** *packets count*

{**no** | **default**} **queue** *queue-num* **depth**

## Purpose

Specifies the depth for the specified queue.

## Command Mode

congestion map configuration  
EDRR policy configuration  
PQ policy configuration

## Syntax Description

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>            | Queue number. The range of values is 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>packets</b> <i>count</i> | <p>Depth of the queue, expressed as the number of packets. The range of values depends on the command mode:</p> <ul style="list-style-type: none"><li>• In EDRR and PQ policy configuration modes, the range of values is 1 to 32,736 in increments of 32 packets; the default and maximum allowable values are functions of the port type to which the policy is attached; see Table 13-11.</li><li>• In congestion map configuration mode, the range of values is 1 to 65,535; the default value is 4,000.</li></ul> |

## Default

In EDRR and PQ policy configuration modes, if you do not configure a depth, the default value for the port type is used; see Table 13-11. In congestion map configuration mode for a priority weighted fair queuing (PWFQ) policy, the default value is 4,000.

## Usage Guidelines

Use the **queue depth** command to specify the depth for the specified queue.

**Note** This command is not available if you are configuring a congestion avoidance map and specified **atmwfq** keyword for the policy type.

The queue that you specify in the *queue-num* argument is the one to which the depth is applied. You can enter this command multiple times to set the depth for each queue. Use the **num-queues** command (in EDRR policy or PQ policy configuration mode) to specify the number of queues available; the number of queues is always eight in congestion map configuration mode.

For EDRR and PQ policy configuration modes, the default and maximum allowable values are functions of the port type to which the policy is attached. The port type, and therefore the default and maximum allowable values, are not known at the time the **queue depth** command is entered.

Table 13-11 lists the default and maximum queue depth values for the various port types.

**Table 13-11 Queue Depth Values by Port Type**

| Port Type <sup>1</sup>     | Default Depth Value | Maximum Depth Value |
|----------------------------|---------------------|---------------------|
| First-generation ATM OC-3  | 1,024               | 4,064               |
| First-generation ATM OC-12 | 4,064               | 4,064               |
| DS-0                       | 256                 | 4,064               |
| DS-1                       | 256                 | 4,064               |
| DS-3                       | 1,024               | 4,064               |
| E1                         | 256                 | 4,064               |
| E3                         | 1,024               | 4,064               |
| Ethernet                   | 1,024               | 4,064               |
| Gigabit Ethernet (GE)      | 4,064               | 4,064               |
| POS OC-3c                  | 1,024               | 4,064               |
| POS OC-12c                 | 4,064               | 32,736              |
| POS OC-48c                 | 32,736              | 32,736              |

1. PQ and EDRR policies are not supported on ATM DS-3 or second-generation ATM OC traffic cards.



**Caution** Risk of performance loss. Because some traffic cards queue a maximum of 4,064 packets, it is possible to configure a depth that is inappropriate for the type of port to which the policy is later attached. In that case, the system displays a warning message when you attach the policy to the port. To reduce the risk, consider the queue depth allowed per port type.

Use the **no** or **default** form of this command to specify the default value.

## Examples

The following example sets the depth for queue 5. The depth is rounded to the nearest increment of 32.

```
[local]Redback(config-policy-pq)#queue 5 depth packets 550
```

## Related Commands

num-queues  
qos policy edrr  
qos policy pq

## queue exponential-weight

**queue** *queue-num* **exponential-weight** *weight-exp*

**no** **queue** *queue-num* **exponential-weight**

### Purpose

Specifies a weight for the specified queue.

### Command Mode

congestion map configuration

### Syntax Description

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>  | Queue number. The range of values is 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                              |
| <i>weight-exp</i> | Exponent representing the inverse of the exponentially weighted moving average. The range of values depends on the type of congestion avoidance map: <ul style="list-style-type: none"><li>Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy—The range of values is 7 to 10 the default value is 9.</li><li>Priority weighted fair queuing (PWFQ) policy—The range of values is 1 to 15; the default value is 9.</li></ul> |

### Default

The exponential weight is assigned the default value, depending on the type of congestion map.

### Usage Guidelines

Use the **queue exponential-weight** command to specify a weight for the specified queue. The queue must be one that you have configured with random early detection (RED) parameters. The weight that you specify applies to every RED profile (**default**, **profile-1**, **profile-2**) for this queue.

The average queue occupancy is computed as a moving average of the instantaneous queue occupancy. Use the *weight-exp* argument to set the inverse of the exponential moving average. The larger the value of the *weight-exp* argument, the longer term the average.

The average queue size is based on the previous average and the current size of the queue according to the following formula:

$$\text{average} = (\text{old\_average} \times (1 - \frac{1}{2^w})) + (\text{current\_queue\_size} \times \frac{1}{2^w})$$

where  $w$  is the value of the *weight-exp* argument.

Use the **no** form of this command to specify the default exponential weight for the type of congestion map.

### Examples

The following example specifies the weights for the default profile in the map-red8 congestion avoidance map:

```
[local]Redback(config)#qos congestion-avoidance-map map-red8
[local]Redback(config-congestion-map)#queue 0 exponential-weight 1
[local]Redback(config-congestion-map)#queue 1 exponential-weight 2
[local]Redback(config-congestion-map)#queue 2 exponential-weight 1
[local]Redback(config-congestion-map)#queue 3 exponential-weight 1
[local]Redback(config-congestion-map)#queue 4 exponential-weight 10
[local]Redback(config-congestion-map)#queue 5 exponential-weight 1
[local]Redback(config-congestion-map)#queue 6 exponential-weight 1
[local]Redback(config-congestion-map)#queue 7 exponential-weight 1
[local]Redback(config-congestion-map)#
```

### Related Commands

**qos congestion-avoidance-map**  
**queue red**

## queue-map

**queue-map** *map-name*

**no queue-map** *map-name*

### Purpose

Assigns a queue map to the quality of service (QoS) scheduling policy.

### Command Mode

ATMWFQ policy configuration

EDRR policy configuration

PQ policy configuration

PWFQ policy configuration

### Syntax Description

*map-name*                      Queue map name.

### Default

No queue map is assigned to any QoS scheduling policy.

### Usage Guidelines

Use the **queue-map** command to assign a queue map to the specified QoS scheduling policy.

To create a queue map, enter the **qos queue-map** command (in global configuration mode). To specify the number of queues for the queue map, enter the **num-queues** command (in queue map configuration mode).

Use the **queue priority** command (in num-queues configuration mode) to customize the mapping of a priority group to each queue.

Use the **no** form of this command to delete the queue map from the QoS policy.

### Examples

The following example assigns the queue map, q-queue-map, to the EDRR configuration policy, qos-edrr-test:

```
[local]Redback(config)#qos policy qos-edrr-test edrr  
[local]Redback(config-policy-edrr)#queue-map q-queue-map
```

### Related Commands

|                          |                        |
|--------------------------|------------------------|
| <b>num-queues</b>        | <b>qos policy pwfq</b> |
| <b>qos policy atmwfq</b> | <b>qos queue-map</b>   |
| <b>qos policy edrr</b>   | <b>queue priority</b>  |
| <b>qos policy pq</b>     |                        |

## queue 0 mode

**queue 0 mode** {**alternate** | **strict**}

**default queue 0 mode**

### Purpose

Defines the mode of the Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) algorithm for queue 0.

### Command Mode

ATMWFQ policy configuration

### Syntax Description

|                  |                                                                                             |
|------------------|---------------------------------------------------------------------------------------------|
| <b>alternate</b> | Serves queue 0 and the other queues configured on the circuit in alternating fashion.       |
| <b>strict</b>    | Indicates that queue 0 always has priority over all other queues configured on the circuit. |

### Default

The default mode is alternate.

### Usage Guidelines

Use the **queue mode** command to define the mode of the ATMWFQ policy algorithm for queue 0.

In alternate mode, the servicing of queues alternates between queue 0 and the remaining queues. Queue 0 is served, then the next queue is served. Queue 0 is served again, and the next queue in turn is served, and so on. For example, if there are 4 queues configured, the order of servicing will be q0, q1, q0, q2, q0, q3, q0, q1, and so on.

In strict mode, high-priority queue 0 is serviced immediately and other queues are serviced in a round-robin fashion; in other words, queue 0 always has priority over all other queues configured on the circuit.

Use the **default** form of this command to return the ATMWFQ algorithm to alternate mode.

### Examples

The following example configures the ATMWFQ policy to use **strict** mode:

```
[local]Redback(config)#qos policy atm-wfq-1 atmwfq
[local]Redback(config-policy-atmwfq)#queue 0 mode strict
```

### Related Commands

**num-queues**  
**qos mode**  
**qos policy atmwfq**

## queue priority

In num-queues configuration mode, the syntax is:

**queue** *queue-num* **priority** *group-num* [*group-num2* [...]]

**no queue** *queue-num* **priority**

In PWFQ policy configuration mode, the syntax is:

**queue** *queue-num* **priority** *group-num* **weight** *weight*

**no queue** *queue-num* **priority**

### Purpose

In num-queues configuration mode, customizes the mapping of quality of service (QoS) priority groups to the specified queue. In PWFQ policy configuration mode, assigns a priority group number and relative weight inside the assigned priority group to the specified queue.

### Command Mode

num-queues configuration  
PWFQ policy configuration

### Syntax Description

|                                |                                                                                                                                                                                                        |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>               | Queue number. The range of values is 0 to 7.                                                                                                                                                           |
| <i>group-num</i>               | Priority group number. The range of values is 0 to 7.                                                                                                                                                  |
| <i>group-num2 group-num3..</i> | Optional. Additional priority group numbers separated by spaces. The range of values is 0 to 7.                                                                                                        |
| <b>weight</b> <i>weight</i>    | Relative weight that is assigned to this queue for the specified priority group; available only for queues defined in priority weighted fair queuing (PWFQ) policies. The range of values is 5 to 100. |

### Default

In num-queues configuration mode, the SmartEdge OS assigns a preset mapping of priority groups to queues; for information about the default values, see the **qos queue-map** command. In PWFQ policy configuration mode, there is no default.

### Usage Guidelines

Use the **queue priority** command in num-queues configuration mode to customize the mapping of one or more priority groups to the specified queue. In PWFQ policy configuration mode, use this command to assign a priority group number and relative weight inside the assigned priority group to the specified queue.

**Note** The relative weights assigned by this command in PWFQ policy configuration mode are within the specified priority group.

**Note** In num-queues configuration mode, this command determines the relationship between the priority in the packet (according to the TOS or DSCP bits) and the queue to which the packet is assigned. In PWFQ policy configuration mode, this command assigns a queue to a scheduling priority group, which is not the same as the packet priority and which is used by the PWFQ scheduler to determine when the packets are scheduled for transmission.

**Note** Although the mapping of priority to queues is arbitrary, in general, the SmartEdge OS assumes that there is a correspondence between the queue number and the scheduling priority, with queue 0 having the highest priority and queue 7 the lowest priority. You could cause performance problems if you assign a lower priority to queue 0 than the other queues. For example, internally generated control packets are assigned to queue 0; if you have assigned that queue a priority 7, they could be dropped due to congestion from priority 7 traffic.

For queue maps:

- To apply the customized mapping of priority groups to queues, enter the **queue-map** command (in ATMWFQ policy, EDRR policy, PQ policy, or PWFQ policy configuration mode).
- In num-queues configuration mode, use the **no** form of this command to remove the customized mapping for the specified queue.

For PWFQ policies:

- You must enter this command for each queue you have defined for the policy with the **num-queues** command (in PWFQ policy configuration mode). The system displays an error message when you attach the policy to a port, tunnel, or permanent virtual circuit (PVC) if not all defined queues have a priority and weight assigned.
- Use the **weight weight** construct to specify the traffic share for each queue. The traffic share for each queue is calculated from the specified weight divided by the sum of the weights specified for all queues in the same priority group. For an example, see the “Examples” section.
- In PWFQ configuration mode, use the **no** form of this command to delete the queue.

## Examples

The following example defines 4 queues for the PWFQ policy, **pwfq4**, and assigns them to priority groups 0 and 1 with relative weights 70, 30, 60, 40:

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#
```

In this example, in priority group 0 queue 0 receives 70% traffic share and queue 1 receives 30% traffic share; in priority group 1 queue 2 receives 60% traffic share and queue 3 receives 40% traffic share.

The following example configures the queue maps, **Custom2**, **Custom4**, **Custom8**, to customize the mapping of priority groups to queues. The assignment of priority group to queue number varies according to the number of queues configured. The custom mapping for 4 queues is referenced by the QoS policy, **myPolicyPQ**.



```
[local]Redback(config)#qos queue-map Custom2
[local]Redback(config-queue-map)#num-queues 2
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1 2 3 4 5 6 7
[local]Redback(config-num-queues)#exit
```

```
[local]Redback(config)#qos queue-map Custom4
[local]Redback(config-queue-map)#num-queues 4
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1 2
[local]Redback(config-num-queues)#queue 2 priority 3 4 5 6
[local]Redback(config-num-queues)#queue 3 priority 7
[local]Redback(config-num-queues)#exit
```

```
[local]Redback(config)#qos queue-map Custom8
[local]Redback(config-queue-map)#num-queues 8
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1
[local]Redback(config-num-queues)#queue 2 priority 2
[local]Redback(config-num-queues)#queue 3 priority 3
[local]Redback(config-num-queues)#queue 4 priority 4
[local]Redback(config-num-queues)#queue 5 priority 5
[local]Redback(config-num-queues)#queue 6 priority 6
[local]Redback(config-num-queues)#queue 7 priority 7
[local]Redback(config-num-queues)#exit
```

```
[local]Redback(config)#qos policy MyPolicy pq
[local]Redback(config-policy-pq)#queue-map Custom4
[local]Redback(config-policy-pq)#num-queues 4
.
.
.
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#bind interface BackboneOne local
[local]Redback(config-port)#qos policy queuing MyPolicy
```

## Related Commands

```
num-queues
qos policy pwfq
qos queue-map
queue 0 mode
```

## queue priority-group

**queue priority-group** *group-num* { **rate kbps** [**exceed**] | **rate percentage** *value* }

**no queue priority-group** *group-num*

### Purpose

Sets the rate for the specified priority group.

### Command Mode

PWFQ policy configuration

### Syntax Description

|                                     |                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>group-num</i>                    | Priority group number. The range of values is 0 to 7.                                                                                                     |
| <b>rate kbps</b>                    | Absolute rate in kilobits per second for the specified priority group; the range of values is 64 to 1,000,000.                                            |
| <b>exceed</b>                       | Optional. Allows the traffic rate to be exceeded for the specified priority group. The default condition is to not allow the traffic rate to be exceeded. |
| <b>rate percentage</b> <i>value</i> | Relative rate, as a percentage of the policy rate, for the specified priority group; the range of values is 1 to 100.                                     |

### Default

None

### Usage Guidelines

Use the **queue priority-group** command to set the rate for the specified priority group. You enter this command for each priority group created for this priority weighted fair queuing (PWFQ) policy.

A priority group is a set of queues that all have the same priority group number assigned to them with the **queue priority** command (in PWFQ policy configuration mode). You enter this command for each priority group.

Use the **rate kbps** construct to specify an absolute rate for the priority group; use the **rate percentage** construct to specify a relative rate. You specify the policy rate using the **rate** command (in PWFQ policy configuration mode).

Use the **no** form of this command to delete the priority group from the policy.

### Examples

The following example sets the rate and burst tolerance for the priority groups in the PWFQ policy, pwfq4:

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
```

```
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#queue priority-group 0 rate 1800
[local]Redback(config-policy-pwfq)#queue priority-group 1 rate 1600
[local]Redback(config-policy-pwfq)#
```

The following example sets relative rates for the priority groups in the PWFQ policy, pwfq-percent:

```
[local]Redback(config)#qos policy pwfq2 pwfq
[local]Redback(config-policy-pwfq)#rate maximum 6000
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 100
[local]Redback(config-policy-pwfq)#queue 1 priority 1 weight 100
[local]Redback(config-policy-pwfq)#queue 2 priority 2 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 2 weight 40
[local]Redback(config-policy-pwfq)#queue priority-group 0 rate percentage 10
[local]Redback(config-policy-pwfq)#queue priority-group 1 rate percentage 20
[local]Redback(config-policy-pwfq)#
```

## Related Commands

**queue priority**  
**rate**

## queue rate

**queue** *queue-num* **rate** *kbps* **burst** *bytes* [**no-exceed**]

**no queue** *queue-num* **rate**

### Purpose

Establishes the rate limit and burst tolerance for the specified quality of service (QoS) priority queuing (PQ) policy queue.

### Command Mode

PQ policy configuration

### Syntax Description

|                           |                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>          | Number of the priority queue for which you are setting the rate limit and burst tolerance. The range of values is 0 to 7. |
| <b>rate</b> <i>kbps</i>   | Rate in kilobits per second. The range of values is 56 to 1,000,000.                                                      |
| <b>burst</b> <i>bytes</i> | Burst tolerance in bytes. The range of values is 1 to 12,000,000.                                                         |
| <b>no-exceed</b>          | Optional. Specifies that the rate is not to be exceeded, even if there are no other traffic classes waiting to be sent.   |

### Default

No limit is placed on the rate of any individual queue.

### Usage Guidelines

Use the **queue rate** command to establish the rate limit and burst tolerance for the specified PQ policy queue. A reasonable guideline for burst tolerance is 10 times the link maximum transmission unit (MTU), or approximately 15,000 to 20,000 bytes. For a DS-1 circuit, the minimum rate is 56 kbps; for all other circuits, the minimum rate is 1,000 kbps.

Use the **no** form of this command to return the rate limit and burst tolerance to their default values.

### Examples

The following example sets the rate limit and burst tolerance for queue 4 for the PQ policy:

```
[local]Redback(config-policy-pq)#queue 4 rate 10000 burst 12000 no-exceed
```

### Related Commands

**num-queues**  
**qos policy pq**

## queue red

In congestion map configuration mode, the command syntax is:

```
queue queue-num red profile [dscp class1[class2[...]]] max-threshold max min-threshold min
probability prob weight weight-exp
```

```
no queue queue-num red profile
```

In EDRR and PQ policy configuration modes, the command syntax is:

```
queue queue-num red max-threshold max min-threshold min probability prob weight weight-exp
```

```
no queue queue-num red
```

### Purpose

In congestion map configuration mode, sets the random early detection (RED) parameters for the specified queue in the specified RED drop profile for the congestion avoidance map. In EDRR and PQ policy configuration modes, sets the RED parameters for the specified quality of service (QoS) queue.

### Command Mode

congestion map configuration

EDRR policy configuration

PQ policy configuration

### Syntax Description

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>                      | Queue number. The range of values is 0 to 7.                                                                                                                                                                                                                                                                                                                                                                              |
| <i>profile</i>                        | Specifies the RED profile in the congestion avoidance map, according to one of the following keywords: <ul style="list-style-type: none"> <li>• <b>default</b>—Specifies the default profile for this queue.</li> <li>• <b>profile-1</b>—Specifies an alternate profile for this queue.</li> <li>• <b>profile-2</b>—Specifies an alternate profile for this queue.</li> </ul>                                             |
| <b>dscp</b> <i>class1 class2 ....</i> | Optional. Differentiated Services Code Point (DSCP) classes, separated by spaces; the range of values is: <ul style="list-style-type: none"> <li>• Congestion avoidance map—An integer from <b>0</b> to <b>63</b> or one of the keywords listed in Table 13-12.</li> <li>• Enhanced deficit round-robin (EDRR) and priority queuing (PQ)—An integer from 1 to 32 or one of the keywords listed in Table 13-12.</li> </ul> |
| <b>max-threshold</b> <i>max</i>       | Average queue occupancy in packets above which all packets are dropped. The range of values is: <ul style="list-style-type: none"> <li>• Congestion avoidance map—2 to 10,000.</li> <li>• EDRR—1 to 10,922.</li> <li>• PQ—1 to 32,736.</li> </ul>                                                                                                                                                                         |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>min-threshold</b> <i>min</i> | <p>Average queue occupancy in packets below which no packets are dropped. The range of values is:</p> <ul style="list-style-type: none"> <li>• Congestion avoidance map—1 to 9,999.</li> <li>• EDRR—1 to 10,922.</li> <li>• PQ—1 to 32,736.</li> </ul>                                                                                                                                                                                         |
| <b>probability</b> <i>prob</i>  | <p>Inverse of the probability of dropping a packet as the average queue occupancy approaches the maximum threshold. The resulting probability (<math>1/prob</math>) is the fraction of packets dropped when the average queue depth is at the maximum threshold. The range of values is:</p> <ul style="list-style-type: none"> <li>• Congestion avoidance map—8 to 32,768.</li> <li>• EDRR—8 to 32,768.</li> <li>• PQ—1 to 65,535.</li> </ul> |
| <b>weight</b> <i>weight-exp</i> | <p>Exponent representing the inverse of the exponentially weighted moving average. The range of values is as follows:</p> <ul style="list-style-type: none"> <li>• Congestion avoidance map—7 to 10.</li> <li>• EDRR—7 to 10.</li> <li>• PQ—1 to 15.</li> </ul>                                                                                                                                                                                |

## Default

For EDRR and PQ policies, RED is disabled. For a congestion avoidance map, none; you must enter a value for each argument and construct.

## Usage Guidelines

Use the **queue red** command in congestion map configuration mode to set the RED parameters for the specified queue in the RED drop profile for the congestion avoidance map. Use the **queue red** command in EDRR or PQ policy configuration mode to set the RED parameters for the specified QoS queue.

RED parameters specify how buffer utilization is to be managed under congestion by signaling to the sources of traffic that the network is on the verge of entering a congested state. This signaling is accomplished by dropping packets with a probability that varies as a function of how many packets are waiting in a queue at any particular time, and of the values of the *max*, *min*, and *weight-exp* arguments.

Use the *profile* argument to specify one of three RED profiles for the RED parameters for this queue. Each queue supports up to three RED profiles.

Use the **dscp class1 class2 ...** construct to specify a list of DSCP classes for which the RED parameters pertain. Table 13-12 lists the keywords for the DSCP classes.

**Table 13-12 DSCP Class Keywords**

| DSCP Class                                            | Keyword     | DSCP Class                                       | Keyword                         |
|-------------------------------------------------------|-------------|--------------------------------------------------|---------------------------------|
| Assured Forwarding (AF) Class 1/<br>Drop precedence 1 | <b>af11</b> | Class Selector 0<br>(same as default forwarding) | <b>cs0</b> (same as <b>df</b> ) |
| AF Class 1/Drop precedence 2                          | <b>af12</b> | Class Selector 1                                 | <b>cs1</b>                      |

**Table 13-12 DSCP Class Keywords** (*continued*)

| DSCP Class                   | Keyword     | DSCP Class                                    | Keyword                         |
|------------------------------|-------------|-----------------------------------------------|---------------------------------|
| AF Class 1/Drop precedence 3 | <b>af13</b> | Class Selector 2                              | <b>cs2</b>                      |
| AF Class 2/Drop precedence 1 | <b>af21</b> | Class Selector 3                              | <b>cs3</b>                      |
| AF Class 2/Drop precedence 2 | <b>af22</b> | Class Selector 4                              | <b>cs4</b>                      |
| AF Class 3/Drop precedence 3 | <b>af23</b> | Class Selector 5                              | <b>cs5</b>                      |
| AF Class 3/Drop precedence 1 | <b>af31</b> | Class Selector 6                              | <b>cs6</b>                      |
| AF Class 3/Drop precedence 2 | <b>af32</b> | Class Selector 7                              | <b>cs7</b>                      |
| AF Class 3/Drop precedence 3 | <b>af33</b> | Default Forwarding (same as Class Selector 0) | <b>df</b> (same as <b>cs0</b> ) |
| AF Class 4/Drop precedence 1 | <b>af41</b> | Expedited Forwarding                          | <b>ef</b>                       |
| AF Class 4/Drop precedence 2 | <b>af42</b> |                                               |                                 |
| AF Class 4/Drop precedence 3 | <b>af43</b> |                                               |                                 |

Use the **max-threshold** *max* construct to set the average queue occupancy in packets above which the probability of a packet being dropped is 100%. As the average occupancy approaches the maximum threshold value, packets are dropped with increasing probability, as a function of the value of the *prob* argument. For EDRR and PQ policies, the value of the *max* argument must be less than the value of the *count* argument in the **queue depth** command.

Use the **min-threshold** *min* construct to set the average queue occupancy in packets at or below which the probability of a packet being dropped is 0%. The value of the *min* argument must be less than the value of the *max* argument in this command, and, for EDRR and PQ policies, less than the value of the *count* argument in the **queue depth** command.

Use the **probability** *prob* construct to establish the probability of a packet being dropped as the average queue occupancy approaches the maximum threshold value. The value of the *prob* argument is the inverse of the probability of a packet being dropped. The higher the value of the *prob* argument, the lower the probability of a packet being dropped.

The average queue occupancy is computed as a moving average of the instantaneous queue occupancy. Use the **weight** *weight-exp* construct to set the inverse of the exponential moving average. The larger the value of the *weight-exp* argument, the longer term the average.

The average queue size is based on the previous average and the current size of the queue according to the following formula:

$$\text{average} = (\text{old\_average} \times (1 - \frac{1}{2^w})) + (\text{current\_queue\_size} \times \frac{1}{2^w})$$

where  $w$  is the value of the *weight-exp* argument.

In congestion map configuration mode, use the **no** form of this command to remove the queue from the specified profile. In EDRR and PQ policy configuration modes, use the **no** form of this command to disable RED parameters.

## Examples

The following example creates the PQ policy, red, and establishes RED parameters for each of the eight queues, so that higher priority traffic has a lower probability of being dropped, while lower priority traffic has a higher probability of being dropped. The example then attaches the policy to a Packet over SONET/SDH (POS) port.

```
[local]Redback(config)#qos policy red pq
[local]Redback(config-policy-pq)#queue 0 red probability 10 weight 12 min-threshold
1900 max-threshold 5200
[local]Redback(config-policy-pq)#queue 1 red probability 9 weight 12 min-threshold 1850
max-threshold 5200
[local]Redback(config-policy-pq)#queue 2 red probability 8 weight 12 min-threshold 1800
max-threshold 5200
[local]Redback(config-policy-pq)#queue 3 red probability 7 weight 12 min-threshold 1750
max-threshold 5200
[local]Redback(config-policy-pq)#queue 4 red probability 6 weight 12 min-threshold 1700
max-threshold 5200
[local]Redback(config-policy-pq)#queue 5 red probability 5 weight 12 min-threshold 1650
max-threshold 5200
[local]Redback(config-policy-pq)#queue 6 red probability 4 weight 12 min-threshold 1600
max-threshold 5200
[local]Redback(config-policy-pq)#queue 7 red probability 1 weight 12 min-threshold 1550
max-threshold 5200
[local]Redback(config-policy-pq)#exit
[local]Redback(config)#port pos 2/1
[local]Redback(config-port)#qos policy queuing red
```

The following example specifies the RED parameters for the default profile and queues 0 through 7 in the congestion avoidance map, map-red:

```
[local]Redback(config)#qos congestion-avoidance-map map-red8 atmwfq
[local]Redback(config-congestion-map)#queue 0 red default probability 10 weight 12
min-threshold 1900 max-threshold 5200
[local]Redback(config-congestion-map)#queue 1 red default probability 9 weight 12
min-threshold 1850 max-threshold 5200
[local]Redback(config-congestion-map)#queue 2 red default probability 8 weight 12
min-threshold 1800 max-threshold 5200
[local]Redback(config-congestion-map)#queue 3 red default probability 7 weight 12
min-threshold 1750 max-threshold 5200
[local]Redback(config-congestion-map)#queue 4 red default probability 6 weight 12
min-threshold 1700 max-threshold 5200
[local]Redback(config-congestion-map)#queue 5 red default probability 5 weight 12
min-threshold 1650 max-threshold 5200
[local]Redback(config-congestion-map)#queue 6 red default probability 4 weight 12
min-threshold 1600 max-threshold 5200
[local]Redback(config-congestion-map)#queue 7 red default probability 1 weight 12
min-threshold 1550 max-threshold 5200
```



## Related Commands

- `num-queues`
- `qos congestion-avoidance-map`
- `qos policy edrr`
- `qos policy pq`
- `queue exponential-weight`

## queue weight

**queue** *queue-num* **weight** *traffic-weight*

**default queue** *queue-num* **weight**

### Purpose

Specifies the weight of the specified Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) or enhanced deficit round-robin (EDRR) queue.

### Command Mode

ATMWFQ policy configuration

EDRR policy configuration

### Syntax Description

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-num</i>      | Queue number. The range of values is 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <i>traffic-weight</i> | <p>For ATMWFQ policies, the traffic weight is expressed as a unit of average packet size. The average packet size is equivalent to 6 ATM cells. For example, a traffic weight of 2,000 is equivalent to 12,000 ATM cells. The range of values is 1 to 5,461; the default value is 2.</p> <p>For EDRR policies, the traffic weight is expressed as a percentage of bandwidth. The range of configurable values is 5 to 100%; the default value is 0%.</p> |

### Default

For ATMWFQ, the weight value is 2. For EDRR, the weight value is 0.

### Usage Guidelines

Use the **queue weight** command to specify the weight of the specified ATMWFQ or EDRR queue.



**Caution** Risk of performance loss. For EDRR, you must assign a weight to each queue that is in use, as specified by either the default queue map or a customized queue map. To reduce the risk, ensure that you assign a weight to each queue.



**Caution** Risk of packet loss. Modifying the parameters of an ATMWFQ policy will momentarily interrupt the traffic on all ATM PVCs using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

Use the **default** form of this command to return the queue to its default weight.

## Examples

The following example provides queue number 3 with 30 % of the bandwidth of the circuit to which the EDRR policy, `scheduling1`, is attached:

```
[local]Redback(config)#qos policy scheduling1 edrr
[local]Redback(config-policy-edrr)#queue 3 weight 30
```

## Related Commands

- `num-queues`
- `qos mode`
- `queue 0 mode`

## rate

For enhanced deficit round-robin (EDRR) policies, the command syntax is:

**rate** *kbps* **burst** *bytes*

**no rate**

For priority weighted fair queuing (PWFQ) policies, the command syntax is:

**rate** {**maximum** | **minimum**} *kbps*

**no rate** {**maximum** | **minimum**}

## Purpose

Sets the rate and burst tolerance for traffic on the circuit, port, or subscriber record to which the quality of service (QoS) policy is attached.

## Command Mode

EDRR policy configuration

PWFQ policy configuration

## Syntax Description

|                           |                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <i>kbps</i>               | Rate in kilobits per second. The range of values is 64 to 1,000,000.                                                  |
| <b>burst</b> <i>bytes</i> | Burst tolerance in bytes. This construct is available for EDRR policies only. The range of values is 1 to 12,000,000. |
| <b>maximum</b>            | Specifies the maximum rate to set.                                                                                    |
| <b>minimum</b>            | Specifies the minimum rate to set.                                                                                    |

## Default

Rate is calculated based on the default values for the *kbps* and *bytes* arguments.

## Usage Guidelines

Use the **rate** command to set the rate and burst tolerance for traffic on the port, circuit, or subscriber record to which the QoS policy is attached.

For PWFQ policies:

- You must specify the maximum rate for the policy using this command; otherwise, you cannot attach the policy to any traffic-managed port, or any of the 802.1Q tunnels, or permanent virtual circuits (PVCs) configured on it.
- You cannot specify a minimum rate if you intend to specify a relative weight for this policy, using the **weight** command (in PWFQ policy configuration mode) and attach the policy to any traffic-managed port, or any of the 802.1Q tunnels, or PVCs configured on it.
- The maximum and minimum rates, if both are specified, are compared to ensure that the minimum value is always less than the maximum value.

**Note** The maximum rate set by the **qos rate** command (in port configuration mode) is the rate at which the port, 802.1Q tunnel, or 802.1Q PVC operates; any priority queuing (PQ), enhanced deficit round-robin (EDRR), or PWFQ queue or circuit with a PQ, EDRR, or PWFQ policy is limited by the rate specified by that command for the circuit. Also, the sum of all traffic on the port carried by the queues belonging to the circuits or subscribers is limited to the rate specified by that command.

Use the **no** form of this command to return to the default traffic rate or burst tolerance.

## Examples

The following example marks all traffic conforming to the configured policy rate with expedited forwarding (ef) and marks traffic that exceeds the policy rate with default forwarding (df):

```
[local]Redback(config)#qos policy GE-in pwfq
[local]Redback(config-policy-pwfq)#rate 6000000
[local]Redback(config-policy-rate)#conform mark dscp ef
[local]Redback(config-policy-rate)#exceed mark dscp df
```

## Related Commands

|                                |                              |
|--------------------------------|------------------------------|
| <b>conform mark dscp</b>       | <b>queue priority-group</b>  |
| <b>conform mark precedence</b> | <b>qos rate</b>              |
| <b>conform mark priority</b>   | <b>violate drop</b>          |
| <b>exceed drop</b>             | <b>violate mark dscp</b>     |
| <b>exceed mark dscp</b>        | <b>violate mark dscp</b>     |
| <b>exceed mark precedence</b>  | <b>violate mark priority</b> |
| <b>exceed mark priority</b>    | <b>violate no-action</b>     |
| <b>exceed no-action</b>        | <b>weight</b>                |

## weight

**weight** *weight*

**no weight** *weight*

### Purpose

Assigns a relative weight that is used to calculate a traffic ratio for all circuits to which you attach this policy.

### Command Mode

PWFQ policy configuration

### Syntax Description

|               |                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| <i>weight</i> | Relative weight that is assigned to any circuit to which you attach this policy. The range of values is 5 to 100. |
|---------------|-------------------------------------------------------------------------------------------------------------------|

### Default

All circuits to which this policy is attached have the same weight.

### Usage Guidelines

Use the **weight** command to assign a relative weight that is used to calculate a traffic ratio for all circuits to which you attach this policy.

You can assign a relative weight, or you can set a minimum absolute rate, for the policy, using the **rate** command (in PWFQ policy configuration mode), but you cannot do both; the relative weight and minimum absolute rate are mutually exclusive.

You can assign a relative weight (using this command), and set a maximum absolute rate, for the policy, using the **rate** command (in PWFQ policy configuration mode).

Use the **no** form of this command to specify the default condition.

### Examples

The following example specifies 70% for the GE-out policy:

```
[local]Redback(config)#qos policy GE-out pwfq  
[local]Redback(config-policy-pwfq)#weight 70
```

### Related Commands

**qos weight**  
**rate**

# QoS Circuit Configuration

---

This chapter describes the tasks and commands used to configure and applications for SmartEdge® OS quality of service (QoS) features.

**Note** In this chapter, the term, circuit, refers to a port, channel, permanent virtual circuit (PVC), or link group.

For information about other QoS configuration tasks and commands, see the following chapters:

- Chapter 12, “QoS Rate- and Class-Limiting Configuration”—Rate- and class-limiting features (metering and policing policies)
- Chapter 13, “QoS Scheduling Configuration”—Scheduling features (scheduling policies)

For information about the tasks and commands used to monitor, troubleshoot, and administer QoS, see the “QoS Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

**Note** In this chapter, the term, first-generation Asynchronous Transfer Mode (ATM) OC traffic card, refers to a 2-port ATM OC-3c/STM-1c or ATM OC-12c/STM-4c traffic card; similarly, the term, second-generation ATM OC traffic card, refers to a 4-port ATM OC-3c/STM-1c or Enhanced ATM OC-12c/STM-4c traffic card.

The term, traffic-managed circuit, refers to a circuit or port on a Gigabit Ethernet 3 (GE3) or Gigabit Ethernet 1020 (GE1020) traffic card.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

The Internet provides only best-effort service, offering no guarantees on when or whether a packet is delivered to the receiver. However, the SmartEdge OS offers QoS differentiation based on the subscriber record, the traffic type, and the application. QoS policies create and enforce levels of service and bandwidth rates, and prioritize how packets are scheduled into egress queues. QoS differentiation for circuits is based on the configuration tasks that are described in the following sections:

- Circuit Configuration with QoS Policies
- Hierarchical Configuration for Traffic-Managed Circuits
- Propagation of QoS Across Layer 3 and Layer 2 Networks

## Circuit Configuration with QoS Policies

You can attach both a metering and a policing policy to any port, channel, or permanent virtual circuit (PVC), to cross-connected ATM and 802.1Q PVCs, and to link groups. QoS metering and policing policies are described in Chapter 12, “QoS Rate- and Class-Limiting Configuration.”

You can attach a scheduling policy to individual circuits (that are not cross-connected); however, the type of scheduling policy depends on the type of traffic card. QoS scheduling policies are described in Chapter 13, “QoS Scheduling Configuration.”

You can also attach metering, policing, and scheduling policies to subscriber circuits; the type of scheduling policy depends on the type of traffic card on which the subscriber session is initiated. Layer 2 Tunneling Protocol (L2TP) network server (LNS) subscriber sessions are limited to priority weighted fair queuing (PWFQ) policies. To attach a QoS policy of any type to a subscriber circuit, you attach it to the subscriber record or profile. The system applies the policy to the subscriber circuit (port, channel, or PVC) on which the session is initiated.

**Note** You can also configure a subscriber record or profile to reference a hierarchical node on a traffic-managed port and attach the PWFQ policy to the hierarchical node. For more information about hierarchical nodes and traffic-managed ports, see the “Hierarchical Configuration for Traffic-Managed Circuits” section. For more information about attaching PWFQ policies to subscriber records and hierarchical nodes, see the “Configuration Guidelines” section.

Table 14-1 lists the traffic cards and their circuits to which QoS scheduling policies can be attached.

**Note** Certain restrictions apply to the attachment of a QoS scheduling policy to a port, channel, or PVC; for detailed usage guidelines for each type of circuit and policy, see the description for the **qos policy queuing** command (in the appropriate circuit configuration mode).

Restrictions also apply to the configuration of the circuit; for information about configuring traffic card ports, channels, and circuits, see the “ATM, Ethernet, and POS Port Configuration,” the “Clear-Channel and Channelized Port and Channel Configuration,” the “Circuit Configuration,” and the “Cross-Connection Configuration” chapters in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.



**Table 14-1 QoS Scheduling Policy Support for SmartEdge Traffic Cards**

| Type                                     | Traffic Card                                                                                                                                     | Circuit                                                                                                                                          | Policy     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| First-generation ATM OC                  | ATM OC-12c/STM-4c IR (1-port)<br>ATM OC-3c/STM-1c IR (2-port)                                                                                    | ATM PVC                                                                                                                                          | EDRR or PQ |
| Second-generation ATM OC                 | Enhanced ATM OC-12c/STM-4c IR (1-port)<br>ATM OC-3c/STM-1c IR (4-port)                                                                           | ATM PVC                                                                                                                                          | ATMWFQ     |
| ATM DS-3                                 | ATM DS-3 (12-port)                                                                                                                               | ATM PVC                                                                                                                                          | ATMWFQ     |
| Ethernet                                 | 10/100 Ethernet (12-port)                                                                                                                        | Port, 802.1Q tunnel, 802.1Q PVC                                                                                                                  | EDRR or PQ |
| Gigabit Ethernet                         | Gigabit Ethernet (4-port)<br>Advanced Gigabit Ethernet (4-port)<br>10-Gbps Gigabit Ethernet (1-port)                                             | Port, 802.1Q tunnel, 802.1Q PVC<br><br>This traffic card does not support scheduling policies.                                                   | EDRR or PQ |
| Gigabit Ethernet with traffic management | Gigabit Ethernet 3 (4-port)<br>Gigabit Ethernet 1020 (10-port)<br>Gigabit Ethernet 1020 (20-port)                                                | Port, 802.1Q tunnel, 802.1Q PVC, hierarchical node                                                                                               | PWFQ       |
| PDH                                      | Channelized DS-3 (3-port)<br>Channelized DS-3 (12-port)<br>Clear-Channel DS-3 (12-port)<br>Clear-Channel E3 (6-port)<br>Channelized E1 (24-port) | Clear-channel port, DS-1 channel, Frame Relay PVC<br><br>Port, Frame Relay PVC<br><br>Clear-channel E1 port, DS-0 channel group, Frame Relay PVC | EDRR or PQ |
| POS                                      | OC-48c/STM-16c ER (1-port)<br>OC-48c/STM-16c LR (1-port)<br>OC-48c/STM-16c SR (1-port)<br>OC-12c/STM-4c IR (4-port)<br>OC-3c/STM-1c IR (8-port)  | Port, Frame Relay PVC                                                                                                                            | EDRR or PQ |
| SDH                                      | Channelized STM-1 (3-port) <sup>1</sup>                                                                                                          | Clear-channel E1 channel, DS-0 channel group, Frame Relay PVC                                                                                    | EDRR or PQ |
| SONET                                    | Channelized OC-12 to DS-3 IR (1-port) <sup>2</sup><br>Channelized OC-12 to DS-1 IR (1-port) <sup>3</sup>                                         | Clear-channel DS-3 channel, Frame Relay PVC<br>Clear-channel DS-3 channel, DS-1 channel, Frame Relay PVC                                         | EDRR or PQ |

1. The ports on this traffic card support the following Plesiochronous Digital Hierarchy (PDH) channels: DS-0 channel groups and E1 channels.

2. The ports on this traffic card support the following PDH channels: clear-channel DS-3 channels.

3. The ports on this traffic card support the following PDH channels: DS-1 channels and DS-3 channels.

## Hierarchical Configuration for Traffic-Managed Circuits

Hierarchical configuration provides two functions to support traffic-managed circuits on Gigabit Ethernet traffic cards that support traffic management:

- Hierarchical scheduling—Performs QoS scheduling at the port, 802.1Q tunnel, and 802.1Q PVC levels, using PWFQ policies.
- Hierarchical nodes and node groups—Performs QoS scheduling and shaping using PWFQ policies for subscriber sessions assigned to hierarchical nodes.

**Note** Traffic-managed ports are limited to ports on the GE3 and GE1020 traffic cards. Hierarchical nodes and scheduling are supported only on these ports.

These functions are described in the following sections:

- Hierarchical Scheduling
- Hierarchical Nodes and Node Groups

### Hierarchical Scheduling

Hierarchical scheduling operates on PWFQ queues in either of two modes: strict and weighted round robin (WRR). In a PWFQ policy, each queue is assigned a priority and a relative weight, which are used as follows:

- In strict mode, each queue is serviced according to the priority that you assigned to the queue.
- In WRR mode, each queue is serviced in round-robin order according to its priority and its traffic share, as determined by the relative weight that you assigned to the queue.

You can specify hierarchical scheduling at any level (port, 802.1Q tunnel, and 802.1Q PVC) on a traffic-managed port and on multiple levels. A level that does not have hierarchical scheduling specified inherits the scheduling specified at the next higher level.

### Hierarchical Nodes and Node Groups

A hierarchical node functions as an individual circuit, such as an 802.1Q PVC; you can assign a traffic rate and attach a PWFQ policy to it. In addition, you can specify the scheduling mode for the queues defined by the PWFQ policy, either strict or WRR.

Each node is a member of a node group. Like the individual nodes within it, a node group functions as a circuit, such as an 802.1Q tunnel. You can assign a traffic rate and a scheduling mode (which might not be the same traffic rate or scheduling mode assigned to any of the nodes within the group) to a node group; node groups do not support PWFQ policies.

When you configure a subscriber record or profile to reference a hierarchical node, all sessions for that subscriber are governed by the QoS PWFQ policy attached to that node and to the hierarchical scheduling for the node and for the node group.

**Note** You can also attach a PWFQ policy directly to a subscriber record or profile. However, if you attach a PWFQ policy to the subscriber record and another PWFQ policy to the hierarchical node, the policy that you attach to the subscriber record supersedes the policy that you attach to the hierarchical node.

## Propagation of QoS Across Layer 3 and Layer 2 Networks

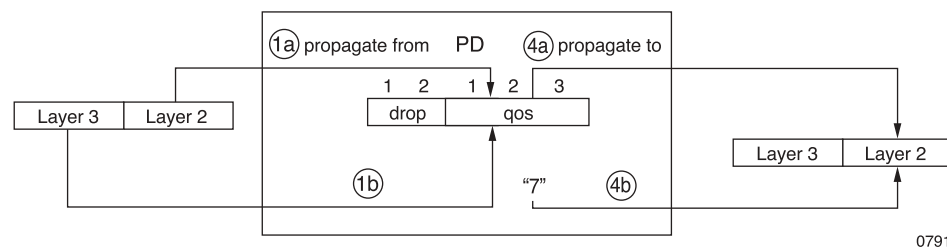
You can configure the SmartEdge OS to propagate IP DSCP settings in Layer 3 packets as they travel across Ethernet virtual LANs (VLANs), Multiprotocol Label Switching (MPLS) networks, and Layer 2 Tunneling Protocol (L2TP) networks. Conversely, Ethernet 802.1p priority bits, MPLS experimental (EXP) bits, and IP DSCP settings in Layer 3 packets encapsulated in L2TP packets can be propagated across IP networks. IP DSCP drop precedence settings can be propagated to the ATM cell loss priority (CLP) bit; however, the reverse is not true.

QoS propagation for a packet uses a packet descriptor (PD), which includes a three-bit qos field and a two-bit drop field, as shown in Figure 14-1. The SmartEdge OS uses these PD fields to perform the following functions for an incoming Layer 2 packet:

1. Depending on configuration for the inbound circuit protocol, it populates the PD for this packet, using one of the following functions:
  - a. If a QoS propagate from command is configured for the Layer 2 protocol, it copies the priority bits from the Layer 2 header to the qos field in the PD, and, depending on the Layer 2 protocol (either 802.1Q or L2TP), it copies the qos field in the PD to the IP DSCP bits in the Layer 3 header.
  - b. If it is not configured, it copies the three-most significant IP DSCP bits from the Layer 3 header in the incoming packet to the qos field in the PD and the drop precedence settings in that header to the drop field in the PD.
2. If a QoS policing policy, which can include a policy access control list (ACL), that includes a mark command (of any type) is attached to the inbound circuit, it modifies the bits in the qos and drop fields in the PD based on the policy.

A decision is made whether to forward the incoming Layer 3 packet to the outbound circuit for further QoS processing.

**Figure 14-1 Propagation of QoS Across Layer 3 and Layer 2 Networks**



3. If a QoS metering policy (which can include a policy ACL) that includes a mark command (of any type) is attached to the outbound circuit, it modifies the bits in the qos and drop fields in the PD based on the policy.
4. It encapsulates the Layer 3 packet in a Layer 2 packet, using one of the following functions:
  - a. If a QoS propagate to command is configured for the Layer 2 protocol, it copies the qos field in the PD to the priority bits in the Layer 2 header.
  - b. If it is not configured, it sets the priority bits in the Layer 2 header to the default (lowest) priority.
5. It then uses the qos field in the PD to determine the egress queue for the outgoing packet.

The following sections further describe QoS propagation:

- Propagation of QoS from IP to ATM
- Propagation of QoS Between IP and Ethernet
- Propagation of QoS Between IP and MPLS
- Propagation of QoS Between IP and L2TP

## Propagation of QoS from IP to ATM

The CLP bit in the ATM header of a cell provides a method of controlling the discarding of cells in a congested ATM environment. A CLP bit contains three settings: 0, 1, or propagate qos. ATM cells with setting of 1 are discarded before cells with a setting of 0. By default, the CLP bit is set to 0. When the CLP bit is configured to propagate QoS, the IP DSCP bits in the PD are used to determine if the CLP bit should be set and thus which ATM cells to discard in an ATM congested network. IP DSCP bits are mapped to the ATM CLP bit as described in Table 14-2.

**Table 14-2 Mapping IP DSCP Bits to the ATM CLP Bit**

| IP DSCP               | ATM CLP Bit |
|-----------------------|-------------|
| Network Control       | 0           |
| Reserved              | 0           |
| EF                    | 0           |
| AF11 AF21, AF31, AF41 | 0           |
| AF12 AF22, AF32, AF42 | 1           |
| AF13 AF23, AF33, AF43 | 1           |
| DF                    | 1           |

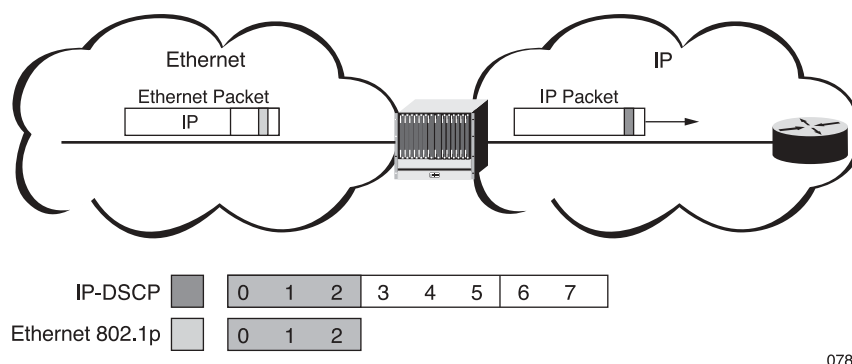
**Note** You can also use the **mark dscp** and **mark precedence** commands (in metering policy or policing policy configuration mode) to indirectly set the ATM CLP bit.

## Propagation of QoS Between IP and Ethernet

802.1p priority is carried in virtual LAN (VLAN) tags defined in IEEE 802.1p. A field in the VLAN tag carries one of eight priority values (3 bits in length), recognizable by Layer 2 devices. This marking determines the service level the packet receives when crossing an 802.1p-enabled network segment. IP DSCP priority bits are mapped to Ethernet 802.1p bits, in either or both directions, depending on whether you configure the **qos propagate from ethernet** and **qos propagate to ethernet** commands (in dot1q profile configuration mode). As shown in Figure 14-2, the following steps occur for an incoming 802.1Q packet:

1. As a 802.1Q packet enters the SmartEdge router, its 802.1p bits are copied to the PD.
2. The PD is copied to the IP DSCP field in the Layer 3 packet.
3. By default, the three most significant bits of the IP DSCP field are copied back to the PD qos field, and the two IP DSCP drop precedence bits are copied to the PD drop field.

Figure 14-2 Propagation of QoS Between IP and Ethernet

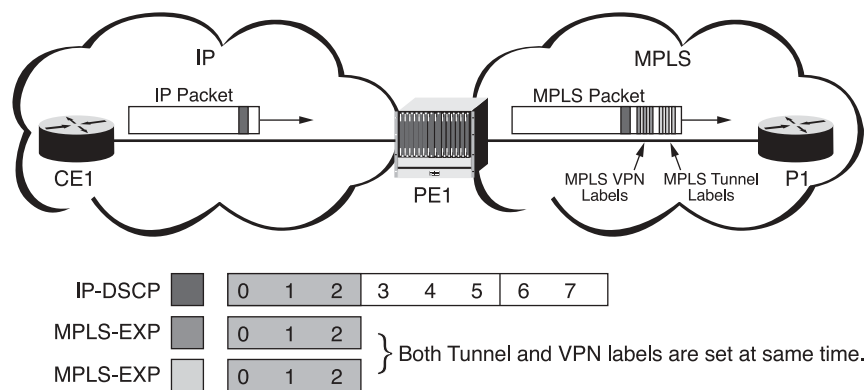


0789

## Propagation of QoS Between IP and MPLS

MPLS EXP bits use one of eight priority values (3 bits in length), recognizable by Layer 2 devices. This marking determines the service level the packet receives when crossing an MPLS-enabled network segment. IP DSCP priority bits are mapped to MPLS EXP bits, in either or both directions, depending on whether you configure the **qos propagate from-mpls** and **qos propagate to-mpls** commands (in MPLS router configuration mode); see Figure 14-3.

Figure 14-3 Propagation of QoS Between IP and MPLS

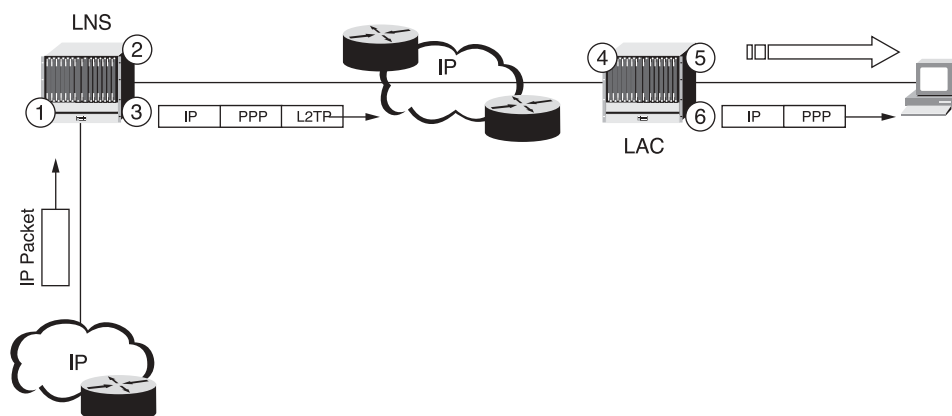


0790

## Propagation of QoS Between IP and L2TP

With L2TP packets, the IP DSCP and the precedence bits of the original IP packet are copied. The downstream process from the network to the SmartEdge router configured as an LNS to the SmartEdge router configured as an L2TP access concentrator (LAC) to the subscriber is illustrated in Figure 14-4.

**Figure 14-4 Propagation of QoS Downstream from the Network**

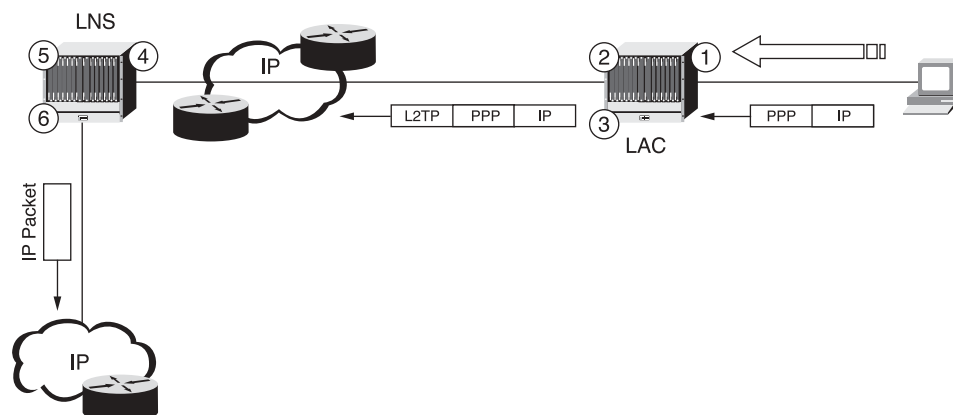


0792

1. At the LNS, the SmartEdge OS copies the IP DSCP bits from the inner subscriber IP packet header in the incoming IP packet to the PD qos field.
2. It then copies the qos field to the IP DSCP bits in the outer L2TP IP packet header, using the **propagate qos to l2tp** command (in L2TP peer configuration mode), if configured. If the command is not configured, it sets the IP DSCP bits to the default (lowest) priority.
3. The SmartEdge OS selects an egress queue for the L2TP packet, based on the qos field.
4. At the LAC, the SmartEdge OS copies the IP DSCP bits in the outer L2TP IP packet header to the PD qos field.
5. It then copies the IP DSCP bits from the inner subscriber IP packet header to the PD qos field, using the **propagate qos from subscriber** command (in L2TP peer configuration mode), if configured. This operation overwrites the qos field set by step 4.
6. The SmartEdge OS selects an egress queue, based on the qos field in the PD.

The upstream process from the subscriber to the SmartEdge router configured as an LAC to the SmartEdge router configured as an LNS to the network is illustrated in Figure 14-5.

**Figure 14-5 Propagation of QoS Upstream from the Subscriber**



0793

1. At the LAC, if the **propagate qos from subscriber** command (in L2TP peer configuration mode) with the **upstream** keyword is configured, the SmartEdge OS copies the IP DSCP bits from the inner subscriber IP packet header in the incoming IP packet to the qos field in the PD. If the **propagate qos from subscriber** command is not configured, it sets the qos field to the default (lowest) priority.
2. It then copies the qos field to the IP DSCP bits in the outer L2TP IP packet header, using the **propagate qos to l2tp** command (in L2TP peer configuration mode), if configured. If the command is not configured, it sets the IP DSCP bits to the default priority.
3. The SmartEdge OS selects an egress queue for the L2TP packet based on the qos field.
4. At the LNS, the SmartEdge OS copies the IP DSCP bits from the outer L2TP IP packet header in the incoming IP packet to the qos field in the PD.
5. It then copies the qos field to the IP DSCP bits in the inner subscriber IP packet header, using the **propagate qos from l2tp** command (in L2TP peer configuration mode), if configured. If it is not, the inner subscriber IP packet header is not altered.
6. The SmartEdge OS selects an egress queue for the IP packet based on the qos field.

## Configuration Tasks

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section. You can enter unnumbered tasks in any sequence.

To configure circuits for QoS features, perform the tasks described in the following sections:

- Configuration Guidelines
- Configure an ATM PVC for QoS
- Configure an Ethernet Circuit for QoS

- Configure a PDH Circuit for QoS
- Configure a POS Circuit for QoS
- Configure Cross-Connected Circuits for QoS
- Configure a Subscriber Circuit for QoS
- Configure L2TP for QoS
- Configure MPLS for QoS

## Configuration Guidelines

This section includes configuration guidelines that affect more than one command or a combination of commands:

- If you attach an enhanced deficit round-robin (EDRR) policy to a PVC, you must also attach it to the port on which you have configured the PVC.
- Channelized DS-3 traffic cards support the attachment of EDRR and PQ policies with two to eight queues to DS-1 channels. However, the total number of queues that are supported on any DS-3 traffic card is limited to 1,018 queues; 348 of which are reserved by the system and 670 of which are available for QoS scheduling policies. Therefore, you can configure up to 167 DS-1 channels with 4-queue policies and up to 83 DS-1 channels with 8-queue policies.
- If you attach a PWFQ policy to a hierarchical node and another PWFQ policy directly to the subscriber record that references that node, the subscriber session is governed by the PWFQ policy attached directly to the subscriber record.
- Subscriber traffic is managed differently with PWFQ policies attached directly to the subscriber record and attached to the hierarchical node:
  - If you attach the policy directly to the subscriber record, the traffic for that subscriber has its own set of queues.
  - If you reference a hierarchical node that has an attached PWFQ policy, the traffic for that subscriber shares the queues for that policy with all other subscribers that reference that node.
- The following guidelines apply to cross-connected circuits:
  - When you attach a QoS metering or policing policy to a cross-connected circuit, you can attach a policy to each individual circuit before or after you make the cross-connection.
  - You can attach a different metering or policing policy to each circuit.
  - You can attach both a metering and a policing policy to each circuit.
  - Scheduling policies are not supported on cross-connected circuits.
- The following guidelines apply to Ethernet and 802.1Q link groups:
  - You attach a policy to an Ethernet port rather than the link group of which it is a member; you attach the policy using one of the QoS policy commands (**qos policy metering**, **qos policy policing**, **qos policy queuing**) in port configuration mode.



- You can attach any type of QoS policy that is supported by that type of Ethernet port. These include metering, policing, EDRR, PQ, and PWFQ policies. However, to preserve the operational characteristics of a link group, it is recommended that you attach the same set of policies (metering, policing, and scheduling) to every constituent port in the link group.

## Configure an ATM PVC for QoS

To configure an ATM PVC for QoS, perform the tasks described in the following sections:

- Configure a PVC on a First-Generation ATM OC Traffic Card
- Configure a PVC on an ATM DS-3 or Second-Generation ATM OC Traffic Card

### Configure a PVC on a First-Generation ATM OC Traffic Card

To configure an ATM PVC on a first-generation ATM OC traffic card, perform the tasks described in Table 14-3; enter all commands in ATM PVC configuration mode, unless otherwise noted.

**Table 14-3 Configure a PVC on a First Generation ATM OC Traffic Card**

| Task                                                                                               | Root Command                       | Notes                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| For packets going out of the SmartEdge router, propagate IP DSCP bits to the CLP bit in ATM cells. | <b>clpbit propagate qos to atm</b> | Enter this command in ATM profile configuration mode.                                                                                                                                       |
| Attach a policing policy.                                                                          | <b>qos policy policing</b>         |                                                                                                                                                                                             |
| Attach a metering policy.                                                                          | <b>qos policy metering</b>         |                                                                                                                                                                                             |
| Attach a scheduling policy.                                                                        | <b>qos policy queuing</b>          | Possible policy types are EDRR and PQ. You must attach an EDRR policy to both the port and the PVC. To attach the EDRR policy to the port, enter this command in ATM OC configuration mode. |
| Optional. Modify the mode of an EDRR policy algorithm.                                             | <b>qos mode</b>                    | Enter this command in ATM OC configuration mode.<br>By default, the mode is normal. Only one mode type is supported on a single port.                                                       |

### Configure a PVC on an ATM DS-3 or Second-Generation ATM OC Traffic Card

To configure an ATM PVC on a second-generation ATM OC or ATM DS-3 traffic card, perform the tasks described in Table 14-4; enter all commands in ATM PVC configuration mode, unless otherwise noted.

**Table 14-4 Configure a PVC on an ATM DS-3 or Second-Generation ATM OC Traffic Card**

| Task                                                                                               | Root Command                       | Notes                                                                 |
|----------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------|
| For packets going out of the SmartEdge router, propagate IP DSCP bits to the CLP bit in ATM cells. | <b>clpbit propagate qos to atm</b> | Enter this command in ATM profile configuration mode.                 |
| Attach a policing policy.                                                                          | <b>qos policy policing</b>         |                                                                       |
| Attach a metering policy.                                                                          | <b>qos policy metering</b>         |                                                                       |
| Attach a scheduling policy to a PVC. <sup>1</sup>                                                  | <b>qos policy queuing</b>          | Only ATMWFQ policies are supported; you can attach them only to PVCs. |

1. An ATMWFQ policy cannot be attached to a PVC that is shaped as UBR.

## Configure an Ethernet Circuit for QoS

To configure a circuit on any Ethernet traffic card for QoS, including any version of a Gigabit Ethernet traffic card, perform the tasks described in the following sections:

- Configure Any Ethernet or Gigabit Ethernet Circuit for QoS
- Configure a Traffic-Managed Port for Hierarchical Scheduling
- Configure a Traffic-Managed Port for Hierarchical Nodes

### Configure Any Ethernet or Gigabit Ethernet Circuit for QoS

To configure an Ethernet or Gigabit Ethernet (any version) port, 802.1Q tunnel, or 802.1Q PVC, perform the tasks described in Table 14-5; enter all commands in port or dot1Q PVC configuration mode, unless otherwise noted.

**Table 14-5 Configure Any Ethernet or Gigabit Ethernet Circuit for QoS**

| Task                                                                                                         | Root Command                       | Notes                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| For packets coming into the SmartEdge router, propagate Ethernet 802.1p user priority bits to IP DSCP bits.  | <b>propagate qos from ethernet</b> | Enter this command in dot1q profile configuration mode.                                                               |
| For packets going out of the SmartEdge router, propagate IP DSCP bits to Ethernet 802.1p user priority bits. | <b>propagate qos to ethernet</b>   | Enter this command in dot1q profile configuration mode.                                                               |
| Assign a priority group to the port, tunnel, or PVC.                                                         | <b>qos priority</b>                | The QoS bit setting for packets traveling across the ingress circuit is not changed by the priority group assignment. |
| Attach a policing policy to the port, tunnel, or PVC.                                                        | <b>qos policy policing</b>         |                                                                                                                       |
| Set the rate for outgoing traffic for a Gigabit Ethernet port.                                               | <b>qos rate</b>                    |                                                                                                                       |
| Attach a metering policy to a port, tunnel, or PVC.                                                          | <b>qos policy metering</b>         |                                                                                                                       |
| Attach a scheduling policy to a port, tunnel, or PVC.                                                        | <b>qos policy queuing</b>          | Possible policy types are EDRR, PQ, and PWFQ. <sup>1</sup>                                                            |
| Optional. Modify the mode of an EDRR policy algorithm.                                                       | <b>qos mode</b>                    | By default, the mode is normal. Only one mode type is supported on a single port.                                     |

1. EDRR and PQ policies are not supported on traffic-managed circuits; these circuits support only PWFQ policies. 10GE traffic cards do not support scheduling policies.

## Configure a Traffic-Managed Port for Hierarchical Scheduling

To configure a traffic-managed port and any 802.1Q tunnels and PVCs configured on it for hierarchical scheduling with a PWFQ policy, perform the tasks described in Table 14-6; enter all commands in port configuration mode, unless otherwise noted. For information about the **dot1q pvc** command (in port configuration mode), see the “Circuit Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

**Table 14-6 Configure a Traffic-Managed Port for Hierarchical Scheduling**

| #  | Task                                                                               | Root Command                 | Notes                                                                                                                                                                                                |
|----|------------------------------------------------------------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Set the maximum and minimum rates for the port.                                    | <b>qos rate</b>              | You must specify the maximum rate; the minimum rate is optional.                                                                                                                                     |
| 2. | Specify the scheduling algorithm for the port.                                     | <b>qos hierarchical mode</b> |                                                                                                                                                                                                      |
| 3. | Attach a PWFQ policy to the port.                                                  | <b>qos policy queuing</b>    | You can attach a policy to any or all 802.1Q tunnels and PVCs as well as the port.                                                                                                                   |
| 4. | Create one or more 802.1Q tunnels or PVCs and access dot1q PVC configuration mode. | <b>dot1q pvc</b>             |                                                                                                                                                                                                      |
| 5. | Set the maximum and minimum rates for the tunnel or PVC.                           | <b>qos rate</b>              | Enter this command in dot1q PVC configuration mode. You must specify the maximum rate; the minimum rate is optional. You cannot set a minimum rate if you also assign a relative weight to this PVC. |
| 6. | Assign a relative weight to this PVC.                                              | <b>qos weight</b>            | Enter this command in dot1q PVC configuration mode. You cannot assign a relative weight if you also set a minimum rate for this PVC.                                                                 |
| 7. | Specify the scheduling algorithm for the tunnel or PVC.                            | <b>qos hierarchical mode</b> | Enter this command in dot1q PVC configuration mode.                                                                                                                                                  |
| 8. | Attach a PWFQ policy to the tunnel or PVC.                                         | <b>qos policy queuing</b>    | Enter this command in dot1q PVC configuration mode. You can attach a policy to any or all tunnels and PVCs, as well as the port.                                                                     |

## Configure a Traffic-Managed Port for Hierarchical Nodes

To configure a traffic-managed port for hierarchical nodes, node groups, and attach PWFQ policies to them, perform the tasks described in Table 14-7; enter all commands in port configuration mode, unless otherwise noted.

**Table 14-7 Configure a Traffic-Managed Port for Hierarchical Nodes**

| #  | Task                                                                                               | Root Command                 | Notes                                                            |
|----|----------------------------------------------------------------------------------------------------|------------------------------|------------------------------------------------------------------|
| 1. | Set the maximum and minimum rates for the port.                                                    | <b>qos rate</b>              | You must specify the maximum rate; the minimum rate is optional. |
| 2. | Specify the scheduling algorithm for the port.                                                     | <b>qos hierarchical mode</b> |                                                                  |
| 3. | Create one or more hierarchical node groups and access hierarchical node group configuration mode. | <b>qos node-group</b>        |                                                                  |

**Table 14-7 Configure a Traffic-Managed Port for Hierarchical Nodes** (*continued*)

| #   | Task                                                                                   | Root Command                 | Notes                                                                                                                                                                                                                     |
|-----|----------------------------------------------------------------------------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.  | Set the maximum and minimum rates for the node groups.                                 | <b>qos rate</b>              | Enter this command in hierarchical node group configuration mode. You must specify the maximum rate; the minimum rate is optional. You cannot set a minimum rate if you also assign a relative weight to this node group. |
| 5.  | Assign a relative weight to this node group.                                           | <b>qos weight</b>            | Enter this command in hierarchical node group configuration mode. You cannot assign a relative weight if you also set a minimum rate for this node group.                                                                 |
| 6.  | Specify the scheduling algorithm for the node groups.                                  | <b>qos hierarchical mode</b> | Enter this command in hierarchical node group configuration mode. The mode need not be the same as the one you specify for the port.                                                                                      |
| 7.  | Create one or more hierarchical nodes and access hierarchical node configuration mode. | <b>qos node</b>              | Enter this command in hierarchical node group configuration mode.                                                                                                                                                         |
| 8.  | Set the maximum and minimum rates for these nodes.                                     | <b>qos rate</b>              | Enter this command in hierarchical node configuration mode. You must specify the maximum rate; the minimum rate is optional. You cannot set a minimum rate if you also assign a relative weight to this node.             |
| 9.  | Assign a relative weight for these nodes.                                              | <b>qos weight</b>            | Enter this command in hierarchical node configuration mode. You cannot assign a relative weight if you also set a minimum rate for this node.                                                                             |
| 10. | Specify the scheduling algorithm for these nodes.                                      | <b>qos hierarchical mode</b> | Enter this command in hierarchical node configuration mode. The mode need not be the same as the one you specify for the port or node group.                                                                              |
| 11. | Attach a PWFQ policy to these nodes.                                                   | <b>qos policy queuing</b>    | Enter this command in hierarchical node configuration mode. The policy need not be the same as the one you attach to the port, tunnel, or PVC.                                                                            |

## Configure a PDH Circuit for QoS

To configure a PDH circuit (port, channel, PVC, or link group) for QoS, perform the tasks described in Table 14-8; enter all commands in DS-0 group, DS-1, DS-3, E1, E3, link group, or Frame Relay PVC configuration mode (depending on the type of PDH circuit), unless otherwise noted.

**Table 14-8 Configure a PDH Circuit for QoS**

| Task                                                   | Root Command               | Notes                                                                                                                 |
|--------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Assign a priority group.                               | <b>qos priority</b>        | The QoS bit setting for packets traveling across the ingress circuit is not changed by the priority group assignment. |
| Attach a policing policy.                              | <b>qos policy policing</b> |                                                                                                                       |
| Attach a metering policy.                              | <b>qos policy metering</b> |                                                                                                                       |
| Attach a scheduling policy.                            | <b>qos policy queuing</b>  | Policy types include EDRR and PQ.                                                                                     |
| Optional. Modify the mode of an EDRR policy algorithm. | <b>qos mode</b>            | By default, the mode is normal. Only one mode type is supported on a single port.                                     |

## Configure a POS Circuit for QoS

To configure a circuit on a Packet over SONET/SDH (POS) traffic card for QoS, perform the tasks described in Table 14-9; enter all commands in port configuration mode.

**Table 14-9 Configure a POS Circuit for QoS**

| Task                                                   | Root Command               | Notes                                                                                                                 |
|--------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Assign a priority group.                               | <b>qos priority</b>        | The QoS bit setting for packets traveling across the ingress circuit is not changed by the priority group assignment. |
| Attach a policing policy.                              | <b>qos policy policing</b> |                                                                                                                       |
| Attach a metering policy.                              | <b>qos policy metering</b> |                                                                                                                       |
| Attach a scheduling policy.                            | <b>qos policy queuing</b>  | Policy types include EDRR and PQ.                                                                                     |
| Optional. Modify the mode of an EDRR policy algorithm. | <b>qos mode</b>            | By default, the mode is normal. Only one mode type is supported on a single port.                                     |

## Configure Cross-Connected Circuits for QoS

To configure a cross-connected circuit for QoS, perform the tasks described in Table 14-10. You cannot attach a scheduling policy to a cross-connected circuit; only metering and policing policies are supported on either or both circuits.

**Note** You can perform the tasks in Table 14-10 in any order.

**Table 14-10 Configure a Cross-Connected Circuit for QoS**

| Task                                                                    | Root Command                                                                          | Notes                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure the inbound circuit for QoS with one of the following tasks:  |                                                                                       |                                                                                                                                                                                                                            |
| • An inbound ATM PVC.                                                   | Perform the tasks in Table 14-3 or Table 14-4, but do not attach a scheduling policy. |                                                                                                                                                                                                                            |
| • An inbound 802.1Q PVC.                                                | Perform the tasks in Table 14-6, but do not attach a scheduling policy.               |                                                                                                                                                                                                                            |
| Configure the outbound circuit for QoS with one of the following tasks: |                                                                                       |                                                                                                                                                                                                                            |
| • An outbound ATM PVC.                                                  | Perform the tasks in Table 14-3 or Table 14-4, but do not attach a scheduling policy. |                                                                                                                                                                                                                            |
| • An outbound 802.1Q PVC.                                               | Perform the tasks in Table 14-6, but do not attach a scheduling policy.               |                                                                                                                                                                                                                            |
| Create the cross-connection between the inbound and outbound circuits.  | <b>xc</b>                                                                             | Enter this command in global configuration mode. For information about this command, see the "Cross-Connection Configuration" chapter in the <i>Ports, Circuits, and Tunnels Configuration Guide</i> for the SmartEdge OS. |

## Configure a Subscriber Circuit for QoS

You configure a subscriber circuit (or an LNS subscriber session) for QoS by configuring the subscriber record or profile; to configure a subscriber record or profile and thus any circuit on which the subscriber session is created, perform one or more of the tasks described in Table 14-11; enter all commands in subscriber configuration mode.

**Table 14-11 Configure a Subscriber Circuit for QoS**

| Task                                                   | Root Command               | Notes                                                                                                          |
|--------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------|
| Create a reference to a hierarchical node.             | <b>qos node-reference</b>  |                                                                                                                |
| Attach a policing policy.                              | <b>qos policy policing</b> |                                                                                                                |
| Attach a metering policy.                              | <b>qos policy metering</b> |                                                                                                                |
| Attach a scheduling policy.                            | <b>qos policy queuing</b>  | Policy types include ATMWFQ, EDRR, PQ, and PWFQ. Only PWFQ policies are supported for LNS subscriber sessions. |
| Optional. Modify the mode of an EDRR policy algorithm. | <b>qos mode</b>            | By default, the mode is normal. Only one mode type is supported on a single port.                              |

## Configure L2TP for QoS

To configure L2TP for QoS to propagate IP DSCP bits in the downstream direction, perform the tasks described in Table 14-12; enter all commands in L2TP peer configuration mode for the default peer.

**Table 14-12 Configure L2TP for QoS in the Downstream Direction**

| Task                                                                                                                                                               | Root Command                         | Notes                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------------------------------------------------------|
| For network packets coming into the SmartEdge router when it is configured as an LNS, propagate the IP DSCP bits to the L2TP IP packet header.                     | <b>propagate qos to l2tp</b>         |                                                          |
| For L2TP IP packets coming into the SmartEdge router when it is configured as a LAC, propagate the IP DSCP bits from the IP packet header to the PD priority bits. | <b>propagate qos from subscriber</b> | Specify the <b>downstream</b> keyword for this function. |

To configure L2TP for QoS to propagate IP DSCP bits in the upstream direction, perform the tasks described in Table 14-13; enter all commands in L2TP peer configuration mode for the default peer.

**Table 14-13 Configure L2TP for QoS in the Upstream Direction**

| Task                                                                                                                                                | Root Command                         | Notes                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------|
| For subscriber IP packets coming into the SmartEdge router when it is configured as a LAC, propagate the IP DSCP bits to the L2TP IP packet header. | <b>propagate qos from subscriber</b> | Specify the <b>upstream</b> keyword for this function. |
| For network packets coming into the SmartEdge router when it is configured as an LAC, propagate the PD priority bits to the L2TP IP packet header.  | <b>propagate qos to l2tp</b>         |                                                        |
| For network packets going out of the SmartEdge router when it is configured as an LNS, propagate PD priority bits to the IP packet header.          | <b>propagate qos from l2tp</b>       |                                                        |

## Configure MPLS for QoS

To configure MPLS for QoS, perform the tasks described in one of the following sections:

- Propagate QoS Using IP DSCP Bits and MPLS EXP Bits
- Propagate QoS Using IP DSCP Bits Only

### Propagate QoS Using IP DSCP Bits and MPLS EXP Bits

To propagate QoS using IP DSCP bits to MPLS experimental (EXP) bits (instead of IP DSCP bits) and vice versa, perform the tasks described in Table 14-14; enter either or both commands in MPLS router configuration mode.

**Table 14-14 Propagate QoS Using IP DSCP Bits and MPLS EXP Bits**

| Task                                                                                    | Root Command                   | Notes |
|-----------------------------------------------------------------------------------------|--------------------------------|-------|
| For packets going out of the SmartEdge router, propagate MPLS EXP bits to IP DSCP bits. | <b>propagate qos from-mpls</b> |       |
| For packets coming into the SmartEdge router, propagate IP DSCP bits to MPLS EXP bits.  | <b>propagate qos to-mpls</b>   |       |

## Propagate QoS Using IP DSCP Bits Only

To propagate QoS by enabling the use of IP DSCP bits (instead of MPLS EXP bits) only, perform the task described in Table 14-15.

**Table 14-15 Propagate QoS Using IP DSCP Bits Only**

| Task                                                | Root Command                  | Notes                                                 |
|-----------------------------------------------------|-------------------------------|-------------------------------------------------------|
| Enable the use of IP DSCP bits (not MPLS EXP bits). | <b>egress prefer dscp-qos</b> | Enter this command in MPLS router configuration mode. |

---

## Configuration Examples

---

QoS configuration examples are included in the following sections:

- Attaching Rate- and Class-Limiting Policies
- Attaching Scheduling Policies
- Propagating QoS

## Attaching Rate- and Class-Limiting Policies

Examples of configuring PVCs and subscriber records for QoS policies are provided in the following sections:

- PVC Configuration
- Cross-Connected Circuit Configuration
- Subscriber Configuration

### PVC Configuration

The following example attaches a metering policy, *meter*, to an 802.1Q PVC on an Ethernet port:

```
[local]Redback(config)#port ethernet 4/2
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 200
[local]Redback(config-dot1q-pvc)#bind interface if-200 local
[local]Redback(config-dot1q-pvc)#qos policy metering meter
```

### Cross-Connected Circuit Configuration

The following example attaches a metering policy, *output*, to the inbound circuits of cross-connected 802.1Q PVCs on Ethernet ports:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 2001
[local]Redback(config-dot1q-pvc)#qos policy metering output
[local]Redback(config-dot1q-pvc)#exit
```



```
[local]Redback(config-port)#dot1q pvc 2051
[local]Redback(config-dot1q-pvc)#qos policy metering output
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 2101
[local]Redback(config-dot1q-pvc)#qos policy metering output
[local]Redback(config-dot1q-pvc)#exit
!
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 2001
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 2051
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 2101
!
[local]Redback(config)#xc 4/1 vlan-id 2001 to 4/3 vlan-id 2001
[local]Redback(config)#xc 4/1 vlan-id 2051 to 4/3 vlan-id 2051
[local]Redback(config)#xc 4/1 vlan-id 2101 to 4/3 vlan-id 2101
```

## Subscriber Configuration

The following example attaches a metering policy, meter, to a subscriber record:

```
[local]Redback(config)#subscriber name redback
[local]Redback(config-sub)#password redback
[local]Redback(config-sub)#qos policy metering meter
```

## Attaching Scheduling Policies

Examples of configuring ports and PVCs for QoS features using scheduling policies are provided in the following sections:

- Port Configuration
- PVC Configuration
- PWFQ Policy and Hierarchical Shaping
- PWFQ Policy and Hierarchical Scheduling

### Port Configuration

The following example attaches a PQ policy to a POS port:

```
[local]Redback(config)#port pos 2/1
[local]Redback(config-port)#qos policy queuing pos-qos
```

### PVC Configuration

The following example attaches a PQ scheduling policy to each of three 802.1Q PVCs:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 100
```

```
[local]Redback(config-dot1q-pvc)#bind interface if-100 local
[local]Redback(config-dot1q-pvc)#qos policy queuing PerVcQueuing
[local]Redback(config-dot1q-pvc)#dot1q pvc 101
[local]Redback(config-dot1q-pvc)#bind interface if-101 local
[local]Redback(config-dot1q-pvc)#qos policy queuing PerVcQueuing
[local]Redback(config-dot1q-pvc)#dot1q pvc 102
[local]Redback(config-dot1q-pvc)#bind interface if-102 local
[local]Redback(config-dot1q-pvc)#qos policy queuing PerVcQueuing
```

The following example attaches an EDRR policy, `example1`, to an ATM PVC and its port on a first-generation ATM OC traffic card:

```
[local]Redback(config)#port atm 6/1
[local]Redback(config-port)#qos policy queuing example1
[local]Redback(config-atm)#atm pvc 200 300 profile prof1 encaps multi
[local]Redback(config-atmpvc)#qos policy queuing example1
```

## **PWFQ Policy and Hierarchical Shaping**

The following example configures a GE3 port with the home node group with 5 DSLAM nodes and attaches a PWFQ policy to each node:

```
[local]Redback(config)#port ethernet 5/2
[local]Redback(config-port)#qos rate maximum 100000000
[local]Redback(config-port)#qos rate minimum 100000
[local]Redback(config-port)#qos hierarchical mode strict
[local]Redback(config-port)#qos node-group home 1
[local]Redback(config-h-node)#qos hierarchical mode wrr
[local]Redback(config-h-node)#qos node dslam 1 through 5
[local]Redback(config-h-node)#qos policy queuing pwfq4
```

## **PWFQ Policy and Hierarchical Scheduling**

The following example configures a GE3 port and its 802.1Q PVC for hierarchical scheduling and attaches a PWFQ policy to both the port (`pwfq-port`) and its PVC (`pwfq-pvc`):

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#qos rate maximum 100000000
[local]Redback(config-port)#qos rate minimum 100000
[local]Redback(config-port)#qos hierarchical mode strict
[local]Redback(config-port)#qos policy queuing pwfq-port
[local]Redback(config-port)#dot1q pvc 200
[local]Redback(config-dot1q-pvc)#qos rate maximum 100000000
[local]Redback(config-dot1q-pvc)#qos rate minimum 100000
[local]Redback(config-dot1q-pvc)#qos hierarchical mode wrr
[local]Redback(config-dot1q-pvc)#qos policy queuing pwfq-pvc
```

## Propagating QoS

The following example configures 802.1q profile, 8021q-on, to propagate QoS information between IP and any 802.1Q tunnel or PVC that has that profile assigned to it:

```
[local]Redback(config)#dot1q profile 8021p-on
[local]Redback(config-dot1q-profile)#propagate qos from ethernet
[local]Redback(config-dot1q-profile)#propagate qos to ethernet
[local]Redback(config-dot1q-profile)#exit
```

The following example propagates QoS on an 802.1Q PVC by configuring it with the 8021p-on profile:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 20 profile 8021p-on
[local]Redback(config-dot1q-pvc)#exit
```

The following example enables IP QoS information to be propagated to ATM on any ATM PVC or virtual path (VP) that has the profile, clp-on, assigned to it:

```
[local]Redback(config)#atm profile clp-on
[local]Redback(config-atm-profile)#clpbit propagate qos to atm
[local]Redback(config-atm-profile)#exit
```

The following example configures MPLS to propagate QoS in both directions:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mpls 100
[local]Redback(config-mpls)#propagate qos from mpls
[local]Redback(config-mpls)#propagate qos to mpls
[local]Redback(config-mpls)#exit
```

## Command Descriptions

This section describes the syntax and usage guidelines for the commands used to configure QoS policies. The commands are presented in alphabetical order.

|                                      |                            |
|--------------------------------------|----------------------------|
| <b>clpbit propagate qos to atm</b>   | <b>qos mode</b>            |
| <b>egress prefer dscp-qos</b>        | <b>qos node</b>            |
| <b>propagate qos from ethernet</b>   | <b>qos node-group</b>      |
| <b>propagate qos from l2tp</b>       | <b>qos node-reference</b>  |
| <b>propagate qos from-mpls</b>       | <b>qos policy metering</b> |
| <b>propagate qos from subscriber</b> | <b>qos policy policing</b> |
| <b>propagate qos to ethernet</b>     | <b>qos policy queuing</b>  |
| <b>propagate qos to l2tp</b>         | <b>qos priority</b>        |
| <b>propagate qos to-mpls</b>         | <b>qos rate</b>            |
| <b>qos hierarchical mode</b>         | <b>qos weight</b>          |

## clpbit propagate qos to atm

**clpbit propagate qos to atm**

{no | default} **clpbit propagate qos to atm**

### Purpose

For traffic going out of the SmartEdge router, propagates the IP Differentiated Services Code Point (DSCP) bits from IP packets to the cell loss priority (CLP) bit in cells transmitted over Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) that reference the ATM profile.

### Command Mode

ATM profile configuration

### Syntax Description

This command has no arguments or keywords.

### Default

IP DSCP bits are not propagated to the ATM CLP bit.

### Usage Guidelines

Use the **clpbit propagate qos to atm** command to propagate IP DSCP bits from IP packets to the CLP bit in cells transmitted over ATM PVCs that reference the ATM profile.

**Note** CLP bit priority settings cannot be propagated to IP DSCP bits.

**Note** For more information about the CLP bit and its use in ATM profiles, see the “Circuit Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

IP DSCP bits are mapped to the ATM CLP bit as described in Table 14-16.

**Table 14-16 IP DSCP Bits Mapped to the ATM CLP Bit**

| IP DSCP Bits          | ATM CLP Bit |
|-----------------------|-------------|
| Network Control       | 0           |
| Reserved              | 0           |
| EF                    | 0           |
| AF11 AF21, AF31, AF41 | 0           |
| AF12 AF22, AF32, AF42 | 1           |
| AF13 AF23, AF33, AF43 | 1           |
| DF                    | 1           |

Use the **no** or **default** form of this command to return the CLP bit setting to zero.

## Examples

The following example propagates IP DSCP bits from IP packets to the CLP bit in cells transmitted over ATM PVCs that reference the ATM profile, `low_rate`:

```
[local]Redback(config)#atm profile low_rate  
[local]Redback(config-atm-profile)#clpbit propagate qos to atm
```

## Related Commands

None

## egress prefer dscp-qos

**egress prefer dscp-qos**

**no egress prefer dscp-qos**

### Purpose

Enables the use of only IP Differentiated Services Code Point (DSCP) bits for queuing at the Multiprotocol Label Switching (MPLS) egress router.

### Command Mode

MPLS router configuration

### Syntax Description

This command has no keywords or arguments.

### Default

If penultimate hop popping is enabled, the tunnel label is removed at the penultimate hop, and the egress router uses the Virtual Private Network (VPN) label experimental (EXP) bits for queuing; however, if there is no VPN label, the egress router uses the IP DSCP bits for queuing. For more information, see the “MPLS Configuration” chapter in the *Routing Protocols Configuration Guide* for the SmartEdge OS.

### Usage Guidelines

Use the **egress prefer dscp-qos** command to enable the use of only IP DSCP bits for queuing at the MPLS egress router.

Use the **no** form of this command to return the system to its default behavior.

### Examples

The following example enables the use of only IP DSCP bits for queuing at the egress router:

```
[local]Redback(config-ctx)#router mpls 234  
[local]Redback(config-mpls)#egress prefer dscp-qos
```

### Related Commands

**propagate qos from-mpls**  
**propagate qos to-mpls**

# propagate qos from ethernet

**propagate qos from ethernet**

**no propagate qos from ethernet**

## Purpose

For packets coming into the SmartEdge router, propagates Ethernet 802.1p user priority bits to IP Differentiated Services Code Point (DSCP) bits.

## Command Mode

dot1q profile configuration

## Syntax Description

This command has no keywords or arguments.

## Default

Ethernet 802.1p user priority bits are not propagated to IP DSCP bits.

## Usage Guidelines

Use the **propagate qos from ethernet** command to propagate Ethernet 802.1p user priority bits to IP DSCP bits.

**Note** This command applies to incoming packets transmitted over 802.1Q permanent virtual circuits (PVCs) that reference the dot1q profile.

Use the **no** form of this command to disable the propagation of Ethernet 802.1p bits to IP DSCP bits.

## Examples

The following example propagates Ethernet 802.1p user priority bits to IP DSCP bits for incoming packets for all 802.1Q PVCs that reference the 802.1Q profile, 8021p-on:

```
[local]Redback(config)#dot1q profile 8021p-on  
[local]Redback(config-dot1q-profile)#propagate qos from ethernet
```

## Related Commands

**propagate qos to ethernet**

## propagate qos from l2tp

**propagate qos from l2tp**

**no propagate qos from l2tp**

### Purpose

For Layer 2 Tunneling Protocol (L2TP) packets coming into the SmartEdge router when it is configured as an L2TP network server (LNS), propagates the IP Differentiated Services Code Point (DSCP) bits from outer L2TP IP packet headers to the IP DSCP bits in inner subscriber IP packet headers.

### Command Mode

L2TP peer configuration (default peer only)

### Syntax Description

This command has no keywords or arguments.

### Default

The IP DSCP bits in the incoming L2TP IP packet headers are not propagated to the IP DSCP bits in subscriber IP packet headers.

### Usage Guidelines

Use the **propagate qos from l2tp** command to propagate the IP DSCP bits from outer L2TP IP packet headers to IP DSCP bits in inner subscriber IP packet headers.

**Note** This propagation occurs only in the upstream direction; this command applies only to a SmartEdge router that is configured as an LNS as it receives packets from an L2TP access concentrator (LAC).

L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber-based IP traffic encapsulated in Point-to-Point (PPP) sessions between routers. The LNS is the IP termination point for subscriber traffic, and as such, IP DSCP bits from the L2TP IP packet header can be propagated into subscriber traffic.

Use the **no** form of this command to disable the propagation of IP DSCP bits.

### Examples

The following example propagates IP DSCP bits from outer L2TP IP packet headers to IP DSCP bits in inner subscriber IP packet headers:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos from l2tp
```

### Related Commands

**propagate qos from subscriber**  
**propagate qos to l2tp**



# propagate qos from-mpls

**propagate qos from-mpls**

**no propagate qos from-mpls**

## Purpose

For outgoing packets, enables the mapping of Multiprotocol Label Switching (MPLS) experimental (EXP) bits to IP Differentiated Services Code Point (DSCP) bits.

## Command Mode

MPLS router configuration

## Syntax Description

This command has no keywords or arguments.

## Default

MPLS EXP bits are not mapped to IP DSCP bits.

## Usage Guidelines

Use the **propagate qos from-mpls** command to enable the mapping of MPLS EXP bits to IP DSCP bits for outgoing packets.

Use the **no** form of this command to disable the mapping of MPLS EXP bits to IP DSCP bits.

## Examples

The following example enables the mapping of MPLS EXP bits to IP DSCP bits for outgoing packets:

```
[local]Redback(config-ctx)#router mpls 234  
[local]Redback(config-mpls)#propagate qos from-mpls
```

## Related Commands

**egress prefer dscp-qos**  
**propagate qos to-mpls**

## propagate qos from subscriber

**propagate qos from subscriber** [upstream | downstream]

**no propagate qos from subscriber** [upstream | downstream]

### Purpose

For packets coming into the SmartEdge router when it is configured as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC), propagates the IP Differentiated Services Code Point (DSCP) bits in inner subscriber IP packet headers to the IP DSCP bits in outer L2TP IP packet headers.

### Command Mode

L2TP peer configuration (default peer only)

### Syntax Description

|                   |                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------|
| <b>upstream</b>   | Optional. Performs the propagation on inbound packets from the subscriber.                |
| <b>downstream</b> | Optional. Performs the propagation on inbound packets from the L2TP network server (LNS). |

### Default

IP DSCP bits are propagated in both directions.

### Usage Guidelines

Use the **propagate qos from subscriber** command for packets coming into the SmartEdge router when it is configured as a LAC, to propagate the IP DSCP bits in inner subscriber IP packet headers to the IP DSCP bits in outer L2TP IP packet headers.

Use the **upstream** keyword to perform the propagation from inbound packets from the subscriber. Use the **downstream** keyword to perform the propagation from inbound packets from the network.

The SmartEdge OS performs a deep packet inspection of inner subscriber IP packet headers and copies the IP DSCP bits in the IP header.

L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber-based Point-to-Point Protocol (PPP) sessions between routers. On L2TP tunnels, subscriber IP packets are encapsulated in PPP packets, which themselves are encapsulated in L2TP packets. IP DSCP bits can be propagated from inner subscriber IP packet headers to outer L2TP IP packet headers, and vice versa. IP DSCP bits are propagated between layers of encapsulated packets so that any Layer 3 device located between an L2TP network server (LNS) and a LAC can recognize and apply IP DSCP settings.

Use the **no** form of this command to disable the propagation of IP DSCP bits in the specified direction or, if neither keyword is specified, in both directions.

## Examples

The following example propagates the IP DSCP bits from subscriber IP packet headers to IP DSCP bits in the L2TP IP packet headers in the upstream direction only:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos from subscriber upstream
```

The following example propagates the IP DSCP bits from subscriber IP packet headers to IP DSCP bits in L2TP IP packet headers in both directions:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos from subscriber
```

## Related Commands

```
propagate qos from l2tp
propagate qos to l2tp
```

## propagate qos to ethernet

**propagate qos to ethernet**

**no propagate qos to ethernet**

### Purpose

For packets going out of the SmartEdge router, propagates IP Differentiated Services Code Point (DSCP) bits to Ethernet 802.1p user priority bits.

### Command Mode

dot1q profile configuration

### Syntax Description

This command has no keywords or arguments.

### Default

IP DSCP bits are not propagated to Ethernet 802.1p user priority bits.

### Usage Guidelines

Use the **propagate qos to ethernet** command to propagate IP DSCP bits from IP packets to Ethernet 802.1p user priority bits.

**Note** This command applies to outgoing packets transmitted over 802.1Q permanent virtual circuits (PVCs) that reference the dot1q profile.

Use the **no** form of this command to disable the propagation of IP DSCP bits.

### Examples

The following example propagates IP DSCP bits from IP packets to Ethernet 802.1p user priority bits for 802.1Q PVCs that reference the 802.1Q profile, 8021p-on:

```
[local]Redback(config)#dot1q profile 8021p-on  
[local]Redback(config-dot1q-profile)#propagate qos to ethernet
```

### Related Commands

**propagate qos from ethernet**

## propagate qos to l2tp

**propagate qos to l2tp**

**no propagate qos to l2tp**

### Purpose

For a SmartEdge router configured as a Layer 2 Tunneling Protocol (L2TP) network server (LNS), propagates the IP Differentiated Services Code Point (DSCP) bits from incoming network IP packet headers to the IP DSCP bits in L2TP IP packet headers.

For a SmartEdge router configured as an L2TP access concentrator (LAC), propagates the IP DSCP bits from incoming subscriber IP packet headers to the IP DSCP bits in L2TP IP packet headers.

### Command Mode

L2TP peer configuration (default peer only)

### Syntax Description

This command has no keyword or arguments.

### Default

IP DSCP bits are not propagated to L2TP IP packet headers.

### Usage Guidelines

For a SmartEdge router configured as an LNS, use the **propagate qos to l2tp** command to propagate the IP DSCP bits from incoming network IP packet headers to the IP DSCP bits in L2TP IP packet headers.

For a SmartEdge router configured as an LAC, use the **propagate qos to l2tp** command to propagate the IP DSCP bits from incoming subscriber IP packet headers to the IP DSCP bits in L2TP IP packet headers.

L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber-based Point-to-Point (PPP) sessions between routers. On L2TP tunnels, subscriber IP packets are encapsulated in PPP packets, which themselves are encapsulated in L2TP packets. IP DSCP bits are propagated between layers of encapsulated packets so that any Layer 3 device located between an LNS and a LAC can recognize and apply IP DSCP settings.

Use the **no** form of this command to disable the propagation of IP DSCP bits.

### Examples

The following example propagates IP DSCP bits from incoming network or subscriber IP packet headers to L2TP IP packet headers:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos to l2tp
```

## Related Commands

`propagate qos from l2tp`  
`propagate qos from subscriber`

# propagate qos to-mpls

**propagate qos to-mpls**

**no propagate qos to-mpls**

## Purpose

For incoming packets, enables the mapping of the IP Differentiated Services Code Point (DSCP) bits to the Multiprotocol Label Switching (MPLS) experimental (EXP) bits.

## Command Mode

MPLS router configuration

## Syntax Description

This command has no keywords or arguments.

## Default

IP DSCP bits are mapped to the MPLS EXP bits.

## Usage Guidelines

Use the **propagate qos to-mpls** command to enable the mapping of IP DSCP bits to MPLS EXP bits for incoming packets.

Use the **no** form of this command to disable the mapping of IP DSCP bits to MPLS EXP bits.

**Note** The default behavior of the SmartEdge router is to map IP DSCP bits to MPLS EXP bits for incoming traffic; only use the **propagate qos to-mpls** command to return the router to its default behavior after it has been changed by the **no** form of this command.

## Examples

The following example enables the mapping of the IP DSCP bits to the MPLS EXP bits at the ingress router:

```
[local]Redback(config-ctx)#router mpls 234  
[local]Redback(config-mpls)#propagate qos to-mpls
```

## Related Commands

**egress prefer dscp-qos**  
**propagate qos from ethernet**  
**propagate qos to ethernet**

## qos hierarchical mode

**qos hierarchical mode** [strict | wrr]  
{no | default} **qos hierarchical mode**

### Purpose

Specifies the quality of service (QoS) scheduling algorithm for the traffic-managed port, or the 802.1Q tunnel, 802.1Q permanent virtual circuit (PVC), hierarchical node group, or hierarchical node on a traffic-managed port.

### Command Mode

dot1q PVC configuration  
hierarchical node configuration  
hierarchical node group configuration  
port configuration

### Syntax Description

|               |                                                                                |
|---------------|--------------------------------------------------------------------------------|
| <b>strict</b> | Optional. Specifies strict priority scheduling algorithm; this is the default. |
| <b>wrr</b>    | Optional. Specifies weighted round-robin (WRR) scheduling algorithm.           |

### Default

Only traffic-managed ports are hierarchical nodes.

### Usage Guidelines

Use the **qos hierarchical mode** command to specify the QoS scheduling algorithm for the traffic-managed port, or a 802.1Q tunnel, 802.1Q PVC, hierarchical node group, or hierarchical node on a traffic-managed port. If you have not already entered the **qos rate** command (in port or dot1q PVC configuration mode) for this tunnel or PVC, this command also makes the tunnel or PVC a node in the hierarchy. A traffic-managed port is always a node at the top of the hierarchy.

**Note** The term, traffic-managed port, refers to a port on a Gigabit Ethernet 3 (GE3) or Gigabit Ethernet 1020 (GE1020) traffic card.

The scheduling algorithms service the QoS queues defined by the priority weighted fair queuing (PWFQ) policy attached to the port, 802.1Q tunnel, or 802.1Q PVC according to the priority (for the strict priority algorithm) and the relative weight (for the WRR algorithm) assigned to each queue with the **queue priority** command (in PWFQ policy configuration mode). The priority determines the servicing order and the relative weight determines the amount of traffic that will be transmitted.

You can specify a different scheduling mode for each tunnel and PVC configured on the port. If you do not enter this command for an 802.1Q tunnel or PVC, the tunnel or PVC is not part of the hierarchy; in this case, a tunnel inherits only the PWFQ policy attached to its port and a PVC inherits the policy attached to its tunnel.



Use the **no** or **default** form of this command to remove the tunnel or PVC from the hierarchy; only the port continues to be a hierarchical node. If you remove the tunnel or PVC from the hierarchy, any QoS policy attached to that tunnel or PVC is removed from the configuration for that tunnel or PVC.

## Examples

The following example specifies the WRR scheduling algorithm for a GE3 port:

```
[local]Redback(config)#port ethernet 1/1  
[local]Redback(config-port)#qos hierarchical mode wrr
```

## Related Commands

**qos policy pwfq**  
**qos rate**  
**queue priority**

## qos mode

**qos mode** {**alternate** | **normal** | **strict**}

{**no** | **default**} **qos mode**

### Purpose

Defines the mode of the quality of service (QoS) enhanced deficit round-robin (EDRR) policy algorithm.

### Command Mode

ATM OC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
link group configuration  
port configuration

### Syntax Description

|                  |                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>alternate</b> | Indicates that in every other round, either queue 0 or one of the other queues configured on the port is serviced, in alternating fashion.                                                                  |
| <b>normal</b>    | Indicates that queue 0 is treated like all other queues on the port. Each queue receives its share of the port's bandwidth according to the configured weights. This is the default mode for EDRR policies. |
| <b>strict</b>    | Indicates that queue 0 has strict priority over all other queues configured on the port.                                                                                                                    |

### Default

The mode is normal.

### Usage Guidelines

Use the **qos mode** command to define the mode of the EDRR policy algorithm.

**Note** Only one EDRR mode type can be supported on a single port.

Use the **no** or **default** form of this command to return EDRR queuing to normal mode.

## Examples

The following example configures a **strict** mode for each configured port on the Ethernet traffic card in slot 4:

```
[local]Redback(config)#qos policy qos-edrr-test edrr
[local]Redback(config-policy-edrr)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos mode strict
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 4/2
[local]Redback(config-port)#qos mode strict
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 4/3
[local]Redback(config-port)#qos mode strict
```

## Related Commands

**qos policy edrr**

## qos node

**qos node** *node-name idx-start* [**through** *idx-end*]

**no qos node** *node-name*

### Purpose

Creates one or more quality of service (QoS) hierarchical nodes as aggregation points for applying traffic shaping and accesses hierarchical node configuration mode.

### Command Mode

hierarchical node group configuration

### Syntax Description

|                               |                               |
|-------------------------------|-------------------------------|
| <i>node-name</i>              | Name of the node.             |
| <i>idx-start</i>              | Initial index number.         |
| <b>through</b> <i>idx-end</i> | Optional. Final index number. |

### Default

No nodes are created.

### Usage Guidelines

Use the **qos node** command to create one or more QoS hierarchical nodes as aggregation points for applying traffic shaping and access hierarchical node configuration mode.

**Note** This command is available only for traffic-managed ports.

**Note** The command prompt for the hierarchical node configuration mode is identical to the prompt for the hierarchical node group configuration mode; see the example in the “Examples” section.

Each node is uniquely referenced by its name, its node index, its node group, and the index for the node group.

Use the **no** form of this command to delete one or more nodes from the configuration.

### Examples

The following example creates 10 hierarchical node groups and 50 hierarchical nodes, with 5 nodes in each node group; the name of each node group is home and the name of each node is dslam:

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#qos node-group home 1 through 10
[local]Redback(config-h-node)#qos node dslam 1 through 5
[local]Redback(config-h-node)#
```

## Related Commands

`qos node-group`  
`qos node-reference`  
`qos policy queuing`

## qos node-group

**qos node-group** *group-name idx-start [through idx-end]*

**no qos node-group** *group-name*

### Purpose

Creates one or more quality of service (QoS) hierarchical node groups as aggregation points for applying traffic shaping and accesses hierarchical node group configuration mode.

### Command Mode

port configuration

### Syntax Description

|                               |                               |
|-------------------------------|-------------------------------|
| <i>group-name</i>             | Name of the node groups.      |
| <i>idx-start</i>              | Initial index number.         |
| <b>through</b> <i>idx-end</i> | Optional. Final index number. |

### Default

No node groups are created.

### Usage Guidelines

Use the **qos node-group** command to create one or more QoS hierarchical node groups as aggregation points for applying traffic shaping and accesses hierarchical node group configuration mode. This command is available only for traffic-managed ports.

Each node group is uniquely referenced by its name and its index.

Use the **no** form of this command to delete the node group from the configuration.

### Examples

The following example creates 10 hierarchical node groups; the name of each group is home:

```
[local]Redback(config)#port ethernet 5/1  
[local]Redback(config-port)#qos node-group home 1 through 10  
[local]Redback(config-h-node)#
```

### Related Commands

**qos node**

## qos node-reference

**qos node-reference** *node-name node-idx group-name group-idx*

**no qos node-reference** *node-name*

### Purpose

Creates a reference to a quality of service (QoS) hierarchical node in the subscriber record, named subscriber profile, or default subscriber profile.

### Command Mode

subscriber configuration

### Syntax Description

|                   |                          |
|-------------------|--------------------------|
| <i>node-name</i>  | Name of the node.        |
| <i>node-idx</i>   | Node index number.       |
| <i>group-name</i> | Name of the node group.  |
| <i>group-idx</i>  | Node group index number. |

### Default

No node references are created in any subscriber record, named subscriber profile, or default subscriber profile.

### Usage Guidelines

Use the **qos node-reference** command to create a reference to a QoS hierarchical node in the subscriber record, named subscriber profile, or default subscriber profile.

Use the **no** form of this command to delete the reference from the subscriber record, named subscriber profile, or default subscriber profile.

### Examples

The following example creates a reference to the hierarchical node group, home, with index 1, in which was created the node, dslam, with index 5, in the subscriber record, joe:

```
[local]Redback(config)#context subs
[local]Redback(config-ctx)#subscriber joe
[local]Redback(config-sub)#qos node-reference home 1 dslam 5
```

### Related Commands

**qos node**  
**qos node-group**

## qos policy metering

**qos policy metering** *pol-name* [**acl-counters**]

**no qos policy metering** *pol-name*

### Purpose

Attaches a metering policy to outgoing packets on the specified circuit, port, or subscriber record.

### Command Mode

ATM DS-3 configuration  
ATM OC configuration  
ATM PVC configuration  
dot1q PVC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
Frame Relay PVC configuration  
link group configuration  
port configuration  
subscriber configuration

### Syntax Description

|                     |                                                                                                                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>pol-name</i>     | Name of the metering policy to be attached.                                                                                                                                            |
| <b>acl-counters</b> | Optional. Enables per-rule access control list (ACL) statistics for a policy ACL associated with the policy. Available in all listed configuration modes, except global configuration. |

### Default

No metering policy is attached to outgoing packets on the circuit, port, or subscriber record.

### Usage Guidelines

Use the **qos policy metering** command to attach a metering policy to outgoing packets on a circuit, port, or subscriber record.

Use this command in link group configuration mode to attach the policy to an Multilink Point-to-Point Protocol (MP) or Multilink Frame Relay (MFR) bundle; use it in port configuration mode to attach the policy to a constituent port in an Ethernet or 802.1Q link group.

**Note** You can attach any QoS policy to a port, whether the port is in a link group or not, as long as the policy is supported by that type of port. However, to preserve the operational characteristics of a link group, it is recommended that you attach the same set of policies (metering, policing, and scheduling) to every constituent port in the link group.



Use the **no** form of this command to remove a metering policy from outgoing packets on a circuit, port, or subscriber record.

## Examples

The following example creates the metering policy, `example2`, and attaches it to an Ethernet port:

```
[local]Redback(config)#qos policy example2 metering
[local]Redback(config-policy-metering)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-metering)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy metering example2
```

## Related Commands

**qos policy policing**

## qos policy policing

**qos policy policing** *pol-name* [**acl-counters**]

**no qos policy policing** *pol-name*

### Purpose

Attaches a policing policy to the incoming packets on the specified circuit, port, or subscriber record.

### Command Mode

ATM DS-3 configuration  
ATM OC configuration  
ATM PVC configuration  
dot1q PVC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
Frame Relay PVC configuration  
link group configuration  
port configuration  
subscriber configuration

### Syntax Description

|                     |                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>pol-name</i>     | Name of the policing policy to be attached.                                                                                                                                     |
| <b>acl-counters</b> | Optional. Enables per-rule access control list (ACL) statistics for a policy ACL associated with the policy. Available in all configuration modes, except global configuration. |

### Default

No policing policy is created or attached to incoming packets on the circuit, port, or subscriber record.

### Usage Guidelines

Use the **qos policy policing** command to attach a policing policy to outgoing packets on a circuit, port, or subscriber record.

Use this command in link group configuration mode to attach the policy to an Multilink Point-to-Point Protocol (MP) or Multilink Frame Relay (MFR) bundle; use it in port configuration mode to attach the policy to an Ethernet or 802.1Q link group.

Use the **no** form of this command to remove a policing policy from outgoing packets on a circuit, port, or subscriber record.

## Examples

The following example creates the `example2` policing policy and attaches it to an Ethernet port:

```
[local]Redback(config)#qos policy example2 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy policing example2
```

The following example attaches the `WholePort` policing policy to a Gigabit Ethernet port, and then attaches the `OneVC` policing policy to one of the 802.1Q PVCs. The policy attached to the PVC supersedes the policy attached to the port. For all the other PVCs on the port, the policy attached to the port takes effect.

```
[local]Redback(config)#qos policy OneVC policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark dscp ef
[local]Redback(config-policy-rate)#exceed mark dscp df
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#qos policy WholePort policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#qos policy policing WholePort
[local]Redback(config-port)#dot1q pvc 100
[local]Redback(config-dot1q-pvc)#bind interface if_100 local
[local]Redback(config-dot1q-pvc)#qos policy policing OneVC
```

## Related Commands

**qos policy metering**

## qos policy queuing

**qos policy queuing** *pol-name*

**no qos policy queuing** *pol-name*

### Purpose

Attaches a quality of service (QoS) scheduling policy to the port, circuit, hierarchical node, or subscriber record.

### Command Mode

ATM DS-3 configuration  
ATM OC configuration  
ATM PVC configuration  
dot1q PVC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
Frame Relay PVC configuration  
hierarchical node configuration  
link group configuration  
port configuration  
subscriber configuration

### Syntax Description

*pol-name*                      Name of the scheduling policy to be attached.

### Default

No queuing policy is not attached to the circuit or port.

### Usage Guidelines

Use the **qos policy queuing** command to attach a QoS scheduling policy to the port, circuit, hierarchical node, or subscriber record.

The specified QoS scheduling policy must already exist. The types of scheduling policies are Asynchronous Transfer Mode weighted fair queuing (ATMWFQ), enhanced deficit round robin (EDRR), priority queuing (PQ), and priority weighted fair queuing (PWFQ).

Use this command in link group configuration mode to attach the policy to an Multilink Point-to-Point Protocol (MP) or Multilink Frame Relay (MFR) bundle; use it in port configuration mode to attach the policy to an Ethernet or 802.1Q link group.

**Note** QoS scheduling policies are not supported on virtual LAN (VLAN) bridge circuits and Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) circuits.

**Note** ATMWFQ policies are applicable only to ATM PVCs (not ports) on ATM DS-3 and second-generation ATM OC traffic cards. However, an ATMWFQ policy cannot be attached to a PVC that is shaped as unspecified bit rate extended (UBRe).



**Caution** Risk of data loss. Modifying the parameters of an ATMWFQ policy will momentarily interrupt the traffic on all ATM PVCs using the policy. To reduce the risk, modify an ATMWFQ policy only when traffic is light.

**Note** PWFQ policies are supported only on traffic-managed ports, and the 802.1Q tunnels, 802.1Q PVCs, and hierarchical nodes configured on them. You can attach the same PWFQ policy to a port, its 802.1Q tunnels, its PVCs, and its hierarchical nodes; similarly, you can attach different PWFQ policies to a port, its tunnels, PVCs and hierarchical nodes. For examples, see the “Examples” section.

The term, traffic-managed port, refers to a port on a Gigabit Ethernet 3 (GE3) or Gigabit Ethernet 1020 (GE1020) traffic card.

**Note** Layer 2 Tunneling Protocol (L2TP) network server (LNS) subscriber sessions support only PWFQ policies; an LNS subscriber session initiated on any type of port except a traffic-managed port will not be governed by the PWFQ policy attached to the subscriber record.

Slot redundancy is not supported; if an LNS subscriber session moves to a traffic-managed port in a different slot, it will no longer be governed by the PWFQ policy attached to the LNS subscriber session. If the session moves to a different port in the same slot, the PWFQ policy will resume queuing after a temporary traffic disruption.

**Note** For first-generation ATM OC traffic cards, you can attach EDRR or PQ policies to both ATM ports and ATM PVCs. PQ and EDRR policies are not supported on second-generation ATM OC or ATM DS-3 traffic cards.

**Note** You can attach only one type of queuing policy to ports and circuits on a single traffic card. That is, you can attach either ATMWFQ, EDRR, PQ, or PWFQ policies, but not any combination of these types. You can, however, attach several queuing policies of the same type to ports, subscribers, and circuits on a single traffic card.

**Note** To attach an EDRR policy to a circuit, you must also attach the policy at the port level. The limit on attaching different EDRR policies to ports and circuits on a single traffic card is 15.

Use the **no** form of this command to remove a QoS scheduling policy from the port, circuit, hierarchical node, or subscriber record.

## Examples

The following example creates a PQ policy and then attaches the policy to a GE3 port:

```
[local]Redback(config)#qos policy example1 pq
[local]Redback(config-policy-pq)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy queuing example1
```

The following example attaches two PWFQ policies, pwfq1 and pwfq2, to a GE3 port, an 802.1Q tunnel on that port, and an 802.1Q PVC within that tunnel:

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#qos policy queuing pwfq1
[local]Redback(config-port)#dot1q pvc 10 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#qos policy queuing pwfq1
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 10:20
[local]Redback(config-dot1q-pvc)#qos policy queuing pwfq2
[local]Redback(config-dot1q-pvc)#exit
```

## Related Commands

- qos policy atmwfq**
- qos policy edrr**
- qos policy pq**
- qos policy pwfq**

## qos priority

**qos priority** *group-num*

**no qos priority** *group-num*

### Purpose

Classifies all traffic, including non-IP traffic, on the ingress circuit with a quality of service (QoS) priority group number.

### Command Mode

ATM DS-3 configuration  
ATM OC configuration  
ATM PVC configuration  
dot1q PVC configuration  
DS-0 group configuration  
DS-1 configuration  
DS-3 configuration  
E1 configuration  
E3 configuration  
Frame Relay PVC configuration  
link group configuration  
port configuration

### Syntax Description

*group-num*                      Priority group number. The range of values is 0 to 7.

### Default

By default, no QoS priority is configured and no priority group is assigned to any traffic.

### Usage Guidelines

Use the **qos priority** command to classify all traffic, including non-IP traffic, on the ingress circuit with a QoS priority group number.

A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, IP Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not changed by this command. The actual queue number depends upon the number of queues configured on the circuit; see the **num-queues** command.

**Note** If a QoS policy is applied to the same traffic assigned to a QoS priority group, the QoS policy overrides the **qos priority** command.

Use the **no** form of this command to remove a QoS priority configuration and to stop assigning traffic to the priority group.

### Examples

The following example configures a priority of 2 to port 1 on the Ethernet traffic card in slot 13:

```
[local]Redback(config)#port ethernet 13/1  
[local]Redback(config-port)#no shutdown  
[local]Redback(config-port)#bind interface eth-pc05 local  
[local]Redback(config-port)#qos priority 2
```

### Related Commands

**num-queues**  
**qos queue-map**



## qos rate

For traffic-managed ports, or the 802.1Q tunnels or permanent virtual circuits (PVCs) configured on them, the syntax is:

```
qos rate {maximum | minimum} kbps
```

```
no qos rate {maximum | minimum}
```

For all other Gigabit Ethernet ports, the syntax is:

```
qos rate maximum mbps burst bytes
```

```
no qos rate maximum
```

### Purpose

Sets the rate for outgoing traffic on a Gigabit Ethernet port, or on an 802.1Q tunnel, 802.1Q PVC, or hierarchical node group or node configured on a traffic-managed port.

### Command Mode

dot1q PVC configuration  
hierarchical node configuration  
hierarchical node group configuration  
port configuration

### Syntax Description

|                           |                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>maximum</b>            | Specifies the maximum rate for the port, tunnel, PVC, or hierarchical node group, or hierarchical node.                                                                                         |
| <b>minimum</b>            | Specifies the minimum rate for the port; available only for traffic-managed ports and the 802.1Q tunnels, PVCs, and hierarchical node groups, and hierarchical nodes configured on them.        |
| <i>kbps</i>               | Rate in Kbps for traffic-managed ports, tunnels, PVCs, and hierarchical node groups; the range of values is 64 to 1,000,000.                                                                    |
| <i>mbps</i>               | Rate in Mbps for all other Gigabit Ethernet ports. The range of values is 100 to 1,000; the default value is 1,000 (the full speed of the port).                                                |
| <b>burst</b> <i>bytes</i> | Burst tolerance in bytes. For all other Gigabit Ethernet ports except traffic-managed ports, the range of values is 1 to 12,000,000. This construct is not available for traffic-managed ports. |

### Default

Outgoing traffic is transmitted at the full speed of the port.

### Usage Guidelines

Use the **qos rate** command to set the maximum rate for outgoing traffic on a Gigabit Ethernet port, or an 802.1Q tunnel, 802.1Q PVC, or hierarchical node group or node configured on a traffic-managed port. You can set the burst for any Gigabit Ethernet port, except for a traffic-managed port.

If you have not already entered the **qos hierarchical mode** command (in port or dot1q PVC configuration mode) for this tunnel or PVC, this command also makes the tunnel or PVC a node in the hierarchy. A Gigabit Ethernet 3 port is always a node at the top of the hierarchy.

**Note** The maximum rate set by this command is the rate at which the port operates; any priority queuing (PQ), enhanced deficit round-robin (EDRR), or priority weighted fair queuing (PWFQ) queue or circuit with a PQ, EDRR, or PWFQ policy is limited by the rate specified by this command for the circuit. Also, the sum of all traffic on the port carried by the queues belonging to the circuits or subscribers is limited to the rate specified by this command.

Use the **no** form of this command to set the port, tunnel, or PVC to the default port rate.

### Examples

The following example sets the maximum rate for outgoing traffic for port 1 on the Gigabit Ethernet traffic card in slot 14 to 600 Mbps with a burst size of 1,000 bytes:

```
[local]Redback(config)#port ethernet 14/1  
[local]Redback(config-port)#qos rate maximum 600 burst 1000
```

### Related Commands

**qos hierarchical mode**  
**qos weight**  
**rate**

## qos weight

**qos weight** *weight*

**no qos weight** *weight*

### Purpose

Assigns to this circuit a relative weight that is used to calculate a traffic ratio for all circuits configured on a traffic-managed port.

### Command Mode

dot1q PVC configuration  
hierarchical node configuration  
hierarchical node group configuration

### Syntax Description

*weight*                      Relative weight that is assigned to this circuit. The range of values is 5 to 100.

### Default

All circuits configured on this port have the same weight.

### Usage Guidelines

Use the **qos weight** command to assign to this circuit a relative weight that is used to calculate a traffic ratio for all circuits configured on a traffic-managed port.

You can assign a relative weight, or you can set a minimum absolute rate, for the circuit, using the **qos rate** command (in dot1q PVC, hierarchical node, or hierarchical node group configuration mode), but you cannot do both; the relative weight and minimum absolute rate are mutually exclusive.

You can assign a relative weight (using this command) and set a maximum absolute rate for the circuit, using the **qos rate** command (in dot1q PVC, hierarchical node, or hierarchical node group configuration mode).

Use the **no** form of this command to specify the default condition.

### Examples

The following example specifies a weight of 3 for the hierarchical nodes `dslam 1` through `dslam 5`:

```
[local]Redback(config)#port ethernet 5/2
[local]Redback(config-port)#qos rate maximum 100000000
[local]Redback(config-port)#qos node-group home 1
[local]Redback(config-h-node)#qos hierarchical mode wrr
[local]Redback(config-h-node)#qos node dslam 1 through 5
[local]Redback(config-h-node)#qos weight 3
```

Related Commands

qos rate  
weight

# Security

---

This part describes the tasks and commands used to configure security features, including authentication, authorization, and accounting (AAA), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), key chains, and lawful intercept (LI). It consists of the following chapters:

- Chapter 15, “AAA Configuration”
- Chapter 16, “RADIUS Configuration”
- Chapter 17, “TACACS+ Configuration”
- Chapter 18, “Key Chain Configuration”
- Chapter 19, “Lawful Intercept Configuration”



# AAA Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS authentication, authorization, and accounting (AAA) features.

For information about the commands used to monitor, troubleshoot, and administer AAA, see the “AAA Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

**Note** In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted. The XCRP Controller card includes 768 MB of main memory; the XCRP3 Controller card can have either 768 or 1,280 MB of main memory. The term, Base, refers to a XCRP3 controller card with 768 MB of memory.

## Overview

---

SmartEdge OS AAA features are described in the following sections:

- Authentication
- Authorization and Reauthorization
- Accounting

## Authentication

Authentication features are described in the following sections:

- Administrators
- Subscribers

### Administrators

By default, the SmartEdge OS configuration performs administrator authentication. You can also authenticate administrators through database records on a Remote Authentication Dial-In User Service (RADIUS) server, through a Terminal Access Controller Access Control System Plus (TACACS+) server, or through one method, followed by another.

You must configure the IP address of a reachable RADIUS or TACACS+ server (or both) in the context in which the administrator is configured. For information about RADIUS and TACACS+, see Chapter 16, “RADIUS Configuration,” and Chapter 17, “TACACS+ Configuration,” respectively.

You can set a maximum limit on the number of administrator sessions that can be simultaneously active in each context.

### Subscribers

Subscriber authentication is described in the following sections:

- Authentication Options
- Maximum Subscriber Sessions
- Limit Subscriber Services
- Binding Order
- IP Address Assignment

#### Authentication Options

By default, the SmartEdge OS configuration performs subscriber authentication. You can also authenticate subscribers through database records on a RADIUS server, or through one method, followed by another.

When the IP address or hostname of the RADIUS server is configured in the SmartEdge OS “local” context, “global RADIUS” authentication is performed. That is, although subscribers may be configured in a nonlocal context, subscribers in nonlocal contexts are authenticated through the RADIUS server configured in the local context. With global RADIUS authentication, the RADIUS server returns the Context-Name vendor-specific attribute (VSA) indicating the name of the particular context to which subscribers are to be bound.

When the IP address or hostname of the RADIUS server is configured in a context other than the local context, “context-specific” RADIUS authentication is performed; that is, only subscribers bound to the context in which the RADIUS server’s IP address or hostname is configured are authenticated.

You can also configure the SmartEdge OS to try authentication through a RADIUS server configured in the nonlocal context first, with a fallback to a RADIUS server configured in the local context, in case the first server becomes unavailable. Or, you can configure the SmartEdge OS to try authentication through a RADIUS server configured in a nonlocal context, with a fallback to the SmartEdge OS configuration.

#### Maximum Subscriber Sessions

You can set a maximum limit on the number of subscriber sessions that can be simultaneously active within a given context and for all configured contexts.



## Limit Subscriber Services

You can limit the services provided to subscribers based on volume (amount of traffic in Kbytes). You can monitor volume-based services in the upstream and downstream directions independently and separately; you can also monitor the aggregated traffic in both directions. Volume limits are imposed by the RADIUS VSA 113 in Access-Accept and Accounting-Request messages.

This attribute implements the following features:

- Both in and out counters for incoming (upstream) and outgoing (downstream) traffic, in Kbytes are supported.
- If the attribute does not include the direction to which the limit is applied, the downstream direction is assumed.
- If no limit is included, the traffic volume is unlimited in both directions and is not monitored.
- A limit of “0” in either direction, is treated as unlimited in that direction and is not monitored.
- VSA 113 is also supported in a subscriber reauthorize Access-Accept message.

## Binding Order

If a subscriber circuit has been configured with a dynamic binding, using the **bind authentication** command (in the circuit’s configuration mode), AAA makes use of the subscriber attributes in messages received during subscriber authentication to determine which IP address (and the associated interface) to use when binding the subscriber circuit.

By default, the SmartEdge OS considers Layer 2 Tunneling Protocol (L2TP) attributes before considering RADIUS attributes. You can reverse this order so that the IP address provided in the RADIUS record is used in preference to one provided by L2TP.

## IP Address Assignment

AAA typically assigns an IP address to a Point-to-Point Protocol (PPP) subscriber from an IP pool after receiving an Access-Accept packet from a RADIUS server. However, you can configure AAA to provide an IP address from an IP pool in the Framed-IP-Address attribute in the RADIUS Access-Request packet. This IP address is provided to the RADIUS server as a “hint” that it is a preferred address. If there are no unassigned IP addresses in the pool, the authentication request is sent without an IP address

The RADIUS server can choose to accept the address or not; Table 15-1 lists the various responses that the RADIUS server can make and the corresponding action that the SmartEdge OS performs.

**Table 15-1 SmartEdge OS and RADIUS Server Actions**

| RADIUS Server Response                                                        | SmartEdge Router Corresponding Action                                                                                    |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Framed-IP-Address attribute contains 255.255.255.254, 0.0.0.0, or is missing. | SmartEdge OS assigns preferred IP address.                                                                               |
| Framed-IP-Address attribute contains a different IP address.                  | SmartEdge OS assigns the IP address in the Framed-IP-Address attribute and returns the preferred IP address to its pool. |

## Authorization and Reauthorization

Authorization and reauthorization features are described in the following sections:

- CLI Commands Authorization
- Dynamic Subscriber Reauthorization

### CLI Commands Authorization

You can specify that commands with a matching privilege level (or higher) require authorization through TACACS+.

### Dynamic Subscriber Reauthorization

When subscribers request new or modified services during active sessions, the requests can be translated to changes that are applied during the active session through dynamic subscriber reauthorization. Reauthentication occurs without the requirement of PPP renegotiation and without interrupting or dropping the active session.

## Accounting

Accounting features are described in the following sections:

- CLI Commands Accounting
- Administrator Accounting
- Subscriber Accounting
- L2TP Accounting

### CLI Commands Accounting

You can configure the SmartEdge OS so that accounting messages are sent to a TACACS+ server whenever an administrator enters commands at the specified privilege level (or higher).

### Administrator Accounting

You can configure administrator accounting, which tracks messages for administrator sessions; the messages are sent to a TACACS+ server.

### Subscriber Accounting

You can configure subscriber accounting, which tracks messages for subscriber sessions; the messages are sent to a RADIUS accounting server. When the IP address or hostname of the RADIUS accounting server is configured in the SmartEdge OS local context, global authentication is performed. That is, although subscribers are configured in a nonlocal context, accounting messages for subscribers sessions in the context are sent through the RADIUS accounting server configured in the local context. With global accounting, the RADIUS accounting server is expected to return the Context-Name VSA that indicates the name of the particular context to which a subscriber is to be bound. When using global RADIUS subscriber accounting, global RADIUS subscriber authentication must be configured.

When the IP address or hostname of the RADIUS accounting server is configured in a context other than the local context, context-specific accounting is performed; that is, accounting messages are sent for only subscribers bound to the context in which the RADIUS accounting server IP address or hostname is configured.

You can configure the SmartEdge OS to send accounting messages to a RADIUS accounting server configured in the nonlocal context and to a RADIUS accounting server configured in the local context; this setup is called “two-stage accounting”.

For example, a copy of the accounting data can be sent to a wholesaler’s RADIUS accounting server and to an upstream service provider’s RADIUS accounting server, allowing end-of-period accounting data to be reconciled and validated by both parties.

You can also specify the error conditions for which the SmartEdge router will suppress the sending of accounting messages to a RADIUS accounting server.

## L2TP Accounting

You can configure L2TP accounting, which tracks messages for L2TP tunnels, or sessions in L2TP tunnels; the messages are sent to a RADIUS accounting server. When the IP address or hostname of the RADIUS accounting server is configured in the SmartEdge OS local context, global authentication is performed. When the IP address or hostname of the RADIUS accounting server is configured in a context other than the local context, context-specific accounting is performed. You can also configure two-stage accounting.

**Note** The SmartEdge OS attempts to send a single “accounting on” message when more than one type of RADIUS accounting is enabled. For example, if you enable both subscriber accounting and L2TP accounting, the SmartEdge OS sends a single “accounting on” message to each RADIUS accounting server, even if you enable L2TP accounting at a later time.

Similarly, the “accounting off” message is not sent until you have disabled all types of RADIUS accounting.

If a subscriber session cannot be tunneled to a specific L2TP network server (LNS) or to an LNS in a group of L2TP peers, or if the SmartEdge router has received a Link Control Protocol (LCP) termination request from the subscriber before session establishment is complete, the Acct-Session-Time attribute is set to 0.

# Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure AAA, perform the tasks described in the following sections:

- Configure Global AAA
- Configure Authentication
- Configure Authorization and Reauthorization
- Configure Accounting

## Configure Global AAA

To configure global attributes for AAA, perform the tasks in the following sections:

- Limit the Number of Active Administrator Sessions
- Limit the Number of Active Subscriber Sessions
- Enable a Direct Connection for Subscriber Circuits
- Define Structured Username Formats

### Limit the Number of Active Administrator Sessions

To limit the number of administrator sessions that can be simultaneously active in a given context, perform the task describer in Table 15-2.

**Table 15-2 Limit the Number of Active Administrator Sessions**

| Task                                                                                             | Root Command                            | Notes                                                                                                                      |
|--------------------------------------------------------------------------------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Limit the number of administrator sessions that can be simultaneously active in a given context. | <b>aaa authentication administrator</b> | Enter this command in context configuration mode.<br>To set the limit, use the <b>maximum sessions num-sess</b> construct. |

### Limit the Number of Active Subscriber Sessions

To limit the number of subscriber sessions that can be simultaneously active, perform the appropriate task (or tasks) described in Table 15-3.

**Table 15-3 Limit the Number of Active Subscriber Sessions**

| Task                                                                                            | Root Command                         | Notes                                             |
|-------------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------------|
| Limit the number of subscriber sessions that can be simultaneously active in the entire system. | <b>aaa global maximum subscriber</b> | Enter this command in global configuration mode.  |
| Limit the number of subscriber sessions that can be simultaneously active in a given context.   | <b>aaa maximum subscriber</b>        | Enter this command in context configuration mode. |

### Enable a Direct Connection for Subscriber Circuits

To enable a direct connection for subscriber circuits by enabling the SmartEdge OS to install the route specified by the RADIUS Framed-IP-Netmask attribute, perform the task described in Table 15-4.

**Table 15-4 Enable a Direct Connection for Subscriber Circuits**

| Task                                                                                          | Root Command               | Notes                                             |
|-----------------------------------------------------------------------------------------------|----------------------------|---------------------------------------------------|
| Enable use of the RADIUS Framed-IP-Netmask attribute to install the route to a remote router. | <b>aaa provision route</b> | Enter this command in context configuration mode. |

## Define Structured Username Formats

To define one or more schemas for matching the format of structured usernames (subscriber and administrator names), perform the task described in Table 15-5.

**Table 15-5 Define Structured Username Formats**

| Task                                                                        | Root Command               | Notes                                                                                                                                                                                     |
|-----------------------------------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Define one or more schemas for matching the format of structured usernames. | <b>aaa username-format</b> | Enter this command in global configuration mode.<br>If no username formats are explicitly defined, the SmartEdge OS checks the default format, <i>username@domain-name</i> , for a match. |

## Configure Authentication

To configure authentication, perform the tasks described in the following sections:

- Configure Administrator Authentication
- Configure Subscriber Authentication
- Disable Subscriber Authentication

### Configure Administrator Authentication

To configure administrator authentication, perform the task described in Table 15-6.

**Table 15-6 Configure Administrator Authentication**

| Task                                    | Root Command                            | Notes                                             |
|-----------------------------------------|-----------------------------------------|---------------------------------------------------|
| Configure administrator authentication. | <b>aaa authentication administrator</b> | Enter this command in context configuration mode. |

### Configure Subscriber Authentication

To configure subscriber authentication, perform the tasks described in the following sections:

- Enable the Assignment of Preferred IP Addresses
- Change the Default Order for Determining Subscriber IP Addresses
- Configure Global RADIUS Authentication
- Configure Context-Specific RADIUS Authentication
- Configure SmartEdge OS Configuration Authentication
- Configure Context-Specific RADIUS and Global RADIUS Authentication
- Configure Context-Specific RADIUS and SmartEdge OS Authentication
- Configure a Last-Resort Authentication Context

## Enable the Assignment of Preferred IP Addresses

To enable the SmartEdge OS to provide a RADIUS server with preferred IP addresses when performing subscriber authentication, perform the task described in Table 15-7.

**Table 15-7 Enable the Assignment of Preferred IP Addresses**

| Task                                                                                                    | Root Command               | Notes                                             |
|---------------------------------------------------------------------------------------------------------|----------------------------|---------------------------------------------------|
| Enable the SmartEdge OS to provide the RADIUS server with preferred IP addresses from unnamed IP pools. | <b>aaa hint ip-address</b> | Enter this command in context configuration mode. |

## Change the Default Order for Determining Subscriber IP Addresses

To change the default order for determining the IP address (and its interface) to be used for binding a subscriber circuit, perform the task in Table 15-8.

**Table 15-8 Change the Default Order for Determining Subscriber IP Addresses**

| Task                                                                                      | Root Command                       | Notes                                             |
|-------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------|
| Change the default order for determining the IP address for binding a subscriber circuit. | <b>aaa provision binding-order</b> | Enter this command in context configuration mode. |

## Configure Global RADIUS Authentication

To configure global RADIUS authentication, perform the tasks described in Table 15-9.

**Table 15-9 Configure Global RADIUS Authentication**

| #  | Task                                                                                                                                               | Root Command                                | Notes                                                                                                                                                                                                            |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Enable global RADIUS authentication.                                                                                                               | <b>aaa global authentication subscriber</b> | Enter this command in global configuration mode.<br><br>At least one RADIUS server IP address or hostname must be configured in the local context; see Chapter 16, "RADIUS Configuration," for more information. |
| 2. | Authenticate subscribers in the current context through one or more RADIUS servers with IP addresses or hostnames configured in the local context. | <b>aaa authentication subscriber</b>        | Enter this command in context configuration mode.<br><br>Use the <b>global</b> keyword with this command.                                                                                                        |

## Configure Context-Specific RADIUS Authentication

To authenticate subscribers using one or more RADIUS servers with IP addresses or hostnames configured in the current context, perform the task described in Table 15-10.

**Table 15-10 Configure Context-Specific RADIUS Authentication**

| Task                                              | Root Command                         | Notes                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure context-specific RADIUS authentication. | <b>aaa authentication subscriber</b> | Enter this command in context configuration mode.<br>Use the <b>radius</b> keyword with this command to configure RADIUS authentication.<br>At least one RADIUS server IP address or hostname must be configured in the current context; see Chapter 16, "RADIUS Configuration," for more information. |

## Configure SmartEdge OS Configuration Authentication

To authenticate subscribers through the SmartEdge OS configuration, perform the task described in Table 15-11.

**Table 15-11 Configure SmartEdge OS Configuration Authentication**

| Task                                                 | Root Command                         | Notes                                                                                                                                   |
|------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Configure SmartEdge OS configuration authentication. | <b>aaa authentication subscriber</b> | Enter this command in context configuration mode.<br>Use the <b>local</b> keyword with this command to configure RADIUS authentication. |

## Configure Context-Specific RADIUS and Global RADIUS Authentication

To configure context-specific RADIUS authentication, followed by global RADIUS authentication, perform the tasks described in Table 15-12.

**Table 15-12 Configure Context-Specific RADIUS and Global RADIUS Authentication**

| #  | Task                                                                        | Root Command                                | Notes                                                                                                                                                                                                        |
|----|-----------------------------------------------------------------------------|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Enable global RADIUS authentication.                                        | <b>aaa global authentication subscriber</b> | Enter this command in global configuration mode.<br>At least one RADIUS server IP address or hostname must be configured in the local context; see Chapter 16, "RADIUS Configuration," for more information. |
| 2. | Configure context-specific RADIUS followed by global RADIUS authentication. | <b>aaa authentication subscriber</b>        | Enter this command in context configuration mode.<br>Use the <b>radius global</b> construct with this command.                                                                                               |

## Configure Context-Specific RADIUS and SmartEdge OS Authentication

To authenticate subscribers using one or more RADIUS servers with IP addresses or hostnames configured in the current context, followed by the SmartEdge OS, perform the task described in Table 15-13.

**Table 15-13 Configure Context-Specific RADIUS and SmartEdge OS Authentication**

| Task                                                                                                     | Root Command                         | Notes                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure context-specific RADIUS authentication, followed by SmartEdge OS configuration authentication. | <b>aaa authentication subscriber</b> | Enter this command in context configuration mode.<br>Use the <b>radius</b> keyword followed by the <b>local</b> keyword with this command. At least one RADIUS server IP address or hostname must be configured in the current context; see Chapter 16, "RADIUS Configuration," for more information. |

## Configure a Last-Resort Authentication Context

To specify a context to attempt authentication of a subscriber when the domain portion of the subscriber name cannot be matched, perform the task described in Table 15-14.

**Table 15-14 Configure a Last-Resort Authentication Context**

| Task                                            | Root Command           | Notes                                            |
|-------------------------------------------------|------------------------|--------------------------------------------------|
| Configure a last-resort authentication context. | <b>aaa last-resort</b> | Enter this command in global configuration mode. |

## Disable Subscriber Authentication

To disable authentication of subscribers in the current context, perform the task described in Table 15-15.

**Table 15-15 Disable Subscriber Authentication**

| Task                               | Root Command                         | Notes                                                                                                                                                                                                                                                        |
|------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable subscriber authentication. | <b>aaa authentication subscriber</b> | Enter this command in context configuration mode. Use the <b>none</b> keyword with this command if subscriber authentication is not required, such as when Dynamic Host Configuration Protocol (DHCP) is used to obtain IP addresses for subscribers' hosts. |



**Caution** Risk of security breach. If you disable subscriber authentication, individual subscriber names and passwords will not be authenticated by the SmartEdge OS and therefore, IP routes and ARP entries within individual subscriber records are not installed. To reduce the risk, verify your network security setup before disabling subscriber authentication.

## Configure Authorization and Reauthorization

To configure authorization and reauthorization, perform the tasks described in the following sections:

- Configure CLI Commands Authorization
- Configure L2TP Peer Authorization
- Configure Dynamic Subscriber Reauthorization



## Configure CLI Commands Authorization

To specify that commands with a matching privilege level (or higher) require authorization through TACACS+, perform the task described in Table 15-16.

**Table 15-16 Configure CLI Commands Authorization**

| Task                                  | Root Command                      | Notes                                                                                                                                                                             |
|---------------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure CLI commands authorization. | <b>aaa authorization commands</b> | Enter this command in context configuration mode.<br>A TACACS+ server must be configured in the specified context; see Chapter 17, "TACACS+ Configuration," for more information. |

## Configure L2TP Peer Authorization

To determine whether L2TP peers are authorized by the SmartEdge OS configuration or by a RADIUS server, perform the task described in Table 15-17.

**Table 15-17 Configure L2TP Peer Authorization**

| Task                               | Root Command                    | Notes                                                                                                                              |
|------------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Configure L2TP peer authorization. | <b>aaa authorization tunnel</b> | Enter this command in context configuration mode.<br>By default, L2TP peers are authorized through the SmartEdge OS configuration. |

## Configure Dynamic Subscriber Reauthorization

To configure dynamic subscriber reauthorization, perform the task described in Table 15-18.

**Table 15-18 Configure Dynamic Subscriber Reauthorization**

| Task                                          | Root Command                    | Notes                                             |
|-----------------------------------------------|---------------------------------|---------------------------------------------------|
| Configure dynamic subscriber reauthorization. | <b>aaa reauthorization bulk</b> | Enter this command in context configuration mode. |

For reauthorization to take effect, Redback VSA 94, Reauth-String, must be configured on the RADIUS server. Redback VSA 95, Reauth-More, is only needed if multiple reauthorization records are used for one command; for example, if you have the following records, the **reauthorize bulk 1** command causes the RADIUS server to process reauthorization for reauth-1@local followed by reauth-2@local.

```
reauth-1@local
Password="redback"
Reauth-String="ID-type;subID;attr-num;attr-value;attr-num;attr-value..."
Reauth-More=1
```

```
reauth-2@local
Password="redback"
Reauth-String="ID-type;subID;attr-num;attr-value;attr-num;attr-value..."
```

```
Reauth_String
Attribute number: 94
Value: String
Format: "xxx"*
```

```
Send in Access-Request packet: No
Send in Accounting-Request packet: No
Receivable in Access-Request packet: Yes
Description: (SE)
* Format for Reauth String
"type;sub_id;attr#;attr_val;attr#;;attr#;attr_val;..."
(vsa_attr: vid-vsa_attr_#)
Reauth_More
Attribute number: 95
Value: integer
Format: 1
Send in Access-Request packet: No
Send in Accounting-Request packet: No
Receivable in Access-Request packet: Yes
Description: More reauth request is needed (SE)
```

For a list of the standard RADIUS attributes and vendor-specific attributes (VSAs) that are supported as part of the Reauth-String and details about them, see Appendix A, “RADIUS Attributes.”

Configure Accounting

To configure accounting, perform the tasks described in the following sections:

- Configure CLI Commands Accounting
- Configure Administrator Accounting
- Configure Subscriber Accounting
- Configure L2TP Accounting

Configure CLI Commands Accounting

To specify that accounting messages are sent to a TACACS+ server whenever an administrator enters commands at the specified privilege level (or higher), perform the task described in Table 15-19.

Table 15-19 Configure CLI Commands Accounting

| Task                               | Root Command                   | Notes                                                                                                                                                       |
|------------------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure CLI commands accounting. | <b>aaa accounting commands</b> | Enter this command in context configuration mode.<br>A TACACS+ server must be configured in the specified context; see Chapter 17, “TACACS+ Configuration.” |

## Configure Administrator Accounting

To enable accounting messages for administrator sessions to be sent to the TACACS+ server, perform the task described in Table 15-20.

**Table 15-20 Configure Administrator Accounting**

| Task                                | Root Command                        | Notes                                                                                                                                                       |
|-------------------------------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure administrator accounting. | <b>aaa accounting administrator</b> | Enter this command in context configuration mode.<br>A TACACS+ server must be configured in the specified context; see Chapter 17, “TACACS+ Configuration.” |

## Configure Subscriber Accounting

To configure subscriber accounting, perform the tasks described in the following sections:

- Configure Global Subscriber Accounting
- Configure Context-Specific Subscriber Accounting
- Configure Two-Stage Subscriber Accounting

### Configure Global Subscriber Accounting

To configure global subscriber accounting, perform the tasks described in Table 15-21.

**Note** You must configure local subscriber authentication; for more information, see “Configure Global RADIUS Authentication” earlier in this section. You must also configure at least one RADIUS accounting server in the local context; for more information, see Chapter 16, “RADIUS Configuration.”

**Table 15-21 Configure Global Subscriber Accounting**

| #  | Task                                                                  | Root Command                                            | Notes                                                                                                                                                                                                                                       |
|----|-----------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Enable global subscriber session accounting messages.                 | <b>aaa global accounting subscriber</b>                 | Enter this command in context configuration mode.<br>Accounting messages for subscriber sessions in all contexts are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.          |
| 2. | Enable global subscriber session accounting update messages.          | <b>aaa global update subscriber</b>                     | Enter this command in global configuration mode.<br>Updated accounting records for subscriber sessions in all contexts are sent to one or more RADIUS accounting server with IP addresses or hostnames configured in the local context.     |
| 3. | Enable global accounting messages for the <b>reauthorize</b> command. | <b>aaa global accounting reauthorization subscriber</b> | Enter this command in global configuration mode.<br>Accounting messages for the reauthorize command issued in any context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context. |

**Table 15-21 Configure Global Subscriber Accounting** (*continued*)

| #  | Task                                                                                           | Root Command                       | Notes                                                                                                                                                                                                                                                                     |
|----|------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. | Enable global accounting messages for subscriber session DHCP lease or reauthorization events. | <b>aaa global accounting event</b> | Enter this command in global configuration mode.<br>Accounting updates for DHCP lease or reauthorization events for subscriber sessions in all contexts are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context. |

### Configure Context-Specific Subscriber Accounting

To configure context-specific subscriber accounting, perform the tasks described Table 15-22. Enter all commands in context configuration mode.

**Note** At least one RADIUS accounting server must be configured in the current context before any messages can be sent. See Chapter 16, “RADIUS Configuration,” for more information.

**Table 15-22 Configure Context-Specific Subscriber Accounting**

| #  | Task                                                                                       | Root Command                                     | Notes                                                                                                                                                                                                                             |
|----|--------------------------------------------------------------------------------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Enable context-specific subscriber accounting messages.                                    | <b>aaa accounting subscriber</b>                 | Accounting messages for subscriber sessions in the current context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.                                               |
| 2. | Enable context-specific subscriber session accounting messages.                            | <b>aaa update subscriber</b>                     | Sends updated accounting records for subscriber sessions in the current context to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.                                           |
| 3. | Enable context-specific accounting messages for the <b>reauthorize</b> command.            | <b>aaa accounting reauthorization subscriber</b> | Accounting messages for the <b>reauthorize</b> command used in the current context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.                               |
| 4. | Enable context-specific accounting messages for DHCP lease or reauthorization information. | <b>aaa accounting event</b>                      | Accounting messages for DHCP lease or reauthorization information for subscriber sessions in the current context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context. |
| 5. | Suppress accounting messages when subscriber sessions cannot be established.               | <b>aaa accounting suppress-acct-on-fail</b>      | Accounting messages are not sent to the RADIUS server when subscriber sessions cannot be established due to an authentication problem, a changed IP address, and so on.                                                           |

### Configure Two-Stage Subscriber Accounting

Two-stage accounting collects RADIUS accounting data on both global RADIUS servers and context-specific RADIUS servers.

To configure two-stage accounting for subscriber sessions, perform the tasks in the “Configure Subscriber Accounting” and “Configure Context-Specific Subscriber Accounting” sections.

## Configure L2TP Accounting

To configure L2TP accounting, perform the tasks described in the following sections:

- Configure Global L2TP Accounting
- Configure Context-Specific L2TP Accounting
- Configure Two-Stage L2TP Accounting

### Configure Global L2TP Accounting

To configure global L2TP accounting, perform the task described in Table 15-23.

**Table 15-23 Configure Global L2TP Accounting**

| Task                              | Root Command                              | Notes                                                                                                                                                                                                                                                      |
|-----------------------------------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure global L2TP accounting. | <b>aaa global accounting l2tp-session</b> | Enter this command in global configuration mode.<br>For all contexts, accounting messages for L2TP tunnels, or sessions in L2TP tunnels, are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context. |

### Configure Context-Specific L2TP Accounting

To configure context-specific L2TP accounting, perform the task described in Table 15-24.

**Table 15-24 Configure Context-Specific L2TP Accounting**

| Task                                        | Root Command               | Notes                                                                                                                                                                                                                                                             |
|---------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure context-specific L2TP accounting. | <b>aaa accounting l2tp</b> | Enter this command in context configuration mode.<br>For the current context, accounting messages for L2TP tunnels, or sessions in L2TP tunnels, are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context. |

### Configure Two-Stage L2TP Accounting

Two-stage accounting collects RADIUS accounting data on both global RADIUS accounting servers and context-specific RADIUS accounting servers.

To configure two-stage accounting for subscriber sessions, perform the tasks in the “Configure Global L2TP Accounting” and “Configure Context-Specific L2TP Accounting” sections.

## Configuration Examples

The following sections provide AAA configuration examples:

- Subscriber Authentication
- Subscriber Reauthorization

## Subscriber Authentication

Subscriber authentication can be configured using several methods of authentication. For example, different subscribers can be authenticated by different RADIUS servers in distinct contexts.

In this example, subscriber `janet` in the `AAA_local` context is authenticated by the configuration in that context. Subscriber `rene` in the `AAA_radius` context is authenticated by the RADIUS server in that context. Subscriber `kevin` in the `AAA_global` context is authenticated by the RADIUS server in the `local` context. The configuration for this example is as follows:

```
[local]Redback(config)#aaa global authentication subscriber radius context local
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius server 10.1.1.1 key TopSecret
.
.
.
[local]Redback(config)#context AAA_local
[local]Redback(config-ctx)#aaa authentication subscriber local
[local]Redback(config-ctx)#interface corpA multibind
[local]Redback(config-if)#ip address 10.1.3.30 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#subscriber name janet
[local]Redback(config-sub)#password dragon
[local]Redback(config-sub)#ip address 10.1.3.30 255.255.255.0
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 6/1
[local]Redback(config-atm-oc)#atm pvc 1 100 profile ubr encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber janet@AAA_local password dragon
.
.
.
[local]Redback(config)#context AAA_radius
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#radius server 10.2.2.2 key TopSecret
[local]Redback(config-ctx)#interface corpB multibind
[local]Redback(config-if)#ip address 10.2.4.40 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 6/1
[local]Redback(config-atm-oc)#atm pvc 2 200 profile ubr encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber rene@AAA_radius password tiger
.
.
.
[local]Redback(config)#context AAA_global
[local]Redback(config-ctx)#aaa authentication subscriber global
[local]Redback(config-ctx)#interface corpC multibind
[local]Redback(config-if)#ip address 10.3.5.50 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
```

```
[local]Redback(config)#port atm 6/1
[local]Redback(config-atm-oc)#atm pvc 3 300 profile ubr encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber kevin@AAA_global password lion
```

## Subscriber Reauthorization

The following example enables RADIUS reauthorization for subscriber circuits and accounting messages:

```
[local]Redback(config-ctx)#radius server 10.10.11.12 key redback
[local]Redback(config-ctx)#radius attribute nas-ip-address interface loop1
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#aaa accounting subscriber radius
[local]Redback(config-ctx)#aaa accounting reauthorization subscriber radius
[local]Redback(config-ctx)#aaa update subscriber 10
[local]Redback(config-ctx)#aaa accounting event reauthorization
[local]Redback(config-ctx)#aaa reauthorization bulk radius
[local]Redback(config-ctx)#radius accounting server 10.10.11.2. key redback
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure AAA. The commands are presented in alphabetical order.

|                                                  |                                                         |
|--------------------------------------------------|---------------------------------------------------------|
| <b>aaa accounting administrator</b>              | <b>aaa global accounting reauthorization subscriber</b> |
| <b>aaa accounting commands</b>                   | <b>aaa global accounting subscriber</b>                 |
| <b>aaa accounting event</b>                      | <b>aaa global authentication subscriber</b>             |
| <b>aaa accounting l2tp</b>                       | <b>aaa global maximum subscriber</b>                    |
| <b>aaa accounting reauthorization subscriber</b> | <b>aaa global update subscriber</b>                     |
| <b>aaa accounting subscriber</b>                 | <b>aaa hint ip-address</b>                              |
| <b>aaa accounting suppress-acct-on-fail</b>      | <b>aaa last-resort</b>                                  |
| <b>aaa authentication administrator</b>          | <b>aaa maximum subscriber</b>                           |
| <b>aaa authentication subscriber</b>             | <b>aaa provision binding-order</b>                      |
| <b>aaa authorization commands</b>                | <b>aaa provision route</b>                              |
| <b>aaa authorization tunnel</b>                  | <b>aaa reauthorization bulk</b>                         |
| <b>aaa global accounting event</b>               | <b>aaa update subscriber</b>                            |
| <b>aaa global accounting l2tp-session</b>        | <b>aaa username-format</b>                              |

## aaa accounting administrator

**aaa accounting administrator tacacs+**

**{no | default} aaa accounting administrator tacacs+**

### Purpose

Enables accounting messages for administrator sessions.

### Command Mode

context configuration

### Syntax Description

|                |                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>tacacs+</b> | Specifies that accounting messages are to be sent to a Terminal Access Controller Access Control System Plus (TACACS+) server. |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|

### Default

TACACS+-based accounting is disabled.

### Usage Guidelines

Use the **aaa accounting administrator tacacs+** command to enable accounting messages for administrator sessions to be sent to the TACACS+ server.

**Note** You must configure at least one TACACS+ server in the current context before any messages can be sent to it. To configure the server, use the **tacacs+ server** command (in context configuration mode); for more information, see Chapter 17, “TACACS+ Configuration.”

Use the **no** or **default** form of this command to disable the sending of TACACS+ accounting messages.

### Examples

The following example enables accounting messages for administrator sessions for the `local` context:

```
[local]Redback(config-ctx)#aaa accounting administrator tacacs+
```

### Related Commands

**tacacs+ server**



## aaa accounting commands

**aaa accounting commands** *level* **tacacs+** [**except** *except-level*]

{**no** | **default**} **aaa accounting commands** *level*

### Purpose

Specifies that accounting messages are sent to a Terminal Access Controller Access Control System Plus (TACACS+) server whenever an administrator enters commands at the specified privilege level (or higher).

### Command Mode

context configuration

### Syntax Description

|                                   |                                                                                                                                                                                                                      |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>level</i>                      | Command privilege level. The range of values is 0 to 15.                                                                                                                                                             |
| <b>tacacs+</b>                    | Indicates that a TACACS+ server must record commands for accounting.                                                                                                                                                 |
| <b>except</b> <i>except-level</i> | Optional. Command privilege level that will not be sent to the server for accounting. The range of values is 1 to 15. The value for this argument must be greater than that specified for the <i>level</i> argument. |

### Default

No TACACS+ accounting of commands is required.

### Usage Guidelines

Use the **aaa accounting commands** command to specify that accounting messages are sent to a TACACS+ server whenever an administrator enters commands at the specified privilege level (or higher).

To use TACACS+, you must configure the IP address or hostname of a TACACS+ server in the context in which commands are accessed. To configure the server's IP address or hostname, use the **tacacs+ server** command (in context configuration mode); see Chapter 17, "TACACS+ Configuration."

For information about default privilege levels for commands and how to modify command privilege levels, see the "Basic System Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Use the **no** or **default** form of this command to disable the sending of accounting messages to the TACACS+ server.

### Examples

The following example sends accounting messages to a TACACS+ server for commands that are configured with a privilege level of 6 or greater with the exception of privilege level 15:

```
[local]Redback(config-ctx)#aaa accounting commands 6 tacacs+ except 15
```

## Related Commands

**aaa authorization commands**  
**tacacs+ server**

## aaa accounting event

**aaa accounting event {dhcp | reauthorization}**

**{no | default} aaa accounting event {dhcp | reauthorization}**

### Purpose

Enables accounting messages for Dynamic Host Configuration Protocol (DHCP) lease or reauthorization information for subscriber sessions in the current context to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the same context.

### Command Mode

context configuration

### Syntax Description

|                        |                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dhcp</b>            | Enables accounting messages to be sent whenever a DHCP lease is created or released.                                                                                                                |
| <b>reauthorization</b> | Enables accounting messages to be sent for subscriber reauthorization sessions. The information sent in the messages provides details about subscriber circuits after reauthorization is completed. |

### Default

RADIUS-based accounting is disabled.

### Usage Guidelines

Use the **aaa accounting event** command to enable accounting messages for DHCP lease or reauthorization information for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

**Note** You must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, “RADIUS Configuration.”

Use **no** or **default** form of this command to disable the sending of RADIUS-based accounting messages.

### Examples

The following example enables accounting messages for reauthorization information for subscriber sessions in the corpA context to be sent to the RADIUS accounting server with an IP address or hostname in the same context:

```
[local]Redback(config)#context corpA
[local]Redback(config-ctx)#aaa accounting event reauthorization
```

## Related Commands

**aaa accounting reauthorization subscriber**  
**aaa global accounting event**  
**radius accounting server**

## aaa accounting l2tp

```
aaa accounting l2tp {session | tunnel} {none | radius}
{no | default} aaa accounting l2tp {session | tunnel}
```

### Purpose

Enables accounting messages for Layer 2 Tunneling Protocol (L2TP) tunnels or sessions in L2TP tunnels for the current context to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the same context.

### Command Mode

context configuration

### Syntax Description

|                |                                         |
|----------------|-----------------------------------------|
| <b>session</b> | Specifies sessions within L2TP tunnels. |
| <b>tunnel</b>  | Specifies L2TP tunnels.                 |
| <b>none</b>    | Disables RADIUS-based accounting.       |
| <b>radius</b>  | Enables RADIUS-based accounting.        |

### Default

RADIUS-based accounting is disabled.

### Usage Guidelines

Use the **aaa accounting l2tp** command to enable accounting messages for L2TP tunnels or sessions in L2TP tunnels for the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

**Note** You must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, “RADIUS Configuration.”

To enable two-stage accounting, configure one or more RADIUS accounting servers in a nonlocal context and configure one or more RADIUS accounting servers in the local context. In two-stage accounting, data for all contexts are sent to both the RADIUS accounting servers in the local context and to any RADIUS accounting servers in the context to which the subscriber is bound.

**Note** If the SmartEdge router is acting as an L2TP network server (LNS) in a context, the accounting data is for the LNS; if it is acting as an L2TP access concentrator (LAC), the accounting data is for the LAC. If it is acting as a tunnel switch, both sets of accounting data are sent to the RADIUS server; in this case, each set of data is tagged, as follows:

- LNS accounting data (facing an LAC)—tag 1
- LAC accounting data (facing the LNS)—tag 2

Use the **no** or **default** form of this command (or the **none** keyword) to disable the sending of RADIUS accounting messages.

### Examples

The following example enables accounting messages for L2TP tunnels in the `siteA` context to be sent to the RADIUS accounting server configured in the `siteA` context:

```
[local]Redback(config)#context siteA  
[local]Redback(config-ctx)#aaa accounting l2tp radius
```

### Related Commands

```
aaa global accounting l2tp-session  
radius accounting server
```

## aaa accounting reauthorization subscriber

**aaa accounting reauthorization subscriber** {none | radius}

{no | default} **aaa accounting reauthorization subscriber**

### Purpose

Enables accounting messages for the **reauthorize** command entered in the current context in exec mode to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the same context.

### Command Mode

context configuration

### Syntax Description

|               |                                                      |
|---------------|------------------------------------------------------|
| <b>none</b>   | Disables RADIUS-based accounting.                    |
| <b>radius</b> | Enables RADIUS-based accounting messages to be sent. |

### Default

RADIUS-based accounting is disabled.

### Usage Guidelines

Use the **aaa accounting reauthorization** command to enable accounting messages for the **reauthorize** command entered in the current context in exec mode to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

**Note** You must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, “RADIUS Configuration.”

Use the **no** or **default** form of this command or the **none** keyword to disable the sending of RADIUS accounting messages.

### Examples

The following example enables accounting messages for subscriber reauthorization in the corpA context to be sent to the RADIUS server configured in the corpA context:

```
[local]Redback(config)#context corpA
[local]Redback(config-ctx)#aaa accounting reauthorization radius
```

## Related Commands

aaa accounting event  
aaa global accounting reauthorization subscriber  
radius accounting server



## aaa accounting subscriber

**aaa accounting subscriber** {none | radius}

{no | default} **aaa accounting subscriber**

### Purpose

Enables accounting messages for subscriber sessions in the current context to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the same context.

### Command Mode

context configuration

### Syntax Description

|               |                                   |
|---------------|-----------------------------------|
| <b>none</b>   | Disables RADIUS-based accounting. |
| <b>radius</b> | Enables RADIUS-based accounting.  |

### Default

RADIUS-based accounting is disabled.

### Usage Guidelines

Use the **aaa accounting subscriber** command to enable accounting messages for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

**Note** You must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, “RADIUS Configuration.”

To enable two-stage accounting, configure one or more RADIUS accounting servers in a nonlocal context and configure one or more RADIUS accounting servers in the local context. You must also configure global authentication using the **aaa authentication subscriber** command (in context configuration mode) and the **aaa global authentication subscriber** command (in global configuration mode). In two-stage accounting, data for all contexts are sent to both the RADIUS accounting servers in the local context and to any RADIUS accounting servers in the context to which the subscriber is bound.

**Note** This command can only enable sending of accounting packets that include packet and byte counts for a circuit if the **counters** command is configured in the Asynchronous Transfer Mode (ATM) profile referenced by the circuit to which the subscriber is bound; for more information about ATM profiles, see the “Circuit Configuration” chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

**Note** The SmartEdge OS does not send the RADIUS accounting packet for a Point-to-Point Protocol (PPP) subscriber until the session completes the Internet Protocol Control Protocol (IPCP) stage of PPP. Delaying the start record assures that standard RADIUS attribute 8, Framed-IP-Address, is populated.

Use the **no** or **default** form of this command or the **none** keyword to disable the sending of RADIUS accounting messages.

## Examples

The following example enables accounting messages for subscriber sessions in the `siteA` context to be sent to the RADIUS accounting server configured in the `siteA` context:

```
[local]Redback(config)#context siteA  
[local]Redback(config-ctx)#aaa accounting subscriber radius
```

## Related Commands

```
aaa authentication subscriber  
aaa global accounting subscriber  
aaa global authentication subscriber  
radius accounting server  
radius server
```

## aaa accounting suppress-acct-on-fail

**aaa accounting suppress-acct-on-fail** [**except-for** *error-cond*]

{**no** | **default**} **aaa accounting suppress-acct-on-fail** [**except-for** *error-cond*]

### Purpose

Suppresses the sending of accounting messages to Remote Authentication Dial-In User Service (RADIUS) servers when a subscriber session cannot be established due to an authentication problem, a changed IP address, and so on.

### Command Mode

context configuration

### Syntax Description

- except-for** *error-cond*      Optional. Error condition for which accounting messages are not suppressed, according to one of the following keywords or constructs:
- **duplicate-ip**—Does not suppress accounting messages if the IP address specified in an Access Accept packet is already in use by another subscriber.
  - **no-l2tp-peer**—Does not suppress accounting messages if the Layer 2 Tunneling Protocol (L2TP) peer cannot be reached and the session not brought up.
  - **duplicate-ip no-l2tp-peer**—Does not suppress accounting messages if either of the error conditions is true.

### Default

RADIUS-based accounting is disabled. When RADIUS-based accounting is enabled using the **aaa accounting subscriber** command (in context configuration mode), the SmartEdge OS always sends an accounting record when a subscriber session cannot be established.

### Usage Guidelines

Use the **aaa accounting suppress-acct-on-fail** command to suppress the sending of accounting messages to RADIUS accounting servers when a subscriber session cannot be established due to an authentication problem, a changed IP address, and so on.

You can specify either or both of the error conditions for which accounting messages will not be suppressed.

Use the **no** or **default** form of this command to always suppress the sending of accounting messages when an error condition occurs.

### Examples

The following example suppresses accounting messages sent to RADIUS accounting servers except when the L2TP peer for a subscriber session cannot be reached and the session not established:

```
[local]Redback(config-ctx)#aaa accounting suppress-acct-on-fail except-for no-l2tp-peer
```

### Related Commands

**aaa accounting subscriber**

## aaa authentication administrator

**aaa authentication administrator** *method* [*method* [*method*]] | [**maximum sessions** *num-sess*]  
 {**no** | **default**} **aaa authentication administrator**

### Purpose

Prioritizes the methods available for authenticating administrators, or modifies the maximum number of administrator sessions that can be simultaneously active.

### Command Mode

context configuration

### Syntax Description

*method*

Authentication method. One method is required. Specifying a second or third method is optional. Separate each value with a space. The *method* argument can take any of the three following values:

- **local**—Specifies authentication by the SmartEdge OS configuration.
- **radius**—Specifies authentication by a Remote Authentication Dial-In User Service (RADIUS) server.
- **tacacs+**—Specifies authentication by a Terminal Access Controller Access Control System Plus (TACACS+) server.

**maximum sessions** *num-sess*

Optional. Maximum number of administrator sessions that be simultaneously active. The range of values is 0 to 20.

For the local context, the default value is 10. For nonlocal contexts, the default value is 0 or 1 (0 when no administrators are configured; 1 when administrators are configured).

The total number of active Telnet, Secure Shell (SSH), or both types of administrator sessions (must be less than or equal to 20 on the system as a whole (for all configured contexts). In addition, one console port administrator session is supported.

### Default

Authentication is performed by the SmartEdge OS configuration. For the local context, the number of administrator sessions that can be simultaneously active is 10; for nonlocal contexts, it is 0 or 1 (0 when no administrators are configured; 1 when administrators are configured).

## Usage Guidelines

Use the **aaa authentication administrator** command to prioritize the available administrator authentication methods or to modify the maximum number of administrator sessions that can be simultaneously active.

Authentication methods are attempted in the order in which you enter the keywords. For example, if you enter the **radius** keyword first, followed by the **tacacs+** keyword, followed by the **local** keyword, authentication is first attempted by the RADIUS server, then by the TACACS+ server, and finally, by the local configuration.

**Note** If a RADIUS or TACACS+ server rejects the authentication of an administrator, authentication is not attempted by the next method. If, however, the RADIUS or TACACS+ server is unavailable or unreachable, authentication is attempted by the next method. Authentication by the SmartEdge OS configuration is always available as a fallback, even when the **local** keyword is not specified. If the SmartEdge OS configuration rejects an administrator, authentication is not attempted by the next method.

**Note** To use RADIUS, the IP address or hostname of at least one RADIUS server must be configured in the context to which the administrator is to be bound. To configure the server's IP address or hostname, use the **radius server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration." To use TACACS+, the IP address or hostname of a TACACS+ server must be configured in the context to which the administrator is to be bound. To configure the server's IP address or hostname, use the **tacacs+ server** command (in context configuration mode); for more information, see Chapter 17, "TACACS+ Configuration."

**Note** The total number of simultaneous, active Telnet and SSH administrator sessions must be less than or equal to 20 on the system as a whole (that is, for all configured contexts).

The maximum number of administrator SSH sessions that can be simultaneously active for all configured contexts can be configured through the **ssh server full-drop** command (in global configuration mode); the default value is 20. If there are active Telnet sessions, the maximum number of global SSH sessions is limited to the maximum number of SSH sessions configured through the **ssh server full-drop** command, minus the number of active Telnet sessions in all contexts. For more information about the **ssh server full-drop** command, see the "System Access Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Use the **no** or **default** form of this command to return to using only the SmartEdge OS configuration for authentication of administrators.

## Examples

The following example configures the SmartEdge router to authenticate users via the RADIUS server, with the SmartEdge OS configuration authentication as a backup:

```
[local]Redback(config-ctx)#aaa authentication administrator radius local
```

The following example modifies the number of administrator sessions that can be simultaneously active in the local context from 10 (the default) to 15:

```
[local]Redback(config-ctx)#aaa authentication administrator maximum sessions 15
```

## Related Commands

`radius server`  
`tacacs+ server`

## aaa authentication subscriber

```
aaa authentication subscriber {global | local [global | none | radius [global | none]] | none |  
radius [global | local [global | none]]}  
{no | default} aaa authentication subscriber
```

### Purpose

Authenticates subscribers through the SmartEdge OS configuration or through one or more Remote Authentication Dial-In User Service (RADIUS) server databases.

### Command Mode

context configuration

### Syntax Description

- global** When used alone, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the local context.
- When used as an optional keyword following **local**, first attempts subscriber authentication through the SmartEdge OS configuration in the current context. In the event that no corresponding subscriber record is found in the local database, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the local context.
- When used as an optional keyword following **radius**, first attempts subscriber authentication through one or more RADIUS servers with IP addresses or hostnames configured in the current context. If those RADIUS servers are not reachable, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the local context.
- local** When used alone, authenticates subscribers through the SmartEdge OS configuration in the current context.
- When used as an optional keyword following **radius**, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the current context. If the RADIUS servers are not reachable, authenticates subscribers through the SmartEdge OS configuration in the current context.
- none** When used alone, specifies that authentication of subscribers is not required—all access succeeds.
- When used as an optional keyword following **local**, subscribers are first authenticated through the SmartEdge OS configuration. In the event that no corresponding subscriber record is found in the local database, access succeeds.
- radius** When used alone, authenticates subscribers by one or more RADIUS servers with IP addresses or hostnames in the current context.
- When used as an optional keyword following **local**, first attempts subscriber authentication through the SmartEdge OS configuration in the current context. In the event that no corresponding subscriber record is found in the local database, authenticates subscribers by one or more RADIUS servers with IP addresses or hostnames in the current context.



## Default

Subscribers are authenticated by the SmartEdge OS configuration.

## Usage Guidelines

Use the **aaa authentication subscriber** command to authenticate subscribers through the SmartEdge OS configuration or through one or more RADIUS server databases.

The SmartEdge OS configuration is also referred to as the “local database,” which is simply a set of commands, such as the **subscriber** command (in context configuration mode) and the **password** command (in subscriber configuration mode). For more information about these commands, see the “Subscriber Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

With RADIUS, the database records of the RADIUS server are used to authenticate subscribers. The IP address or hostname of one or more RADIUS servers can be configured in the “local” context or in the context to which the subscriber’s circuit is to be bound. Each context can use its own set of RADIUS servers for authentication. Alternatively, a context can be configured to use the RADIUS servers with IP addresses or hostnames configured in the “local” context—this is known as “global authentication.”

With global authentication, the RADIUS servers are expected to return the Context-Name vendor-specific attribute (VSA) that indicates the particular context to which the subscriber is to be bound. You can also configure the SmartEdge OS to try authentication through one or more RADIUS servers with IP addresses or hostnames configured in the current context first, with a fallback to the global RADIUS server or to the local database, in case the RADIUS server configured in the current context becomes unreachable.

**Note** To use RADIUS, the IP address or hostname of at least one RADIUS server must be configured in the local context or in the context to which the subscriber is to be bound. To configure the server’s IP address or hostname, use the **radius server** command (in context configuration mode); for more information, see Chapter 16, “RADIUS Configuration.”

To disable authentication of subscribers, use the **none** keyword with this command. Do this only when subscriber authentication is not required, such as when Dynamic Host Configuration Protocol (DHCP) is used to obtain IP addresses for subscribers’ hosts.



**Caution** Risk of security breach. With the **aaa authentication subscriber none** command, the SmartEdge OS does not read any of the subscriber records configured, except for the default subscriber record. This means that individual subscriber usernames and passwords are not authenticated by the SmartEdge OS. Therefore, IP addresses, routes, and Address Resolution Protocol (ARP) entries within individual subscriber records are not installed. Verify your network security setup before using the **aaa authentication subscriber none** command.

Use the **no** or **default** form of this command to authenticate subscribers through the SmartEdge OS configuration.

### Examples

The following example authenticates subscriber sessions for the `siteB` context by first using the RADIUS server configured within the context, followed by the SmartEdge OS configuration for the context should the RADIUS server become unreachable:

```
[local]Redback(config)#context siteB
[local]Redback(config-ctx)#radius server 10.2.3.4 key TopSecret
[local]Redback(config-ctx)#aaa authentication subscriber radius local
```

### Related Commands

`aaa global authentication subscriber`  
`radius server`

# aaa authorization commands

```
aaa authorization commands level tacacs+ [none] [except except-level]  
{no | default} aaa authorization commands level
```

## Purpose

Specifies that commands with a matching privilege level (or higher) require authorization through Terminal Access Controller Access Control System Plus (TACACS+).

## Command Mode

context configuration

## Syntax Description

|                                   |                                                                                                                                                                                                                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>level</i>                      | Privilege level. The range of values is 0 to 15. A user account with a privilege level that matches or is greater than the value of the <i>level</i> argument must be authorized by TACACS+ before the user can enter SmartEdge OS CLI commands set to this privilege level. |
| <b>tacacs+</b>                    | Enforces authorization through TACACS+.                                                                                                                                                                                                                                      |
| <b>none</b>                       | Optional. Disables authorization if the server is unavailable.                                                                                                                                                                                                               |
| <b>except</b> <i>except-level</i> | Optional. Command privilege level that will not be sent to the server for authorization. The range of values is 1 to 15. The value for this argument must be greater than that specified for the <i>level</i> argument.                                                      |

## Default

Commands do not require authorization through TACACS+.

## Usage Guidelines

Use the **aaa authorization commands** command to specify that commands with a matching privilege level (or higher) require authorization through TACACS+.



**Caution** Risk of administrative failure. If a TACACS+ server has not been set up and configured before this command is issued, you may not have authorization to use commands on your SmartEdge router. To reduce the risk, you must first configure the IP address or hostname of a TACACS+ server in the context in which commands are accessed. To do so, enter the **tacacs+ server** command (in context configuration mode); for more information, see Chapter 17, “TACACS+ Configuration.”



**Caution** Risk of administrative failure. If you have configured authorization without the **none** keyword and the TACACS+ server is not available, you might not have authorization to use commands on your SmartEdge router. To reduce the risk, always include the **none** keyword when entering this command.



**Caution** Risk of administrative failure. If the administrator record on the TACACS+ server is set up to authorize only a limited set of commands, the administrator might not be allowed to perform critical tasks using the SmartEdge OS. To reduce the risk, we recommend, therefore, that you configure at least one administrator record on the TACACS+ server that has authorization to access all commands.

**Note** For information about default command privilege levels and how to modify them, see the “Basic System Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Use the **no** or **default** form of this command to disable the requirement for TACACS+ authorization.

## Examples

The following example requires TACACS+ authorization in the `restricted` context for the use of commands with privilege levels of `10` or higher with the exception of privilege level `15`:

```
[restricted]Redback(config)#configure
[restricted]Redback(config-ctx)#aaa authorization commands 10 except 15
```

## Related Commands

**aaa accounting commands**  
**tacacs+ server**

## aaa authorization tunnel

**aaa authorization tunnel {local | radius}**

**{no | default} aaa authorization tunnel {local | radius}**

### Purpose

Specifies the type of authorization for Layer 2 Tunneling Protocol (L2TP) peers.

### Command Mode

context configuration

### Syntax Description

|               |                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------|
| <b>local</b>  | Specifies that L2TP peers are authorized by the local configuration.                                      |
| <b>radius</b> | Specifies that L2TP peers are authorized by a Remote Authentication Dial-In User Service (RADIUS) server. |

### Default

L2TP peers are authorized by the SmartEdge OS configuration.

### Usage Guidelines

Use the **aaa authorization tunnel** command to specify the type of authorization for L2TP peers.

Use the **no** or **default** form of this command to specify the default behavior.

### Examples

The following example configures the `local` context to authorize L2TP peers by a RADIUS server:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#aaa authorization tunnel radius
```

### Related Commands

None

## aaa global accounting event

**aaa global accounting event {dhcp | reauthorization}**

**{no | default} aaa global accounting event {dhcp | reauthorization}**

### Purpose

Enables accounting messages for Dynamic Host Configuration Protocol (DHCP) lease or reauthorization information for subscriber sessions in all contexts to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

### Command Mode

global configuration

### Syntax Description

|                        |                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dhcp</b>            | Enables accounting messages to be sent whenever a DHCP lease is created or released.                                                                                                                |
| <b>reauthorization</b> | Enables accounting messages to be sent for subscriber reauthorization sessions. The information sent in the messages provides details about subscriber circuits after reauthorization is completed. |

### Default

RADIUS-based accounting is disabled.

### Usage Guidelines

Use the **aaa global accounting event** command to enable accounting messages for DHCP lease or reauthorization information for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

Use the **no** or **default** form of this command to disable RADIUS-based accounting.

### Examples

The following example enables accounting messages for reauthorization information for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context:

```
[local]Redback(config)#aaa global accounting event reauthorization
```

### Related Commands

**aaa accounting event**  
**aaa reauthorization bulk**  
**radius accounting server**

## aaa global accounting l2tp-session

**aaa global accounting l2tp-session radius context local**

**{no | default} aaa global accounting l2tp-session**

### Purpose

Enables accounting messages for Layer 2 Tunneling Protocol (L2TP) tunnels or sessions in L2TP tunnels in all contexts to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

### Command Mode

global configuration

### Syntax Description

|                             |                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius context local</b> | Indicates accounting messages are sent by RADIUS accounting servers with IP addresses or hostnames configured in the local context. |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|

### Default

Disabled.

### Usage Guidelines

Use the **aaa global accounting l2tp-session** command to enable accounting messages for L2TP tunnels or sessions in L2TP tunnels in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

**Note** To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration," for more information.

Use the **no** or **default** form of this command to return the system to its default behavior of performing accounting based on the SmartEdge OS configuration.

### Examples

The following example configures the system to send accounting messages for L2TP sessions in all contexts to one or more RADIUS servers with IP addresses or hostnames configured in the local context:

```
[local]Redback(config)#aaa global accounting l2tp-session radius context local
```

### Related Commands

**aaa accounting l2tp**  
**radius accounting server**

## aaa global accounting reauthorization subscriber

**aaa global accounting reauthorization subscriber radius context local**

**{no | default} aaa global accounting reauthorization subscriber**

### Purpose

Enables accounting messages for the **reauthorize** command entered in any context in exec mode to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

### Command Mode

global configuration

### Syntax Description

|                             |                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius context local</b> | Indicates accounting messages are sent by RADIUS accounting servers with IP addresses or hostnames configured in the <code>local</code> context. |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

RADIUS-based accounting is disabled.

### Usage Guidelines

Use the **aaa global accounting reauthorization subscriber** command to enable accounting messages for the **reauthorize** command entered in any context in exec mode to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context. These messages indicate that subscriber reauthorization has been completed.

**Note** To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration."

Use the **no** or **default** form of this command to return the system to its default behavior of performing accounting based on the SmartEdge OS configuration.

### Examples

The following example configures the system to send accounting messages for subscriber reauthorization in all contexts to one or more RADIUS servers with IP addresses or hostnames configured in the `local` context:

```
[local]Redback(config)#aaa global accounting reauthorization subscriber radius context local
```



## Related Commands

`aaa accounting reauthorization subscriber`  
`radius accounting server`

## aaa global accounting subscriber

**aaa global accounting subscriber radius context local**

**{no | default} aaa global accounting subscriber**

### Purpose

Enables accounting messages for subscriber sessions in all contexts to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

### Command Mode

global configuration

### Syntax Description

|                             |                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius context local</b> | Indicates accounting messages are sent by RADIUS accounting servers with IP addresses or hostnames configured in the <code>local</code> context. |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

Disabled.

### Usage Guidelines

Use the **aaa global accounting subscriber** command to enable accounting messages for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

**Note** To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration."

Use the **no** or **default** form of this command to return the system to its default behavior of performing accounting based on the SmartEdge OS configuration.

### Examples

The following example configures the system to send accounting messages for subscriber sessions in all contexts to one or more RADIUS servers with IP addresses or hostnames configured in the `local` context:

```
[local]Redback(config)#aaa global accounting subscriber radius context local
```

### Related Commands

**aaa accounting subscriber**  
**aaa update subscriber**  
**radius accounting server**

# aaa global authentication subscriber

**aaa global authentication subscriber radius context local**

**{no | default} aaa global authentication subscriber**

## Purpose

Enables global subscriber authentication through one or more Remote Authentication Dial-In User Service (RADIUS) servers with IP addresses or hostnames configured in the local context.

## Command Mode

global configuration

## Syntax Description

|                             |                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>radius context local</b> | Indicates authentication is performed by the RADIUS servers with IP addresses or hostnames configured in the local context. |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|

## Default

Disabled.

## Usage Guidelines

Use the **aaa global authentication subscriber** command to enable global subscriber authentication through one or more RADIUS servers with IP addresses or hostnames configured in the local context.

**Note** To use RADIUS, you must configure the IP address or hostname of at least one RADIUS server in the local context. To configure the server's IP address or hostname, enter the **radius server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration."

Use the **no** or **default** form of this command to disable global subscriber authentication.

## Examples

The following example configures the context `siteA` to globally authenticate its subscriber sessions using the RADIUS server with the IP address of `10.2.3.4` configured in the `local` context:

```
[local]Redback(config)#aaa global authentication subscriber radius context local
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius server 10.2.3.4 key TopSecret
[local]Redback(config)#context siteA
[local]Redback(config-ctx)#aaa authentication subscriber global
```

## Related Commands

**aaa authentication subscriber**  
**radius server**

## aaa global maximum subscriber

**aaa global maximum subscriber active** *count*

{**no** | **default**} **aaa global maximum subscriber**

### Purpose

Limits the total number of subscriber sessions that can be simultaneously active in all configured contexts.

### Command Mode

global configuration

### Syntax Description

**active** *count*      Maximum number of subscriber sessions that can be simultaneously active.

The range of values is dependent on the purchased subscriber license, the SmartEdge router platform, and the controller card. The range of values is as follows:

- SE800-XCRP—16,000
- SE800-XCRP3-Base—16,000
- SE800-XCRP3—48,000
- SE400-XCRP3-Base—16,000
- SE400-XCRP3—32,000

The **subscriber** command (in software license configuration mode) specifies the maximum number of active subscriber sessions and is described in the “Basic System Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

### Default

There is no limit to the number of subscriber sessions that can be simultaneously active in all configured contexts.

### Usage Guidelines

Use the **aaa global maximum subscriber** command to limit the total number of subscriber sessions that can be simultaneously active in all configured contexts.

Use the **no** or **default** form of this command to restore the default of no limit to the number of subscriber sessions.

### Examples

The following example sets the maximum number of simultaneous active subscriber sessions for all configured contexts to 12000:

```
[local]Redback(config)#aaa global maximum subscriber active 12000
```

## Related Commands

`aaa maximum subscriber`

## aaa global update subscriber

**aaa global update subscriber** *interval*

{no | default} **aaa global update subscriber**

### Purpose

Sends updated accounting records for subscribers in all contexts to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

### Command Mode

global configuration

### Syntax Description

*interval*                      Period (in minutes) between accounting updates. The range of values is 10 to 10,080.

### Default

Disabled.

### Usage Guidelines

Use the **aaa global update subscriber** command to send updated accounting records for subscribers in all contexts to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

**Note** You must configure accounting using the **aaa global accounting subscriber** command (in global configuration mode).

**Note** To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration."

Use the **no** or **default** form of this command to disable subscriber account updating.

### Examples

The following example globally configures an update to be sent for all subscribers in the system when each subscriber's session comes up, and every 20 minutes thereafter, for as long as the subscriber session lasts:

```
[local]Redback(config)#aaa global update subscriber 20
```

## Related Commands

`aaa global accounting subscriber`  
`aaa update subscriber`  
`radius accounting server`

## aaa hint ip-address

**aaa hint ip-address**

**no aaa hint ip-address**

### Purpose

Enables the SmartEdge OS to notify the Remote Authentication Dial-In User Service (RADIUS) server that the IP address in the Framed-IP-Address attribute is the preferred IP address.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

This feature is disabled.

### Usage Guidelines

Use the **aaa hint ip-address** command to enable the SmartEdge OS to notify the RADIUS server that the IP address in the Framed-IP-Address attribute is the preferred IP address.

This feature applies only to subscribers that you have configured using the **ip address** command (in subscriber configuration mode) with the **pool** keyword. The SmartEdge OS selects an unused IP address from the pool and sends it to the RADIUS server in an Access-Request message. The **ip address** command is described in the “Subscriber Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS. It does not apply to subscribers who are configured for SmartEdge OS authentication.

The IP address selected from the unnamed IP pool is a “hint” to the RADIUS server that the selected address is preferred. The RADIUS server can choose to honor the hint or override it with a different IP address. The SmartEdge OS uses the address only if the RADIUS server confirms that it is acceptable; the SmartEdge OS action corresponding to the RADIUS response is described in the “IP Address Assignment” section.

**Note** This command is not available if you have enabled global subscriber authentication using the **aaa global authentication subscriber** command (in global configuration mode).

Use the **no** form of this command to disable this feature.

### Examples

The following example enables this feature in the customers context:

```
[local]Redback(config)#context customers
[local]Redback(config-cxt)#aaa hint ip-address
```



## Related Commands

`aaa global authentication subscriber`

## aaa last-resort

**aaa last-resort context** *ctx-name* [**append**]

**no aaa last-resort**

### Purpose

Specifies the context in which authentication of a subscriber should be attempted if the subscriber name does not contain a valid domain or context that has been configured in the system.

### Command Mode

global configuration

### Syntax Description

|                                |                                                                           |
|--------------------------------|---------------------------------------------------------------------------|
| <b>context</b> <i>ctx-name</i> | Name of the last resort context.                                          |
| <b>append</b>                  | Optional. Appends the @ symbol and context name to the subscriber's name. |

### Default

No last resort context is configured.

### Usage Guidelines

Use the **aaa last-resort** command to specify the context in which authentication of a subscriber name is to be attempted whenever the domain portion of the subscriber name provided cannot be matched to any configured context or domain.

At the time you enter this command, the SmartEdge OS does not check to ensure you specify a valid context. When a subscriber attempts to connect, and the SmartEdge OS attempts to validate the subscriber in the last resort context, an error message displays if the context does not exist.

Only one last resort context can be in effect at a time. To change the last resort context, create a new one and it overwrites the existing one.

**Note** To use Remote Authentication Dial-In User Service (RADIUS), the IP address or hostname of at least one RADIUS server must be configured in the last resort context. To configure the server's IP address or hostname, enter the **radius server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration."

Use the **no** form of this command to remove the last resort context.

### Examples

The following configuration assumes three contexts: `california`, `nevada`, and `otherstates`. A username, `jill@arizona`, is submitted for authentication, but there is no configured `arizona` context. The following example configures the system in such a way that `jill@arizona` would be submitted for authentication in the `otherstates` context:

```
[local]Redback(config)#aaa last-resort context otherstates
```

## Related Commands

`aaa authentication subscriber`  
`aaa global authentication subscriber`

## aaa maximum subscriber

**aaa maximum subscriber active** *count*

{no | default} **aaa maximum subscriber**

### Purpose

Limits the number of subscriber sessions that can be simultaneously active in a given context.

### Command Mode

context configuration

### Syntax Description

**active count** Maximum number of subscriber sessions that can be simultaneously active.

The range of values is dependent on the purchased subscriber license, the SmartEdge platform, and the controller card. The range of values is as follows:

- SE800-XCRP—16,000
- SE800-XCRP3-Base—16,000
- SE800-XCRP3—48,000
- SE400-XCRP3-Base—16,000
- SE400-XCRP3—32,000

The **subscriber** command (in software license configuration mode) specifies the maximum number of active subscriber sessions and is described in the “Basic System Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

### Default

There is no limit to the number of subscriber sessions that can be simultaneously active in a given context.

### Usage Guidelines

Use the **aaa maximum subscriber** command to limit the number of subscriber sessions that can be simultaneously active in a given context.

Use the **no** or **default** form of this command to restore the default of no limit to the number of subscriber sessions.

### Examples

The following example sets the maximum number of simultaneous active subscriber sessions for the `local` context to 100:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa maximum subscriber active 100
```

## Related Commands

`aaa global maximum subscriber`

## aaa provision binding-order

**aaa provision binding-order ip-address-attr l2tp-attr**

**no aaa provision binding-order ip-address-attr l2tp-attr**

### Purpose

Changes the default order in which the SmartEdge OS searches for the Remote Authentication Dial-In User Service (RADIUS) and Layer 2 Tunneling Protocol (L2TP) attributes to find the IP address be used to bind a subscriber circuit.

### Command Mode

context configuration

### Syntax Description

**ip-address-attr** Uses the IP address in the Framed-IP-Address attribute in the authentication message received from a RADIUS server.

**l2tp-attr** Uses the IP address in the Sub-Address attribute value pair (AVP) in the incoming call request (ICRQ) message received from the L2TP access concentrator (LAC) peer.

### Default

SmartEdge OS searches for the L2TP attribute before searching for the RADIUS attribute.

### Usage Guidelines

Use the **aaa provision binding-order** command to change the default order in which the SmartEdge OS searches for the RADIUS and L2TP attributes to find the IP address to be used to bind a subscriber circuit. The circuit binding has been created using the **bind authentication** command (in the circuit's configuration mode).

Use this command to enable the SmartEdge OS to look for the RADIUS Framed-IP-Address attribute before looking at the L2TP Sub-Address AVP. If the Framed-IP-Address attribute does not exist, the L2TP ICRQ message is examined for the Sub-Address AVP. If the Sub-Address AVP does not exist, the session is not brought up.

Use the **no** form of this command to specify the default order.

For more information about using the **bind authentication** command to create a dynamic binding, see the "Bindings Configuration" chapter in the *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS.

### Examples

The following example specifies that the IP address (and its interface) in the RADIUS record be used to bind a subscriber circuit:

```
[local]Redback(config-ctx)#aaa provision binding-order ip-address-attr l2tp-attr
```

**Related Commands**

None

## aaa provision route

**aaa provision route ip-netmask encapsulation** *encaps-type*

{**no** | **default**} **aaa provision route ip-netmask**

### Purpose

Enables the SmartEdge OS to install a route specified by the Remote Authentication Dial-In User Service (RADIUS) Framed-IP-Netmask attribute.

### Command Mode

context configuration

### Syntax Description

- |                                         |                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip-netmask</b>                       | Installs the subnet route specified by the RADIUS Framed-IP-Netmask attribute in the route table.                                                                                                                                                                                                                                                                                                   |
| <b>encapsulation</b> <i>encaps-type</i> | <p>Encapsulation type according to one of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>ppp</b>—Specifies Point-to-Point Protocol (PPP)-encapsulated subscriber circuits.</li> <li>• <b>pppoe</b>—Specifies PPP over Ethernet (PPPoE)-encapsulated subscriber circuits.</li> <li>• <b>ppp pppoe</b>—Specifies PPP- and PPPoE-encapsulated subscriber circuits.</li> </ul> |

### Default

The Framed-IP-Netmask attribute is ignored.

### Usage Guidelines

Use the **aaa provision route** command to enable the SmartEdge OS to install a route specified by the RADIUS Framed-IP-Netmask attribute. The subnet route specified by the Framed-IP-Netmask attribute is installed in the route table. This command is available only for PPP- or PPPoE-encapsulated circuits.

Use the **no** or **default** form of this command to ignore the Framed-IP-Netmask attribute.

### Examples

The following example enables a direct connection to PPP routers:

```
[local]Redback(config)#context remote
[local]Redback(config-ctx)#aaa provision route ip-netmask encapsulation ppp
```

### Related Commands

None



## aaa reauthorization bulk

**aaa reauthorization bulk** {global | none | radius}

{no | default} **aaa reauthorization bulk**

### Purpose

Configures subscriber reauthorization so that attribute changes can be dynamically applied to active subscriber sessions, without requiring Point-to-Point Protocol (PPP) renegotiation and without interrupting or dropping active sessions.

### Command Mode

context configuration

### Syntax Description

|               |                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>global</b> | Enables reauthorization of all subscribers in the current context through one or more Remote Authentication Dial-In User Service (RADIUS) servers with IP addresses or hostnames configured in the local context. |
| <b>none</b>   | Disables subscriber reauthorization.                                                                                                                                                                              |
| <b>radius</b> | Enables reauthorization of subscribers in the current context through one or more RADIUS servers with IP addresses or hostnames in the same context.                                                              |

### Default

None

### Usage Guidelines

Use the **aaa reauthorization bulk** command to configure subscriber reauthorization so that attribute changes can be dynamically applied to active subscriber sessions, without requiring PPP renegotiation and without interrupting or dropping active sessions. After this command has been enabled, enter the **reauthorize** command (in exec mode) to initiate subscriber reauthorization.

The standard RADIUS attributes and Redback VSAs that are supported with dynamic subscriber reauthorization are listed in Appendix A, “RADIUS Attributes.”

**Note** The SmartEdge OS appends the context name to the subscriber name when sending reauthorization messages; for example, joe@local.

**Note** You must configure at least one RADIUS server in the local or the current context before any messages can be sent to it. To configure the server, enter the **radius server** command (in context configuration mode); for more information, see Chapter 16, “RADIUS Configuration.”

**Note** To enable RADIUS authentication, you must enter the **aaa authentication subscriber** command (in context configuration mode).

Use the **no** or **default** form of this command to disable dynamic subscriber reauthorization.

### Examples

The following example enables the global reauthorization of all subscribers in the SmartEdge OS:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa reauthorization bulk global
```

The following is an example of a subscriber record on a RADIUS server. The subscriber has requested a new service that is translated to a particular session timeout value.

```
#reauth of absolute timeout
reauth-501@local User-Password=="redback"
    Service-Type=Outbound-User,
    Reauth_String="2;pppoe1@local;27;1000;"
```

Before the administrator enters the **reauthorize** command (in exec mode), the subscriber record appears as:

```
[local]Redback>show subscribers active
```

```
pppoe1@local
  Circuit 13/1 vpi-vci 0 33
  Internal Circuit 13/1:1023:63/1/2/22
  Current port-limit unlimited
  ip address 10.1.1.4
```

In the following example, the administrator enters the **reauthorize** command (in exec mode) and the subscriber session is reauthorized with the new timeout attribute added:

```
[local]Redback>reauthorize username pppoe1@local
[local]Redback>show subscribers active
```

```
pppoe1@local
  Circuit 13/1 vpi-vci 0 33
  Internal Circuit 13/1:1023:63/1/2/22
  Current port-limit unlimited
  ip address 10.1.1.4
  timeout absolute 1000
```

### Related Commands

**aaa authentication subscriber**

## aaa update subscriber

**aaa update subscriber** *interval*

{**no** | **default**} **aaa update subscriber**

### Purpose

Sends updated accounting records for subscriber sessions in the current context to one or more Remote Authentication Dial-In User Service (RADIUS) servers with IP addresses or hostnames configured in the same context.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                                      |
|-----------------|--------------------------------------------------------------------------------------|
| <i>interval</i> | Period (in minutes) between accounting updates. The range of values is 10 to 10,080. |
|-----------------|--------------------------------------------------------------------------------------|

### Default

Updates for subscriber accounts are not performed.

### Usage Guidelines

Use the **aaa update subscriber** command to send updated accounting records for subscriber sessions in the current context to one or more RADIUS servers with IP addresses or hostnames configured in the same context.

**Note** You must configure accounting using the **aaa accounting subscriber** command (in context configuration mode) with the **radius** keyword.

**Note** To use RADIUS, the IP address or hostname of at least one RADIUS accounting server must be configured in the context to which the subscriber is to be bound. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see Chapter 16, "RADIUS Configuration."

Use the **no** or **default** form of this command to disable subscriber account updating.

### Examples

The following example configures an update to be sent every 20 minutes, for as long as the subscriber session lasts:

```
[local]Redback(config-ctx)#aaa update subscriber 20
```

## Related Commands

aaa accounting subscriber  
aaa global update subscriber  
radius accounting server

## aaa username-format

**aaa username-format** {domain | username} separator

**no aaa username-format** {domain | username} separator

### Purpose

Defines one or more schemas for matching the format of structured usernames.

### Command Mode

global configuration

### Syntax Description

|                  |                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domain</b>    | Specifies that the domain portion of the structured username is to precede the user portion.                                                                                                                                                                                                                                                                               |
| <b>username</b>  | Specifies that the user portion of the structured username is to precede the domain portion.                                                                                                                                                                                                                                                                               |
| <i>separator</i> | Character that separates the user portion of the structured username from the domain portion. The possible characters are %, -, @, _, \, #, and /. To designate a backslash (\), you must enter it on the command line as two backslashes (\\). A single backslash has a reserved meaning in the SmartEdge OS. A maximum of six characters can be used in a single schema. |

### Default

If no username formats are specified with this command, the SmartEdge OS default format of *username@domain-name* is checked for a format match.

### Usage Guidelines

Use the **aaa username-format** command to define one or more schemas for matching the format of structured usernames. A username can be for a subscriber or an administrator.

You can use this command multiple times to create a list of formats against which an incoming username is matched. The first format configured is checked first for a match, then the second, and so on until a match is found, or until the configured username formats are exhausted.

If no username formats are explicitly defined with the **aaa username-format** command, the SmartEdge OS checks the default format of *username@domain-name* for a match.

Use the **no** form of this command to remove the specified format from those considered to be valid structured-username formats.

### Examples

The following example configures a structured-username format with the subscriber name specified first, separated from its domain by the % symbol:

```
[local]Redback(config)#aaa username-format username %
```

In this example, for a subscriber, joe, configured in the local context, the SmartEdge OS checks for a match against the structured-username joe%local.

The following example configures a structured-username format with the domain name specified first, separated from the subscriber name by the / symbol:

```
[local]Redback(config)#aaa username-format domain /
```

In this example, for a subscriber, joe, configured in the local context, the SmartEdge OS checks for a match against the format local/joe.

### Related Commands

**aaa authentication subscriber**

**aaa global authentication subscriber**

# RADIUS Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS Remote Authentication Dial-In User Service (RADIUS) features.

For information about RADIUS attributes, see Appendix A, “RADIUS Attributes.”

For information about tasks and commands used to monitor, troubleshoot, and administer RADIUS, see the “RADIUS Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

The RADIUS protocol, which is based on a client/server architecture, enables the building of a system that secures remote access to networks and network services. When configured with the IP address or hostname of a RADIUS server, the SmartEdge router can act as a RADIUS client.

To enable authentication through RADIUS, you must also configure authentication, authorization, and accounting (AAA); for more information, see Chapter 15, “AAA Configuration.”

In addition to providing authentication, a RADIUS server can collect and store accounting data for subscriber sessions. You can configure a single server that provides both authentication and accounting functions, or you can configure separate authentication versus accounting servers.

Load balancing between multiple servers is valuable in situations where the number of sessions being established and terminated per second is large, and a single RADIUS server is unable to handle the load.

Two load-balancing algorithms are supported:

- Strict-priority—Requests are always sent first to the first server configured in the SmartEdge OS, and, if the request fails, the requests are sent to the next server, and so on.
- Round-robin priority—Requests are sent to the server following the one where the last request was sent; if the SmartEdge OS receives no response from the server, requests are sent to the next server, and so on.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure RADIUS, perform the tasks described in the following sections:

- Configure the Server IP Address or Hostname
- Configure an IP Source Address (Optional)
- Configure Load Balancing Between RADIUS Servers (Optional)
- Modify RADIUS Connection Parameters (Optional)
- Strip the Domain Portion of Structured Usernames (Optional)
- Change the Server Source Port Value (Optional)
- Configure and Assign a RADIUS Policy to a Context (Optional)
- Configure and Send Attributes in RADIUS Packets (Optional)
- Remap Account Termination Codes (Optional)

### Configure the Server IP Address or Hostname

To configure the IP address or hostname of a RADIUS accounting server or RADIUS server, perform the appropriate task described in Table 16-1. Enter all commands in context configuration mode.

**Table 16-1** Configure the Server IP Address or Hostname

| Task                                                           | Root Command                    | Notes                                                                                                                                                                                      |
|----------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure the RADIUS accounting server IP address or hostname. | <b>radius accounting server</b> | To enable accounting through RADIUS, you must also enter the <b>aaa accounting subscriber radius</b> command (in context configuration mode); see Chapter 15, “AAA Configuration.”         |
| Configure the RADIUS server IP address or hostname.            | <b>radius server</b>            | To enable authentication through RADIUS, you must also enter the <b>aaa authentication subscriber radius</b> command (in context configuration mode); see Chapter 15, “AAA Configuration.” |



## Configure an IP Source Address (Optional)

By default, the local IP address of the interface on which RADIUS is transmitted is included in the IP header of RADIUS packets sent by the SmartEdge router. To not publish the IP address to the RADIUS server, you can configure a loopback interface to appear to be the source address for RADIUS packets as described in Table 16-2.

**Table 16-2 Configure an IP Source Address**

| Task                            | Root Command                    | Notes                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure an IP source address. | <b>ip source-address radius</b> | Enter this command in interface configuration mode. The interface must be reachable by the RADIUS server; for command details, see the "Interface Configuration" chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS. |

## Configure Load Balancing Between RADIUS Servers (Optional)

To load balance between multiple RADIUS accounting or RADIUS servers, perform the appropriate task described in Table 16-3. Enter all commands in context configuration mode.

**Table 16-3 Configure Load Balancing Between RADIUS Servers**

| Task                                                                                | Root Command                       | Notes |
|-------------------------------------------------------------------------------------|------------------------------------|-------|
| Specify a load-balancing algorithm to use among multiple RADIUS accounting servers. | <b>radius accounting algorithm</b> |       |
| Specify a load-balancing algorithm to use among multiple RADIUS servers.            | <b>radius algorithm</b>            |       |

## Modify RADIUS Connection Parameters (Optional)

To configure how the SmartEdge router responds to connections with RADIUS servers or RADIUS accounting servers, perform the tasks described in the following sections:

- Send Accounting On and Off Messages
- Modify RADIUS Timeout Parameters

### Send Accounting On and Off Messages

To send "accounting on" or "accounting off" messages to any other RADIUS servers that are configured in the current context when a RADIUS server is added or removed, perform the task described in Table 16-4.

**Table 16-4 Send Accounting On and Off Messages**

| Task                                                                                                                                                                                                            | Root Command                              | Notes                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------------------------------------------------|
| When an accounting server is added to or removed from the configuration, send an accounting on or accounting off message, respectively, to any other RADIUS servers that are configured in the current context. | <b>radius accounting send-acct-on-off</b> | Enter this command in context configuration mode. By default, the SmartEdge OS sends these messages. |

## Modify RADIUS Timeout Parameters

RADIUS timeout parameters allow you to configure three different intervals that are used by the system to manage responses when a RADIUS server is not responding. Table 16-5 presents a timeline that describes the intervals and how you can configure them.

**Table 16-5 RADIUS Timeout Intervals**

| Time        | RADIUS Action                                                                                  | Interval Set By                                                         |
|-------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| T0          | Sends a request to a RADIUS server and sets a time for interval T1.                            | <b>radius timeout</b><br><b>radius accounting timeout</b>               |
| T0+T1       | T1 expires. Assumes packet is lost or server is unreachable; sets a timer for interval T2.     | <b>radius server-timeout</b><br><b>radius accounting server-timeout</b> |
| T0+T1+T2    | T2 expires. Marks the server as “dead” and tries another server; sets a timer for interval T3. | <b>radius deadtime</b><br><b>radius accounting deadtime</b>             |
| T0+T1+T2+T3 | T3 expires. Sends another request to the first server.                                         | —                                                                       |

To modify the RADIUS timeout parameters that the SmartEdge OS uses for managing the connections to and from RADIUS servers and RADIUS accounting servers, perform the appropriate tasks described in Table 16-6. Enter all commands in context configuration mode.

**Table 16-6 Modify RADIUS Timeout Parameters**

| #  | Task                                                                                                                          | Root Command                            | Notes                                         |
|----|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------------------|
| 1. | Optional. Modify the interval that the SmartEdge OS waits for a response from a RADIUS server after sending a packet:         |                                         |                                               |
|    | For a RADIUS accounting server.                                                                                               | <b>radius accounting timeout</b>        |                                               |
|    | For a RADIUS server.                                                                                                          | <b>radius timeout</b>                   |                                               |
| 2. | Optional. Modify the maximum number of retransmission attempts during the timeout interval:                                   |                                         |                                               |
|    | For a RADIUS accounting server.                                                                                               | <b>radius accounting max-retries</b>    |                                               |
|    | For a RADIUS server.                                                                                                          | <b>radius max-retries</b>               |                                               |
| 3. | Optional. Modify the interval that the SmartEdge OS waits for a response before marking a non-responsive server “dead”:       |                                         |                                               |
|    | For a RADIUS accounting server.                                                                                               | <b>radius accounting server-timeout</b> | Setting the value to 0 disables the feature.  |
|    | For a RADIUS server.                                                                                                          | <b>radius server-timeout</b>            |                                               |
| 4. | Optional. Modify the interval that the SmartEdge OS treats a non-responsive server as “dead” before trying to reach it again: |                                         |                                               |
|    | For a RADIUS accounting server.                                                                                               | <b>radius accounting deadtime</b>       | Setting this value to 0 disables the feature. |
|    | For a RADIUS server.                                                                                                          | <b>radius deadtime</b>                  |                                               |

**Table 16-6 Modify RADIUS Timeout Parameters** (*continued*)

| #  | Task                                                                  | Root Command                             | Notes |
|----|-----------------------------------------------------------------------|------------------------------------------|-------|
| 5. | Optional. Modify the number of outstanding requests that can be sent: |                                          |       |
|    | For a RADIUS accounting server.                                       | <b>radius accounting max-outstanding</b> |       |
|    | For a RADIUS server.                                                  | <b>radius max-outstanding</b>            |       |

## Strip the Domain Portion of Structured Usernames (Optional)

To specify that the domain portion of structured usernames is to be removed before sending the usernames to a RADIUS server for authentication, perform the task described in Table 16-7.

**Table 16-7 Strip the Domain Portion of Structured Usernames**

| Task                                              | Root Command               | Notes                                             |
|---------------------------------------------------|----------------------------|---------------------------------------------------|
| Strip the domain portion of structured usernames. | <b>radius strip-domain</b> | Enter this command in context configuration mode. |

## Change the Server Source Port Value (Optional)

To increase the number of outstanding authentication requests per RADIUS server by sending the requests, using a different source port value, perform the task described in Table 16-8.

**Table 16-8 Change the Server Source Port Value**

| Task                                 | Root Command              | Notes                                             |
|--------------------------------------|---------------------------|---------------------------------------------------|
| Change the server source port value. | <b>radius source-port</b> | Enter this command in context configuration mode. |

## Configure and Assign a RADIUS Policy to a Context (Optional)

To configure and assign a RADIUS policy to a context, perform the tasks described in Table 16-9.

**Table 16-9 Configure and Assign a RADIUS Policy to a Context**

| #  | Task                                                                                                     | Root Command         | Notes                                                   |
|----|----------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------|
| 1. | Create or modify a RADIUS policy and access RADIUS policy configuration mode.                            | <b>radius policy</b> | Enter this command in global configuration mode.        |
| 2. | Specify the RADIUS attribute or VSA, and optionally the RADIUS messages, from which it is to be dropped. | <b>attribute</b>     | Enter this command in RADIUS policy configuration mode. |
| 3. | Assign the policy to a context.                                                                          | <b>radius policy</b> | Enter this command in context configuration mode.       |

## Configure and Send Attributes in RADIUS Packets (Optional)

To configure and send attributes in RADIUS request packets, perform one or more of the tasks described in Table 16-10. Enter all commands in context configuration mode, unless otherwise noted.

**Table 16-10 Configure and Send Attributes in RADIUS Request Packets**

| Task                                                                                                                                                                                       | Root Command                               | Notes                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Send the Acct-Delay-Time attribute in RADIUS Access-Request and Accounting-Request packets.                                                                                                | <b>radius attribute acct-delay-time</b>    | By default, this attribute is not sent.                                                                                                                                                                                                                                              |
| Send the Acct-Session-Id attribute in RADIUS Access-Request packets.                                                                                                                       | <b>radius attribute acct-session-id</b>    | By default, this attribute is sent only in Accounting-Request packets.                                                                                                                                                                                                               |
| Send the Calling-Station-Id attribute in RADIUS Access-Request and Accounting-Request packets.                                                                                             | <b>radius attribute calling-station-id</b> | By default, this attribute is not sent.                                                                                                                                                                                                                                              |
| Specify the behavior of the SmartEdge OS when it receives a RADIUS Filter-Id attribute that does not specify a direction and there is an access control list (ACL) applied to the circuit. | <b>radius attribute filter-id</b>          |                                                                                                                                                                                                                                                                                      |
| Send the NAS-IP-Address attribute in RADIUS Access-Request and Accounting-Request packets.                                                                                                 | <b>radius attribute nas-ip-address</b>     | By default, this attribute is not sent.                                                                                                                                                                                                                                              |
| Modify the format in which the NAS-Port attribute is sent in RADIUS Access-Request and Accounting-Request packets.                                                                         | <b>radius attribute nas-port</b>           | By default, this attribute is sent using the <b>slot-port</b> format.                                                                                                                                                                                                                |
| Modify the format in which the NAS-Port-Id attribute is sent in RADIUS Access-Request and Accounting-Request packets.                                                                      | <b>radius attribute nas-port-id</b>        | By default, this attribute is sent using the <b>all</b> format.                                                                                                                                                                                                                      |
| Modify the value of the NAS-Port-Type attribute sent in RADIUS Access-Request and Accounting-Request packets.                                                                              | <b>radius attribute nas-port-type</b>      | Enter this command in ATM profile, dot1q profile, or port configuration mode.<br>By default, this attribute is sent using a value of either 0 or 5, indicating an asynchronous connection through a console port or a virtual connection through a transport protocol, respectively. |
| Specify the character the SmartEdge OS uses to separate the fields for the medium access control (MAC) addresses in the Redback VSA 145, Mac-Addr.                                         | <b>radius attribute vendor-specific</b>    |                                                                                                                                                                                                                                                                                      |

## Remap Account Termination Codes (Optional)

When a subscriber session is terminated, the system reports the reason for the termination to RADIUS, using one of several terminate cause codes that are defined in RFC 2866, *RADIUS Accounting*, in attribute 49 (Acct-Terminate-Cause). Because the set of codes defined for RADIUS attribute 49 is very limited, the SmartEdge OS defines a more extensive set of terminate cause codes to more precisely indicate the reason for the termination. The system transmits these codes in Redback VSA 142 (Session-Error-Code) and 143 (Session-Error-message).

Terminate error codes and their RADIUS attribute 49 error codes are listed in the “RADIUS Attribute 49 Error Codes” appendix in the *IP Services and Security Operations Guide* for the SmartEdge OS. You can change the RADIUS attribute 49 error code for a Redback terminate cause code to different attribute 49 error code. To remap an Redback terminate error code to a different RADIUS attribute 49 error code, perform the tasks described in Table 16-11.

**Table 16-11 Remap Redback Terminate Error Codes**

| #  | Task                                                                                                         | Root Command                                       | Notes                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 1. | Enable the remapping of account termination error codes and access terminate error cause configuration mode. | <b>radius attribute acct-terminate-cause remap</b> | Enter this command in global configuration mode.                                                                             |
| 2. | Remap a Redback terminate error code to a different RADIUS attribute 49 error code.                          | <b>rbak-term-ec</b>                                | Enter this command in terminate error cause configuration mode for each Redback terminate error code that you want to remap. |

## Configuration Examples

The following example configures the IP address of the RADIUS server, 10.43.32.56, using the key, Secret, and configures related behaviors of the SmartEdge OS:

```
[local]Redback(config-ctx)#radius server 10.43.32.56 key Secret
[local]Redback(config-ctx)#radius max-retries 5
[local]Redback(config-ctx)#radius timeout 30
```

The following example configures the interface at IP address, 108.1.1.1, to connect to the RADIUS server; however, a loopback interface is also configured using IP address, 11.200.1.1, which is sent to the RADIUS server as the source IP address for RADIUS packets.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to-radius-server
[local]Redback(config-if)#ip address 108.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface loop1 loopback
[local]Redback(config-if)#ip address 11.200.1.1/32
[local]Redback(config-if)#ip source-address radius
```

The following example creates the custom RADIUS policy to drop RADIUS attribute 123 in all RADIUS messages, Redback VSA 10 in Access-Request messages, and Redback VSAs 11 and 12 in various Accounting messages, and then assigns it to the gold-isp context:

```
[local]Redback(config)#radius policy name custom
[local]Redback(config-rad-policy)#attribute 123 drop
[local]Redback(config-rad-policy)#attribute rbak 10 drop access-request
[local]Redback(config-rad-policy)#attribute rbak 11 drop acct-start acct-update
[local]Redback(config-rad-policy)#attribute rbak 12 drop acct-start acct-stop
[local]Redback(config-rad-policy)#exit
[local]Redback(config)#context gold-isp
[local]Redback(config-ctx)#radius policy custom
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure RADIUS. The commands are presented in alphabetical order.

|                                                    |                                         |
|----------------------------------------------------|-----------------------------------------|
| <b>attribute</b>                                   | <b>radius attribute nas-ip-address</b>  |
| <b>radius accounting algorithm</b>                 | <b>radius attribute nas-port</b>        |
| <b>radius accounting deadline</b>                  | <b>radius attribute nas-port-id</b>     |
| <b>radius accounting max-outstanding</b>           | <b>radius attribute nas-port-type</b>   |
| <b>radius accounting max-retries</b>               | <b>radius attribute vendor-specific</b> |
| <b>radius accounting send-acct-on-off</b>          | <b>radius deadline</b>                  |
| <b>radius accounting server</b>                    | <b>radius max-outstanding</b>           |
| <b>radius accounting server-timeout</b>            | <b>radius max-retries</b>               |
| <b>radius accounting timeout</b>                   | <b>radius policy</b>                    |
| <b>radius algorithm</b>                            | <b>radius server</b>                    |
| <b>radius attribute acct-delay-time</b>            | <b>radius server-timeout</b>            |
| <b>radius attribute acct-session-id</b>            | <b>radius source-port</b>               |
| <b>radius attribute acct-terminate-cause remap</b> | <b>radius strip-domain</b>              |
| <b>radius attribute calling-station-id</b>         | <b>radius timeout</b>                   |
| <b>radius attribute filter-id</b>                  | <b>rbak-term-ec</b>                     |

## attribute

```
attribute [vendor-specific {rbak | vendor-num}] {attribute-name | attribute-num}
        drop [msg-type-1 ... msg-type-n]
{no | default} [vendor-specific {rbak | vendor-num}] attribute-num
```

### Purpose

Specifies one or more Remote Authentication Dial-In User Service (RADIUS) messages in which the specified attribute is to be dropped.

### Command Mode

RADIUS policy configuration

### Syntax Description

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vendor-specific</b>                     | Optional. Specifies a vendor-specific attribute (VSA) instead of a RADIUS standard attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>rbak</b>                                | Specifies that the attribute is a Redback VSA. Required only if you enter the <b>vendor-specific</b> keyword.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <i>vendor-num</i>                          | Specifies that the attribute is a VSA of another vendor. Required only if you enter the <b>vendor-specific</b> keyword.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <i>attribute-name</i>                      | RADIUS attribute or VSA name. See Appendix A, “RADIUS Attributes,” for the supported RADIUS standard attributes and Redback VSAs. See the online help in the command-line interface (CLI) for the keywords to use for these RADIUS standard attributes and Redback VSAs.                                                                                                                                                                                                                                                                         |
| <i>attribute-num</i>                       | RADIUS attribute or VSA number. See Appendix A, “RADIUS Attributes,” for the numbers of supported RADIUS standard attributes and Redback VSAs.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>drop</b>                                | Specifies one or more attributes to be dropped. Not entered in the <b>no</b> form.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <i>msg-type-1</i> ...<br><i>msg-type-n</i> | Optional. One or more RADIUS message types in which the attribute is to be removed, according to one of the following keywords: <ul style="list-style-type: none"> <li>• <b>access-request</b>—Access-Request message.</li> <li>• <b>acct-start</b>—Accounting-Request message.</li> <li>• <b>acct-stop</b>—Access-Request message.</li> <li>• <b>acct-update</b>—Access-Request message.</li> </ul> <p>If not specified, the attribute is dropped from all types of RADIUS messages in which it appears. Not entered in the <b>no</b> form.</p> |

### Default

This RADIUS attribute or the VSA is not dropped from any RADIUS message in which it appears.

### Usage Guidelines

Use the **attribute** command to specify one or more RADIUS messages in which the specified attribute is to be dropped.

You can specify the attribute using either the *attribute-name* or *attribute number* argument. If the name for a standard RADIUS attribute or Redback VSA is listed in Appendix A, “RADIUS Attributes,” but its name is not listed in the online help for the CLI, enter the number.

**Note** The online help for the CLI includes all RADIUS standard attributes and Redback VSAs, some of which are not supported by the SmartEdge OS.

You can specify any or all message types, separated by spaces, in a single instance of the command, or you can enter them individually.

Use the **no** or **default** form of this command to restore this RADIUS attribute or VSA to any RADIUS message in which it appears.

### Examples

The following example creates the custom RADIUS policy to drop RADIUS attribute 123 in all RADIUS messages and Redback VSA 10 in Access-Request messages:

```
[local]Redback(config)#radius policy name custom
[local]Redback(config-rad-policy)#attribute 123 drop
[local]Redback(config-rad-policy)#attribute rbak 10 drop access-request
```

### Related Commands

**radius policy**



## radius accounting algorithm

**radius accounting algorithm {first | round-robin}**

**no radius accounting algorithm**

### Purpose

Specifies a load-balancing algorithm to use among multiple Remote Authentication Dial-In User Service (RADIUS) accounting servers.

### Command Mode

context configuration

### Syntax Description

|                    |                                                                            |
|--------------------|----------------------------------------------------------------------------|
| <b>first</b>       | Specifies that the first configured RADIUS server is always queried first. |
| <b>round-robin</b> | Specifies that RADIUS servers are queried in round-robin fashion.          |

### Default

The SmartEdge router uses the first configured RADIUS server first.

### Usage Guidelines

Use the **radius accounting algorithm** command to specify a load-balancing algorithm to use among multiple RADIUS accounting servers.

Use the **no** form of this command to reset the load-balancing algorithm to use the first configured RADIUS server first.

### Example

The following example sets the load-balancing algorithm to round-robin:

```
[local]Redback(config-ctx)#radius accounting algorithm round-robin
```

### Related Commands

**aaa accounting subscriber**  
**radius accounting max-outstanding**  
**radius accounting max-retries**  
**radius accounting server**  
**radius accounting timeout**

## radius accounting deadtime

**radius accounting deadtime** *interval*

**default radius accounting deadtime**

### Purpose

Sets the interval during which the SmartEdge OS treats a nonresponsive Remote Authentication Dial-In User Service (RADIUS) accounting server as “dead”.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| <i>interval</i> | Deadtime interval in minutes. The range of values is 0 to 65,535; the default value is 5. The 0 value disables the feature. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|

### Default

The waiting interval is five minutes.

### Usage Guidelines

Use the **radius accounting deadtime** command to set the interval during which the SmartEdge OS treats a nonresponsive RADIUS accounting server as “dead”. During the interval, the SmartEdge OS tries to reach another RADIUS accounting server; after the interval expires, the SmartEdge OS tries again to reach the accounting server. If there is no response, the RADIUS accounting server remains marked as “dead” and the timer is set again to the configured interval.

If you disable this feature (with the 0 value), the SmartEdge OS never waits but attempts to reach the server immediately.

**Note** You must configure at least one RADIUS accounting server using the **radius accounting server** command (in context configuration mode) prior to entering this command.

Use the **default** form of this command to specify the default interval.

### Examples

The following example sets the deadtime interval to 10 minutes:

```
[local]Redback(config-ctx)#radius accounting deadtime 10
```

### Related Commands

**radius accounting server**  
**radius accounting server-timeout**  
**radius accounting timeout**

## radius accounting max-outstanding

**radius accounting max-outstanding** *requests*

{**no** | **default**} **radius accounting max-outstanding**

### Purpose

Modifies the number of simultaneous outstanding accounting requests that can be sent by the SmartEdge router to Remote Authentication Dial-In User Service (RADIUS) accounting servers.

### Command Mode

context configuration

### Syntax Description

*requests*

Number of simultaneous outstanding requests per RADIUS server in the current context. The range of values is 1 to 256.

### Default

The number of simultaneous outstanding accounting requests sent by the SmartEdge router is 256.

### Usage Guidelines

Use the **radius accounting max-outstanding** to modify the number of simultaneous outstanding accounting requests that can be sent by the SmartEdge router to RADIUS accounting servers.

Use this command if the RADIUS servers cannot handle the default of 256 simultaneous outstanding accounting requests that the SmartEdge router can send to RADIUS accounting servers configured within the context.

Use the **no** or **default** form of this command to reset the maximum number of allowable outstanding requests to 256.

### Examples

The following example limits the number of simultaneous outstanding requests to 128:

```
[local]Redback(config-ctx)#radius accounting max-outstanding 128
```

### Related Commands

**aaa accounting subscriber**  
**radius accounting algorithm**  
**radius accounting max-retries**  
**radius accounting server**  
**radius accounting timeout**

## radius accounting max-retries

**radius accounting max-retries** *retries*

**default radius accounting max-retries**

### Purpose

Modifies the number of retransmission attempts the SmartEdge router makes to a Remote Authentication Dial-In User Service (RADIUS) server in the event that no response is received from the server within the timeout period.

### Command Mode

context configuration

### Syntax Description

|                |                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>retries</i> | Number of times the SmartEdge router retransmits a RADIUS accounting packet. The range of values is 1 to 2,147,483,647; the default value is 3. |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

The SmartEdge router sends three retransmissions.

### Usage Guidelines

Use the **radius accounting max-retries** command to modify the number of retransmission attempts the SmartEdge router makes to a RADIUS accounting server in the event that no response is received from the server within the timeout period.

If an acknowledgment is not received, each successive, configured server is tried (wrapping from the last server to the first, if necessary) until the maximum number of retransmissions is reached.

Use the **default** form of this command to reset the number of retries to 3.

### Example

The following example sets the retransmit value to 5:

```
[local]Redback(config-ctx)#radius accounting max-retries 5
```

The following example resets the retransmit value to the default of 3:

```
[local]Redback(config-ctx)#default radius accounting max-retries
```

### Related Commands

**aaa accounting subscriber**  
**radius accounting algorithm**

**radius accounting max-outstanding**

**radius accounting server**  
**radius accounting timeout**

## radius accounting send-acct-on-off

**radius accounting send-acct-on-off**

**no radius accounting send-acct-on-off**

**default radius accounting send-acct-on-off**

### Purpose

Enables the sending of “accounting on” and “accounting off” messages to all Remote Authentication Dial-In User Service (RADIUS) accounting servers that are configured in the current context.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

Accounting on and accounting off messages are sent.

### Usage Guidelines

Use the **radius accounting send-acct-on-off** command to enable the sending of accounting on and accounting off messages to all RADIUS accounting servers that are configured in the current context. Messages are sent under the following conditions:

- The SmartEdge OS sends an accounting on message when accounting is enabled in the context; the message is sent to all RADIUS accounting servers configured in the context.
- The SmartEdge OS sends an accounting on message when a RADIUS accounting server is added to the context; the message is sent only to the server just added.
- The SmartEdge OS sends an accounting off message accounting is disabled in the context; the message is sent to all RADIUS accounting servers configured in the context.
- The SmartEdge OS sends an accounting off message when a RADIUS accounting server is removed from the context; the message is sent only to the server just removed.

**Note** The SmartEdge OS attempts to send a single accounting on message when more than one type of RADIUS accounting is enabled. For example, if you enable both subscriber accounting and L2TP accounting, the SmartEdge OS sends a single accounting on message to each RADIUS accounting server, even if you enable L2TP accounting at a later time.

Similarly, the accounting off message is not sent until you have disabled all types of RADIUS accounting.

Use the **no** form of this command to prevent the SmartEdge router from sending these messages.

Use the **default** form of this command to return the system to its default behavior.

### Examples

The following example disables the sending of accounting on and off messages to all other RADIUS accounting servers in the `local` context:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#no radius send-acct-on-off
```

### Related Commands

**radius accounting server**

## radius accounting server

**radius accounting server** {*ip-addr* | *hostname*} **key** *key* [**oldports** | **port** *udp-port*]

**no radius accounting server**

### Purpose

Configures the IP address or hostname of a Remote Authentication Dial-In User Service (RADIUS) accounting server.

### Command Mode

context configuration

### Syntax Description

|                             |                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>              | IP address of the RADIUS accounting server.                                                                             |
| <i>hostname</i>             | Hostname of the RADIUS accounting server. Domain Name System (DNS) must be enabled to use the <i>hostname</i> argument. |
| <b>key</b> <i>key</i>       | Authentication key used when communicating with the accounting server.                                                  |
| <b>oldports</b>             | Optional. Designates the old RADIUS User Datagram Protocol (UDP) port 1646.                                             |
| <b>port</b> <i>udp-port</i> | Optional. RADIUS accounting UDP port. The range of values is 1 to 65,536; the default value is 1813.                    |

### Default

RADIUS accounting server hostnames and IP addresses are not preconfigured. The UDP accounting port is 1813.

### Usage Guidelines

Use the **radius accounting server** command to configure the IP address or hostname of a RADIUS accounting server. Use this command multiple times to configure up to five RADIUS accounting servers per context. To use the *hostname* argument, you must enable DNS; for more information, see Chapter 6, “DNS Configuration.”

**Note** To enable accounting to be performed by RADIUS, you must also enter the **aaa accounting subscriber** command (in context configuration mode); for more information, see Chapter 15, “AAA Configuration.”

Use the **no** form of this command to delete a previously configured RADIUS accounting server.

### Examples

The following example configures a RADIUS accounting server IP address of 10.3.3.3 with the key, secret, using port 4445 for accounting:

```
[local]Redback(config-ctx)#radius accounting server 10.3.3.3 key secret port 4445
```

## Related Commands

aaa accounting subscriber  
radius accounting algorithm  
radius accounting max-outstanding  
radius accounting max-retries  
radius accounting timeout



## radius accounting server-timeout

**radius accounting server-timeout** *interval*

**default radius accounting server-timeout**

### Purpose

Sets the time interval the SmartEdge OS waits before marking a non-responsive Remote Authentication Dial-In User Service (RADIUS) accounting server as “dead”.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                                                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interval</i> | Time period that the SmartEdge OS checks back for successful responses, after an individual RADIUS request times out, before treating the accounting server as “dead”. The range of values is 0 to 2, 147,483, 647 seconds; the default value is 60 seconds. |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

The maximum time interval is 60 seconds.

### Usage Guidelines

Use the **radius accounting server-timeout** command to set the time interval the SmartEdge OS waits before marking a non-responsive RADIUS accounting server as “dead”.

The SmartEdge OS marks a RADIUS accounting server as “dead” when no response is received to any RADIUS requests during the time period specified by the *interval* argument. Setting the value to 0 disables this feature; in this case, no RADIUS accounting server is marked as “dead”.

Use the **default** form of this command to specify the default interval.

### Examples

The following example sets the waiting interval to 80 seconds:

```
[local]Redback(config-ctx)#radius accounting server-timeout 80
```

### Related Commands

**radius accounting deadtime**

**radius accounting timeout**

## radius accounting timeout

**radius accounting timeout** *timeout*

**default radius accounting timeout**

### Purpose

Sets the maximum time the SmartEdge OS waits for a response from a Remote Authentication Dial-In User Service (RADIUS) accounting server before assuming that a packet is lost, or that the RADIUS accounting server is unreachable.

### Command Mode

context configuration

### Syntax Description

|                |                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------|
| <i>timeout</i> | Timeout period in seconds. The range of values is 1 to 2,147,483,647; the default value is 10 seconds. |
|----------------|--------------------------------------------------------------------------------------------------------|

### Default

The maximum time is 10 seconds.

### Usage Guidelines

Use the **radius accounting timeout** command to set the maximum time the SmartEdge router waits for a response from a RADIUS accounting server before assuming that a packet is lost, or that the RADIUS accounting server is unreachable.

Use the **default** form of this command to specify the default interval.

### Examples

The following example sets the timeout interval to 30 seconds:

```
[local]Redback(config-ctx)#radius accounting timeout 30
```

### Related Commands

- aaa accounting subscriber**
- radius accounting algorithm**
- radius accounting max-outstanding**
- radius accounting max-retries**
- radius accounting server**

# radius algorithm

**radius algorithm {first | round-robin}**

**default radius algorithm**

## Purpose

Specifies the algorithm to use among multiple Remote Authentication Dial-In User Service (RADIUS) servers.

## Command Mode

context configuration

## Syntax Description

|                    |                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------|
| <b>first</b>       | Specifies that the first configured RADIUS server is always queried first.                     |
| <b>round-robin</b> | Specifies that the RADIUS servers are queried in round-robin fashion, enabling load balancing. |

## Default

The SmartEdge router queries the first configured server first.

## Usage Guidelines

Use the **radius algorithm** command to specify the algorithm to use among multiple RADIUS servers.

Use the **default** form of this command to reset the SmartEdge router to query the first configured RADIUS server first.

## Examples

The following example sets the algorithm to round-robin:

```
[local]Redback(config-ctx)#radius algorithm round-robin
```

## Related Commands

**aaa authentication subscriber**  
**radius max-outstanding**  
**radius max-retries**  
**radius server**  
**radius source-port**  
**radius strip-domain**  
**radius timeout**

## radius attribute acct-delay-time

**radius attribute acct-delay-time**

**{no | default} radius attribute acct-delay-time**

### Purpose

Sends the Acct-Delay-Time attribute in Remote Authentication Dial-In User Service (RADIUS) Access-Request packets for the current context.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

The Acct-Delay-Time attribute is only sent in Accounting-Request packets.

### Usage Guidelines

Use the **radius attribute acct-delay-time** command to send the Acct-Delay-Time attribute in RADIUS Access-Request packets for the current context.

Standard RADIUS attribute 40, Acct-Delay-Time, is described in Appendix A, “RADIUS Attributes.”

Use the **no** or **default** form of this command to disable the sending of the Acct-Delay-Time attribute in Access-Request packets.

### Examples

The following example configures the SmartEdge OS to send the Acct-Delay-Time attribute in RADIUS Access-Request packets:

```
[local]Redback(config-ctx)#radius attribute acct-delay-time
```

### Related Commands

**radius attribute acct-session-id**  
**radius attribute calling-station-id**  
**radius attribute nas-ip-address**  
**radius attribute nas-port**  
**radius attribute nas-port-id**  
**radius attribute nas-port-type**

## radius attribute acct-session-id

**radius attribute acct-session-id access-request**

**{no | default} radius attribute acct-session-id access-request**

### Purpose

Sends the Acct-Session-Id attribute in Remote Authentication Dial-In User Service (RADIUS) Access-Request packets for the current context.

### Command Mode

context configuration

### Syntax Description

|                       |                                                                       |
|-----------------------|-----------------------------------------------------------------------|
| <b>access-request</b> | Specifies that the attribute is to be sent in Access-Request packets. |
|-----------------------|-----------------------------------------------------------------------|

### Default

The Acct-Session-Id attribute is only sent in Accounting-Request packets.

### Usage Guidelines

Use the **radius attribute acct-session-id** command to send the Acct-Session-Id attribute in RADIUS Access-Request packets for the current context.

This command affects only subscriber sessions, not administrator sessions.

Standard RADIUS attribute 41, Acct-Session-Id, is described in Appendix A, “RADIUS Attributes.”

Use the **no** or **default** form of this command to disable the sending of the Acct-Session-Id attribute in Access-Request packets.

### Examples

The following example configures the SmartEdge OS to send the Acct-Session-Id attribute in RADIUS access-request packets:

```
[local]Redback(config-ctx)#radius attribute acct-session-id access-request
```

### Related Commands

**radius attribute calling-station-id**  
**radius attribute nas-ip-address**  
**radius attribute nas-port**  
**radius attribute nas-port-id**  
**radius attribute nas-port-type**

## radius attribute acct-terminate-cause remap

**radius attribute acct-terminate-cause remap**

**no radius attribute acct-terminate-cause remap**

### Purpose

Enables the remapping of Redback account termination error codes and accesses terminate error cause configuration mode.

### Command Mode

global configuration

### Syntax Description

This command has no keywords or attributes.

### Default

Remapping of account termination error codes is disabled.

### Usage Guidelines

Use the **radius attribute acct-terminate cause remap** command to enable the remapping of Redback account termination error codes and access terminate error cause configuration mode. By default, the SmartEdge OS maps a Redback termination error code to a Remote Authentication Dial-In User Service (RADIUS) Attribute 49 (Acct-Terminate-Cause) terminate cause error code, which it sends in RADIUS Accounting-Stop packets. RADIUS attribute 49 terminate cause error codes and their definitions are included in RFC 2866, *RADIUS Accounting*. The “RADIUS Attribute 49 Error Codes” appendix in the *IP Services and Security Operations Guide* for the SmartEdge OS lists the default mapping of Redback account termination error codes to RADIUS attribute 49 error codes.

Use the **no** form of this command to remove the remapping of all Redback account termination error codes.

### Examples

The following example enables the remapping of Redback account termination error codes:

```
[local]Redback(config)#radius attribute acct-terminate-cause remap
[local]Redback(config-term-ec)#
```

### Related Commands

**rbak-term-ec**

## radius attribute calling-station-id

```
radius attribute calling-station-id {format {agent-circuit-id [remote-agent-id] | description |
hostname {agent-circuit-id [remote-agent-id] | remote-agent-id} | remote-agent-id |
slot-port [agent-circuit-id [remote-agent-id] | remote-agent-id}} | separator separator}
```

**no radius attribute calling-station-id format**

**default radius attribute calling-station-id separator** *separator*

### Purpose

Using the specified format, sends the Calling-Station-Id attribute in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets for the current context.

### Command Mode

context configuration

### Syntax Description

|                                   |                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>format</b>                     | Indicates a particular format to be applied.                                                                                                                                                                                                                                        |
| <b>agent-circuit-id</b>           | Specifies that the format or the type of the information for the Calling-Station-Id attribute is Agent-Circuit-Id. Optional only when specifying the <b>slot-port</b> keyword.                                                                                                      |
| <b>remote-agent-id</b>            | Optional. Specifies that the format or the type of the information for the Calling-Station-Id attribute is Agent-Remote-Id. Optional only when specifying the <b>agent-circuit-id</b> keyword.                                                                                      |
| <b>description</b>                | Specifies a circuit description format using the information configured with the <b>description</b> command in the configuration mode for the circuit with the hostname prepended to it.                                                                                            |
| <b>hostname</b>                   | Prepends the SmartEdge router hostname to the contents of the Calling-Station-Id attribute in RADIUS packets. The hostname is either the one that has been configured using the <b>system hostname</b> command (in context configuration mode), or the default hostname, “Redback”. |
| <b>slot-port</b>                  | Specifies a slot number/port number format that has the hostname prepended to it.                                                                                                                                                                                                   |
| <b>separator</b> <i>separator</i> | Character that separates the elements of the attribute string. The default separator character is the number symbol (#).                                                                                                                                                            |

### Default

The Calling-Station-Id attribute is not sent.

## Usage Guidelines

Use the **radius attribute calling-station-id** command to send the Calling-Station-Id attribute, using the specified format, in RADIUS Access-Request and Accounting-Request packets for the current context.

If you specify the **agent-circuit-id** keyword, you can also specify the **remote-agent-id** keyword.

For Dynamic Host Configuration Protocol (DHCP) clients, the information for the Calling-Station-Id attribute is extracted from the suboption1 information in option 82 of the DHCP request packet; for Point-to-Point Protocol over Ethernet (PPPoE) clients, the information is extracted in the PPPoE Active Discovery Request (PADR) packet.

If the **agent-circuit-id** keyword is specified, but the agent-circuit-id information is not present in the DHCP request packet or in the PADR packet sent by the client, the SmartEdge OS inserts the “Agent-Circuit-Id Not Present” string.

If the **remote-agent-id** keyword is specified, but the remote-agent-id information is not present in the DHCP request packet or in the PADR packet sent by the client, the SmartEdge OS inserts the “Agent-Remote-Id Not Present” string.

For ATM PVCs, the format for the **slot-port** keyword is #Hostname#slot/port#VPI#VCI; the **description** format is #Hostname#VC description#VPI#VCI.

**Note** If the **description** keyword is used, but the description of the ATM PVC itself has not been configured using the **description** command (in ATM PVC configuration mode), the SmartEdge OS defaults to the **slot-port** format.

For VLANs, the format for the **slot-port** keyword is #Hostname#slot/port#Vlan-ID; the information in **description** format is #Hostname#Vlan description#Vlan-ID.

**Note** This command has no effect on incoming virtual circuit sessions that use the Layer 2 Tunneling Protocol (L2TP) or clientless IP service selection (CLIPS). Those circuits use the standard RADIUS attribute 31, Calling-Station-Id, independently of this command. Standard RADIUS attribute 31, Calling-Station-Id, is described in Appendix A, “RADIUS Attributes.”

Use the **show subscribers active** command (in any mode) to display Agent-Circuit-Id and Agent-Remote-Id information; for more information, see the “Context, Interface, and Subscriber Operations” chapter in the *Basic System Operations Guide* for the SmartEdge OS.

Use the **no** form of this command to disable the sending of the Calling-Station-Id attribute.

Use the **default** form of this command to specify the default separator.

## Examples

The following example sends the Calling-Station-Id attribute using the **slot-port** format and inserts **agent-circuit-id** and **remote-agent-id** information into Access-Request and Accounting-Request packets:

```
[local]Redback(config-ctx)#radius attribute calling-station-id format slot-port
agent-circuit-id remote-agent-id separator #
```

The format in which the Calling-Station-Id attribute is sent for VLAN connections is as follows:

```
hostname#slot#port#(VLAN ID)#(Agent-Circuit-Id)#(Agent-Remote-Id)
```



The following example configures the context so that the Calling-Station-Id attribute is sent in Access-Request and Accounting-Request packets using a slash (/) as the separator character:

```
[local]Redback(config-ctx)#radius attribute calling-station-id separator /
```

## Related Commands

**radius attribute acct-session-id**

**radius attribute nas-ip-address**

**radius attribute nas-port**

**radius attribute nas-port-id**

**radius attribute nas-port-type**

## radius attribute filter-id

**radius attribute filter-id direction** {in | out | both | none}

{no | default} **radius attribute filter-id**

### Purpose

Specifies the behavior of the SmartEdge OS when it receives a Remote Authentication Dial-In User Service (RADIUS) Filter-Id attribute that does not specify a direction and there is an access control list (ACL) applied to the circuit.

### Command Mode

context configuration

### Syntax Description

|                  |                                                                                            |
|------------------|--------------------------------------------------------------------------------------------|
| <b>direction</b> | Specifies the direction of the packets to which the ACL is applied.                        |
| <b>in</b>        | Applies the ACL to inbound packets only.                                                   |
| <b>out</b>       | Applies the ACL to outbound packets only.                                                  |
| <b>both</b>      | Applies the ACL to inbound and outbound packets.                                           |
| <b>none</b>      | Ignores the Filter-Id attribute and does not apply the ACL to packets in either direction. |

### Default

If the Filter-Id attribute does not include a direction, the SmartEdge OS applies the ACL to outbound packets only.

### Usage Guidelines

Use the **radius attribute filter-id** command to specify the behavior of the SmartEdge OS when it receives a RADIUS Filter-Id attribute that does not specify a direction and there is an ACL applied to the circuit. The choice of behavior depends on the nature of the ACL and the type of data that is exchanged.

The following sequence determines how the SmartEdge OS applies the ACL:

- If the Filter-Id attribute includes a direction, it is honored.
- If the Filter-Id attribute does not include a direction, and you have configured this command, the SmartEdge OS determines the direction from the configuration for this command.
- If the Filter-Id attribute does not include a direction, and this command is not configured, the SmartEdge OS applies the ACL to outbound packets only (the default condition).

Use the **no** or **default** form of this command to specify the default condition.

## Examples

The following example specifies that the ACL be applied to inbound packets only:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#radius attribute filter-id in
```

## Related Commands

None

## radius attribute nas-ip-address

**radius attribute nas-ip-address interface** *if-name*

**{no | default} radius attribute nas-ip-address**

### Purpose

Includes the network access server (NAS)-IP-Address attribute in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets sent by the SmartEdge router.

### Command Mode

context configuration

### Syntax Description

|                                 |                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface</b> <i>if-name</i> | Interface name. Uses the primary IP address associated with the interface as the source IP address sent in RADIUS packets. If the interface is not configured or is unreachable, the IP address of the outgoing interface is used instead as the source IP address for packets. |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

The NAS-IP-Address attribute is not sent.

### Usage Guidelines

Use the **radius attribute nas-ip-address** command to include the NAS-IP-Address attribute in RADIUS Access-Request and Accounting-Request packets sent by the SmartEdge router.

Standard RADIUS attribute 4, NAS-IP-Address, is described in Appendix A, “RADIUS Attributes.”

Use the **no** or **default** form of this command to reset the SmartEdge router behavior so that the NAS-IP-Address attribute is not included.

### Examples

The following example sends the primary IP address for interface `ether21` as the source IP address in RADIUS Access-Request and Accounting-Request packets sent by the SmartEdge router:

```
[local]Redback(config-ctx)#radius attribute nas-ip-address interface ether21
```

### Related Commands

**radius attribute acct-session-id**  
**radius attribute calling-station-id**  
**radius attribute nas-port**  
**radius attribute nas-port-id**  
**radius attribute nas-port-type**

# radius attribute nas-port

radius attribute nas-port format [physical | slot-port | session-info]  
{no | default} radius attribute nas-port format

## Purpose

Modifies the format of the network access server (NAS)-Port attribute, which is sent in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets for the current context.

## Command Mode

context configuration

## Syntax Description

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| format    | Indicates a particular attribute string format is to be applied.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| physical  | <p>Optional. Provides slot, port, virtual path identifier (VPI), and virtual channel identifier (VCI) in the NAS-Port attribute sent to the RADIUS server.</p> <p>For ATM circuits and PPPoE over ATM sessions, the attribute format is <i>slot-port-vpi-vci</i>, such that:</p> <ul style="list-style-type: none"><li>slot—SSSS (4 bits)</li><li>port—PPPP (4 bits)</li><li>vpi—CCCCCCCC (8 bits)</li><li>vci—CCCCCCCCCCCCCCCC (16 bits)</li></ul> <p>For Ethernet and VLAN circuits, the attribute format is <i>slot-port-unused</i>, such that:</p> <ul style="list-style-type: none"><li>slot—SSSS (4 bits)</li><li>port—PPPP (4 bits)</li><li>unused—XXXXXXXXXXXXXXXXXXXXXXXXXXXX (24 bits)</li></ul> |
| slot-port | <p>Optional. Provides slot, port, and channel information in the NAS-Port attribute sent to the RADIUS server. The attribute format is <i>slot-port-channel</i>, such that:</p> <ul style="list-style-type: none"><li>slot—SSSSSSSS (8 bits)</li><li>port—PPPPPPPP (8 bits)</li><li>channel—CCCCCCCCCCCCCCCC (16 bits)</li></ul> <p>If there is no channel, the <i>channel</i> argument is filled in with zeros.</p> <p>This is the default format for standard RADIUS attribute 5, NAS-Port.</p>                                                                                                                                                                                                          |

**session-info** Optional. Provides slot, port, and session information in the NAS-Port attribute sent to the RADIUS server.

For ATM circuits, the attribute format is *slot-port-vpi-vci*, such that:

- *slot*—SSSS (4 bits)
- *port*—PPPP (4 bits)
- *vpi*—CCCCCCCC (8 bits)
- *vci*—CCCCCCCCCCCCCCCC (16 bits)

For PPPoE over ATM, Ethernet, and VLAN circuits, the format is *slot-port-unused-pppoe\_session*, such that:

- *slot*—SSSS (4 bits)
- *port*—PPPP (4 bits)
- *unused*—XXXXXXXX (8 bits)
- *session*—CCCCCCCCCCCCCCCC (16 bits)

## Default

Standard RADIUS attribute 5, NAS-Port, is sent using the default format, **slot-port**.

## Usage Guidelines

Use the **radius attribute nas-port** command to modify the format of the NAS-Port attribute, which is sent in RADIUS Access-Request and Accounting-Request packets for the current context.

The standard RADIUS attribute 5, NAS-Port, is described in Appendix A, “RADIUS Attributes.”

Use the **no** or **default** form of this command to send the NAS-Port attribute using the default format.

## Examples

The following example sends the attribute NAS-Port using the *slot-port* format in RADIUS Access-Request and Accounting-Request packets for the *local* context:

```
[local]Redback(config)#context local  
[local]Redback(config-ctx)#radius attribute nas-port format slot-port
```

## Related Commands

**radius attribute acct-session-id**  
**radius attribute calling-station-id**  
**radius attribute nas-ip-address**  
**radius attribute nas-port-id**  
**radius attribute nas-port-type**

## radius attribute nas-port-id

```
radius attribute nas-port-id {format {agent-circuit-id [remote-agent-id] | all |
    hostname {agent-circuit-id [remote-agent-id]} | physical | remote-agent-id} |
    modified-agent-circuit-id | separator separator}
```

```
no radius attribute nas-port-id format
```

```
default radius attribute nas-port-id {format | separator separator}
```

### Purpose

Modifies the format of the network access server (NAS)-Port-Id attribute, which is sent in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets for the current context.

### Command Mode

context configuration

### Syntax Description

|                                  |                                                                                                                                                                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>format</b>                    | Indicates a particular format to be applied.                                                                                                                                                                                                                                 |
| <b>agent-circuit-id</b>          | Specifies that the format or the type of the information for the NAS-Port-Id attribute is Agent-Circuit-Id.                                                                                                                                                                  |
| <b>remote-agent-id</b>           | Optional. Specifies that the format or the type of the information for the Calling-Station-Id attribute is Agent-Remote-Id. Optional only when specifying the <b>agent-circuit-id</b> keyword.                                                                               |
| <b>hostname</b>                  | Prepends the SmartEdge router hostname to the contents of the NAS-Port-Id attribute in RADIUS packets. The hostname is either the one that has been configured using the <b>system hostname</b> command (in context configuration mode), or the default hostname, "Redback". |
| <b>all</b>                       | Specifies a format that includes the physical circuit and session information. This is the default format.                                                                                                                                                                   |
| <b>physical</b>                  | Specifies a format that includes the physical circuit only.                                                                                                                                                                                                                  |
| <b>modified-agent-circuit-id</b> | Specifies that the format or the type of the information for the NAS-Port-Id attribute is a modified form of the Agent-Circuit-Id.                                                                                                                                           |
| <b>separator separator</b>       | Character that separates the elements of the attribute string. The default separator character is the number symbol (#).                                                                                                                                                     |

### Default

Standard RADIUS attribute 87, NAS-Port-Id, is sent using the **all** format.

## Usage Guidelines

Use the **radius attribute nas-port-id** command to modify the format of the NAS-Port-Id attribute, which is sent in RADIUS Access-Request and Accounting-Request packets for the current context.



**Caution** Risk of interoperability loss. The NetOp™ Policy Manager (PM) requires the default format setting for this command to assimilate the RADIUS attribute information. To avoid loss of interoperability with NetOp PM, use this command with its default setting only.

If you specify the **agent-circuit-id** keyword, you can also specify the **remote-agent-id** keyword.

For Dynamic Host Configuration Protocol (DHCP) clients, the information for the NAS-Port-Id attribute is extracted from the suboption1 information in option 82 of the DHCP request packet; for Point-to-Point Protocol over Ethernet (PPPoE) clients, the information is extracted in the PPPoE Active Discovery Request (PADR) packet.

If the **agent-circuit-id** keyword is specified, but the agent-circuit-id information is not present in the DHCP request packet or in the PADR packet sent by the client, the SmartEdge OS inserts the “Agent-Circuit-Id Not Present” string.

If the **remote-agent-id** keyword is specified, but the remote-agent-id information is not present in the DHCP request packet or in the PADR packet sent by the client, the SmartEdge OS inserts the “Agent-Remote-Id Not Present” string.

If you specify the **all** keyword, the physical circuit information includes the slot, port, circuit identifier, and session identifier; the format in which the NAS-Port-Id attribute is sent is:

*slot/port* [**vpi-vci** *vpi vci* | **vlan-id** [*tunl-vlan-id*]:*pvc-vlan-id*] [**pppoe** *sess-id* | **clips** *sess-id*]

The circuit identifier can be the virtual path identifier (VPI) with the virtual channel identifier (VCI), or it can be the virtual LAN (VLAN) identifier, depending on the type of circuit.

If you specify the **physical** keyword, the format in which the NAS-Port-Id attribute is sent is:

*slot/port* [**vpi-vci** *vpi vci* | **vlan-id** [*tunl-vlan-id*]:*pvc-vlan-id*].

If you specify the **modified-agent-circuit-id** keyword, the system inserts the specific subscriber line information in the NAT-Port-ID attribute. Line information includes:

*slot/port* [**vpi-vci** *vpi vci* | **vlan-id** [*tunl-vlan-id*]:*pvc-vlan-id*]

which is prepended to the subscriber identification fields.

Standard RADIUS attribute 87, NAS-Port-Id, and Redback® vendor-specific attributes (VSAs) 96, Remote-Agent-Id, and 97, Agent-Circuit-Id, are described in Appendix A, “RADIUS Attributes.”

Use the **no** or **default** form of this command to reset the format for the NAS-Port-Id attribute to the **all** format.

Use the **default** form of this command to specify the default separator.

## Examples

The following example sends the NAS-Port-Id attribute using the **physical** format in RADIUS Access-Request and Accounting-Request packets for the **local** context:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius attribute nas-port-id format physical
```



## Related Commands

**radius attribute acct-session-id**  
**radius attribute calling-station-id**  
**radius attribute nas-ip-address**  
**radius attribute nas-port**  
**radius attribute nas-port-type**

## radius attribute nas-port-type

**radius attribute nas-port-type** *port-type*

{no | default} **radius attribute nas-port-type** *port-type*

### Purpose

Modifies the value for the network access server (NAS)-Port-Type attribute sent in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets.

### Command Mode

ATM profile configuration  
dot1q profile configuration  
port configuration

### Syntax Description

*port-type*                      Value that represents the type of connection the subscriber has to the network access server (NAS) through which it is authenticated. The range of values is 0 to 255. Values 0 to 19 are defined in Table 16-12.

The default value is either 0 or 5, indicating an asynchronous connection through a console port or a virtual connection through a transport protocol, respectively.

### Default

The Nas-Port-Type attribute is sent in RADIUS Access-Request and Accounting-Request packets. The value is either 0 or 5, depending on how the subscriber is connected to its authenticating NAS.

### Usage Guidelines

Use the **radius attribute nas-port-type** command to modify the value for the NAS-Port-Type attribute sent in RADIUS Access-Request and Accounting-Request packets.

Table 16-12 lists the definitions of the values for the *port-type* argument.

**Table 16-12 Values for the *port-type* Argument**

| Value | Definition                          |
|-------|-------------------------------------|
| 0     | async                               |
| 1     | sync                                |
| 2     | ISDN (sync)                         |
| 3     | ISDN (async V120)                   |
| 4     | ISDN (async V110)                   |
| 5     | Virtual                             |
| 6     | PIAFS (wireless ISDN used in Japan) |

**Table 16-12 Values for the *port-type* Argument** (*continued*)

| Value | Definition                                                       |
|-------|------------------------------------------------------------------|
| 7     | HDLC (clear-channel)                                             |
| 8     | X.25                                                             |
| 9     | X.75                                                             |
| 10    | G3_Fax (G.3 Fax)                                                 |
| 11    | SDSL (Symmetric DSL)                                             |
| 12    | ADSL_CAP (Asymmetric DSL Carrierless Amplitude Phase Modulation) |
| 13    | ADSL_DMT (Asymmetric DSL, Discrete Multi-Tone)                   |
| 14    | IDSL (ISDN Digital Subscriber Line)                              |
| 15    | Ethernet                                                         |
| 16    | xDSL (Digital Subscriber Line of unknown type)                   |
| 17    | Cable                                                            |
| 18    | Wireless (Wireless - Other)                                      |
| 19    | Wireless_802_11 (Wireless - IEEE 802.11)                         |

Standard RADIUS attribute 61, NAS-Port-Type, is described in Appendix A, “RADIUS Attributes.”

Use the **no** or **default** form of this command to reset the SmartEdge OS behavior to the default condition.

## Examples

The following example modifies the NAS-Port-Type attribute in RADIUS Access-Request and Accounting-Request packets to type 4 (ISDN):

```
[local]Redback(config)#context local
[local]Redback(config-atm-profile)#radius attribute nas-port-type 4
```

## Related Commands

```
radius attribute acct-session-id
radius attribute calling-station-id
radius attribute nas-ip-address
radius attribute nas-port
radius attribute nas-port-id
```

## radius attribute vendor-specific

**radius attribute vendor-specific Redback mac-address separator** *char*

{**no** | **default**} **radius attribute vendor-specific Redback mac-address**

### Purpose

Specifies the character the SmartEdge OS uses to separate the fields in the specified Remote Authentication Dial-In User Service (RADIUS) attribute.

### Command Mode

context configuration

### Syntax Description

|                              |                                                                                    |
|------------------------------|------------------------------------------------------------------------------------|
| <b>Redback</b>               | Specifies Redback as the vendor.                                                   |
| <b>mac-address</b>           | Specifies Redback vendor-specific attribute (VSA) 145, Mac-Addr, as the attribute. |
| <b>separator</b> <i>char</i> | Character to be used as a separator. The default is hyphen (-).                    |

### Default

The SmartEdge OS uses the hyphen (-) character.

### Usage Guidelines

Use the **radius attribute vendor-specific** command to specify the character the SmartEdge OS uses to separate the fields in the specified RADIUS attribute.

Use the **no** or **default** form of this command to specify the default character as the separator.

### Examples

The following example specifies the colon (:) as the separator character:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius attribute vendor-specific Redback mac-address
separator :
```

### Related Commands

None

# radius deadtime

**radius deadtime** *interval*

**default radius deadtime**

## Purpose

Sets the interval during which the SmartEdge OS treats a nonresponsive Remote Authentication Dial-In User Service (RADIUS) server as “dead”.

## Command Mode

context configuration

## Syntax Description

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| <i>interval</i> | Deadtime interval in minutes. The range of values is 0 to 65,535; the default value is 5. The 0 value disables this feature. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|

## Default

The waiting interval is five minutes.

## Usage Guidelines

Use the **radius deadtime** command to set the interval during which the SmartEdge OS treats a nonresponsive RADIUS server as “dead”. During the interval, the SmartEdge OS tries to reach another RADIUS server; after the interval expires, the SmartEdge OS tries again to reach the server. If there is no response, the RADIUS server remains marked as “dead” and the timer is set again to the configured interval.

If you disable this feature (with the 0 value), the SmartEdge OS never waits but attempts to reach the server immediately.

**Note** You must configure at least one RADIUS server using the **radius server** command (in context configuration mode) prior to entering this command.

Use the **default** form of this command to specify the default interval.

## Examples

The following example sets the deadtime interval to 10 minutes:

```
[local]Redback(config-ctx)#radius deadtime 10
```

## Related Commands

**radius server**  
**radius server-timeout**  
**radius timeout**

## radius max-outstanding

**radius max-outstanding** *requests*

{**no** | **default**} **radius max-outstanding**

### Purpose

Modifies the number of simultaneous outstanding requests that can be sent by the SmartEdge router to Remote Authentication Dial-In User Service (RADIUS) servers.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------|
| <i>requests</i> | Number of simultaneous outstanding requests per RADIUS server in the current context. The range of values is 1 to 256. |
|-----------------|------------------------------------------------------------------------------------------------------------------------|

### Default

The maximum number of allowable outstanding requests is 256.

### Usage Guidelines

Use the **radius max-outstanding** command to modify the number of simultaneous outstanding requests the SmartEdge router can send to RADIUS servers.

Use the **no** or **default** form of this command to reset the maximum number of outstanding requests to 256.

### Examples

The following example limits the number of simultaneous outstanding requests to 128:

```
[local]Redback(config-ctx)#radius max-outstanding 128
```

### Related Commands

- aaa authentication subscriber**
- radius max-retries**
- radius server**
- radius source-port**
- radius strip-domain**
- radius timeout**

## radius max-retries

**radius max-retries** *retries*

**default radius max-retries**

### Purpose

Modifies the number of retransmission attempts the SmartEdge router makes to a Remote Authentication Dial-In User Service (RADIUS) server in the event that no response is received from the server within the timeout period.

### Command Mode

context configuration

### Syntax Description

*retries*

Number of retransmission attempts the SmartEdge router will make. The range of values is 1 to 2,147,483,647; the default value is 3.

### Default

The SmartEdge router makes three retransmission attempts.

### Usage Guidelines

Use the **radius max-retries** command to modify the number of retransmission attempts the SmartEdge router makes to a RADIUS server in the event that no response is received from the server within the timeout period.

You set the timeout period with the **radius timeout** command (in context configuration mode).

If an acknowledgment is not received, each successive server is tried (wrapping from the last server to the first, if necessary) until the maximum number of retransmissions is reached.

Use the **default** form of this command to specify the default number of retries.

### Examples

The following example sets the retransmit value to 5:

```
[local]Redback(config-ctx)#radius max-retries 5
```

The following example resets the retransmit value to the default (3):

```
[local]Redback(config-ctx)#default radius max-retries
```

### Related Commands

**aaa authentication subscriber**  
**radius max-outstanding**

**radius timeout**

## radius policy

In global configuration mode, the syntax is:

**radius policy name** *pol-name*

**no radius policy name** *pol-name*

In context configuration mode, the syntax is:

**radius policy** *pol-name*

**no radius policy** *pol-name*

### Purpose

In global configuration mode, creates or modifies a Remote Authentication Dial-In User Service (RADIUS) policy and accesses RADIUS policy configuration mode; in context configuration mode, assigns a RADIUS policy to the context.

### Command Mode

context configuration

global configuration

### Syntax Description

|                             |                                                      |
|-----------------------------|------------------------------------------------------|
| <i>pol-name</i>             | Name of the RADIUS policy being assigned.            |
| <b>name</b> <i>pol-name</i> | Name of the RADIUS policy being created or modified. |

### Default

No RADIUS policy is created or assigned to a context.

### Usage Guidelines

Use the **radius policy** command in global configuration mode to create or modify a RADIUS policy and access RADIUS policy configuration mode; use it in context configuration mode to assign a RADIUS policy to the context.

The RADIUS policy specifies which RADIUS attributes and vendor-specific attributes (VSAs) are to be removed from RADIUS Access-Request and various Accounting-Request messages, such as Accounting-Start, Accounting-Stop, and Accounting-Update. Use the **attribute** command (in RADIUS policy configuration mode) to specify the attributes to be removed from the messages.

Use the **no** form of this command in global configuration mode to delete the policy; use it in context configuration mode to remove the policy from the context configuration.



## Examples

The following example creates the custom RADIUS policy:

```
[local]Redback(config)#radius policy name custom
[local]Redback(config-rad-policy)#
```

The following example assigns the custom RADIUS policy to the gold-isp context:

```
[local]Redback(config)#context gold-isp
[local]Redback(config-ctx)#radius policy custom
```

## Related Commands

**attribute**

## radius server

**radius server** {*ip-addr* | *hostname*} **key** *key* [**oldports** | **port** *udp-port*]

**no radius server** {*ip-addr* | *hostname*}

### Purpose

Configures the IP address or hostname of a Remote Authentication Dial-In User Service (RADIUS) server.

### Command Mode

context configuration

### Syntax Description

|                             |                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>              | IP address of the RADIUS server.                                                                                                                                                                          |
| <i>hostname</i>             | Hostname of the RADIUS server. The Domain Name System (DNS) must be enabled in order to use the <i>hostname</i> argument.                                                                                 |
| <b>key</b> <i>key</i>       | Alphanumeric string indicating the authentication key that must be shared with the RADIUS server.                                                                                                         |
| <b>oldports</b>             | Optional. Uses the RADIUS User Datagram Protocol (UDP) ports 1645 for authentication.                                                                                                                     |
| <b>port</b> <i>udp-port</i> | Optional. RADIUS authentication UDP port. The range of values is 1 to 65,536. If no port is specified, port 1812 is used for authentication. The <i>udp-port</i> value indicates the authentication port. |

### Default

RADIUS server hostnames and IP addresses are not preconfigured. 1812 is the UDP authentication port.

### Usage Guidelines

Use the **radius server** command to configure the IP address or hostname of a RADIUS server. You can use this command multiple times to configure up to five RADIUS servers per context.

To use the *hostname* argument, DNS must be enabled; for more information, see Chapter 6, “DNS Configuration.”

**Note** To enable authentication to be performed by RADIUS, you must also enter the **aaa authentication subscriber** command (in context configuration mode); for more information, see Chapter 15, “AAA Configuration.”

Use the **no** form of this command to delete a previously configured RADIUS server.

## Examples

The following example configure a RADIUS server IP address of 10.3.3.3 with the key, secret, using ports 4444 for authentication:

```
[local]Redback(config-ctx)#radius server 10.3.3.3 key secret port 4444
```

## Related Commands

```
aaa authentication subscriber  
radius source-port
```

## radius server-timeout

**radius server-timeout** *interval*

**default radius server-timeout**

### Purpose

Sets the time interval the SmartEdge OS waits before marking a non-responsive Remote Authentication Dial-In User Service (RADIUS) server as “dead”.

### Command Mode

context configuration

### Syntax Description

|                 |                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interval</i> | Number of seconds after which the SmartEdge OS checks for successful responses after an individual RADIUS request times out, before treating the server as “dead”. The range of values, in seconds, is 0 to 2,147,483,647; the default value is 60. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Default

The maximum time interval is 60 seconds.

### Usage Guideline

Use the **radius server-timeout** command to set the time interval the SmartEdge OS waits before marking a non-responsive RADIUS accounting server as “dead”.

The SmartEdge OS marks a RADIUS server as “dead” when no response is received to any RADIUS requests during the time period specified by the *interval* argument. Setting the value to 0 disables this feature; in this case, no RADIUS server is marked as “dead”.

Use the **default** form of this command to specify the default interval.

### Examples

The following example sets the waiting interval to 80 seconds:

```
[local]Redback(config-ctx)#radius server-timeout 80
```

### Related Commands

**radius deadtime**

## radius source-port

**radius source-port** *port-num num-ports*

**no radius source-port**

### Purpose

Increases the number of outstanding requests per Remote Authentication Dial-In User Service (RADIUS) server by sending requests using a different source port value.

### Command Mode

global configuration

### Syntax Description

|                  |                                                      |
|------------------|------------------------------------------------------|
| <i>port-num</i>  | Port number. The range of values is 1,024 to 65,535. |
| <i>num-ports</i> | Number of ports. The range of values is 1 to 10.     |

### Default

Disabled.

### Usage Guidelines

Use the **radius source-port** command to increase the number of outstanding requests per RADIUS server by sending requests using a different source port value.

Use the **no** form of this command to return to the default number of outstanding requests.

### Examples

The following example configures a port number of 2000 and sets the number of ports to 5:

```
[local]Redback(config)#radius source-port 2000 5
```

### Related Commands

- aaa authentication subscriber**
- radius algorithm**
- radius max-outstanding**
- radius max-retries**
- radius server**
- radius strip-domain**
- radius timeout**

## radius strip-domain

**radius strip-domain**

**no radius strip-domain**

### Purpose

Strips the domain portion of a structured username before relaying an authentication request to a Remote Authentication Dial-In User Service (RADIUS) server.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

The entire username, including the domain name, is sent to the RADIUS server.

### Usage Guidelines

Use the **radius strip-domain** command to strip the domain portion of a structured username before relaying an authentication request to a RADIUS server. The username can be either a subscriber name or administrator name.

Use the **no** form of this command to disable stripping the domain portion of the structured username.

### Examples

The following example prevents the domain portion of the structured username from being sent to the RADIUS server for authentication:

```
[local]Redback(config-ctx)#radius strip-domain
```

### Related Commands

**aaa authentication subscriber**  
**radius algorithm**  
**radius max-outstanding**  
**radius max-retries**  
**radius server**  
**radius source-port**  
**radius timeout**

# radius timeout

**radius timeout** *timeout*

**default radius timeout**

## Purpose

Sets the maximum time the SmartEdge router waits for a response from a Remote Authentication Dial-In User Service (RADIUS) server before assuming that a packet is lost, or that the RADIUS server is unreachable.

## Command Mode

context configuration

## Syntax Description

|                |                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------|
| <i>timeout</i> | Timeout period in seconds. The range of values is 1 to 2,147,483,647; the default value is 10 seconds. |
|----------------|--------------------------------------------------------------------------------------------------------|

## Default

The maximum time is 10 seconds.

## Usage Guidelines

Use the **radius timeout** command to set the maximum time the SmartEdge router waits for a response from a RADIUS server before assuming that a packet is lost, or that the RADIUS server is unreachable.

Use the **default** form of this command to specify the default interval.

## Examples

The following example sets the timeout interval to 30 seconds:

```
[local]Redback(config-ctx)#radius timeout 30
```

## Related Commands

- aaa authentication subscriber**
- radius algorithm**
- radius max-outstanding**
- radius max-retries**
- radius server**
- radius source-port**
- radius strip-domain**

## rbak-term-ec

**rbak-term-ec** *term-error-code* **ietf-attr-49** *error-code*  
**no** **rbak-term-ec** *term-error-code*

### Purpose

Remaps a Redback account (session) termination error code to a different Remote Authentication Dial-In User Service (RADIUS) attribute 49 (Acct-Terminate-Cause) error code.

### Command Mode

terminate error cause configuration

### Syntax Description

|                                       |                                                                                  |
|---------------------------------------|----------------------------------------------------------------------------------|
| <i>term-error-code</i>                | Redback account termination error code to be remapped.                           |
| <b>ietf-attr-49</b> <i>error-code</i> | Attribute 49 error code to which the Redback termination error code is remapped. |

### Default

No Redback account termination error codes are remapped.

### Usage Guidelines

Use the **rbak-term-ec** command to remap a Redback account (session) termination error code to a different RADIUS attribute 49 (Acct-Terminate-Cause) error code. The “RADIUS Attribute 49 Error Codes” appendix in the *IP Services and Security Operations Guide* for the SmartEdge OS lists the default mapping of Redback account termination error codes to RADIUS attribute 49 (Acct-Terminate-Cause) error codes. RADIUS attribute 49 error codes and their definitions are included in RFC 2866, *RADIUS Accounting*.

Use the **no** form of this command to specify the default RADIUS attribute 49 error code for the specified Redback account termination error code.

### Examples

The following example remaps Redback account termination code 24 (Authentication failed) from its default RADIUS attribute 49 error code 17 (User error), to the RADIUS attribute 49 error code 2 (network access server [NAS] error).

```
[ local ]Redback(config)#radius attribute acct-terminate-cause remap
[ local ]Redback(config-term-ec)#rbak-term-ec 24 ietf-attr-49 2
```

### Related Commands

**radius attribute acct-terminate-cause remap**



# TACACS+ Configuration

---

This chapter describes the commands used to configure SmartEdge® OS Terminal Access Controller Access Control System Plus (TACACS+) features.

For information about TACACS+ attribute-value (AV) pairs, see Appendix B, “TACACS+ Attribute-Value Pairs.”

For information about the commands used to monitor, troubleshoot, and administer TACACS+, see the “TACACS+ Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

The TACACS+ protocol enables the building of a system that secures remote access to networks and network services. TACACS+ is based on a client/server architecture. When configured with the IP address or hostname of a TACACS+ server, the SmartEdge router can act as a TACACS+ client. TACACS+ servers are configured on a per-context basis, with a limit of six servers in each context.

The SmartEdge OS supports the TACACS+ features of One-Time Passwords in Everything (OPIE), S/Key, and SecurID, if they are supported by and enabled on the TACACS+ server. These functions are limited to Telnet sessions only.

The SmartEdge OS uses Simple Network Management Protocol (SNMP) notifications when the SmartEdge router has difficulty in communicating with a TACACS+ server and declares it down and also when communication to the server is restored.

Configurable options for a TACACS+ server include:

- Timeout interval, maximum number of retries, deadtime interval
- Domain stripping of structured usernames

- Authenticating of administrators and authorizing the use of specific command-line interface (CLI) commands.
- Sending of accounting messages for administrator sessions and CLI command accounting records to TACACS+ servers.

To enable authentication and accounting features, you must also configure authentication, authorization, and accounting (AAA). For information about AAA tasks and commands, see Chapter 15, “AAA Configuration.”

To enable administrator authentication through TACACS+, enter the **aaa authentication administrator** command (in context configuration mode). To configure CLI authorization, enter the **aaa authorization commands** command (in context configuration mode). To enable accounting messages to be sent to a TACACS+ server, enter the **aaa accounting administrators** and **aaa accounting commands** commands (in context configuration mode).

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

The SmartEdge OS supports up to six TACACS+ servers in each context. Servers are assigned priority based on the order in which they are configured in the SmartEdge OS. The first configured server is used first. If the first server becomes unavailable or unreachable, the second server is used, and so on.

By default, the local IP address for the interface on which TACACS+ is transmitted is included in packets sent by the SmartEdge OS. To not publish the IP address to the TACACS+ server, you must configure a loopback interface to appear to be the source address for TACACS+ packets. The interface must be reachable by the TACACS+ server; for details about this command, see the “Interface Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

To configure a TACACS+ server, perform the tasks described in Table 17-1; enter all commands in context configuration mode, unless otherwise noted. For information about the **ip source-address** command (in interface configuration mode) with the **tacacs+** keyword, see the “Interface Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

**Table 17-1 Configure a TACACS+ Server**

| #  | Task                                                                                                                                                      | Root Command            | Notes |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------|
| 1. | Configure the IP address or hostname of a TACACS+ server.                                                                                                 | <b>tacacs+ server</b>   |       |
| 2. | Optional. Configure server parameters, using one or more of the following tasks:                                                                          |                         |       |
|    | Modify the interval during which the SmartEdge OS is to treat a nonresponsive TACACS+ server as dead, and try instead to reach another configured server. | <b>tacacs+ deadtime</b> |       |
|    | Modify the timeout value.                                                                                                                                 | <b>tacacs+ timeout</b>  |       |

**Table 17-1** Configure a TACACS+ Server (*continued*)

| # | Task                                                                                                                                                                             | Root Command                | Notes                                                                                      |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------------------------------------------------------------------------------------|
|   | Modify the number of retransmission attempts to open a TCP connection to the TACACS+ server in the event that no response is received from the server within the timeout period. | <b>tacacs+ max-retries</b>  |                                                                                            |
|   | Strip the domain portion of a structured username before relaying an authentication, authorization, or accounting request.                                                       | <b>tacacs+ strip-domain</b> |                                                                                            |
|   | Configure an IP source address.                                                                                                                                                  | <b>ip source-address</b>    | Enter this command in interface configuration mode and specify the <b>tacacs+</b> keyword. |

For information about configuring interfaces and the **ip source-address** command (in interface configuration mode), see the “Interface Configuration” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

## Configuration Examples

The following example configures a TACACS+ server IP address, 10.43.32.56, with the key, Secret. The SmartEdge router will attempt to open a TCP connection to the TACACS+ server up to 5 times when no response is received within 30 seconds.

```
[local]Redback(config-ctx)#tacacs+ server 10.43.32.56 key Secret
[local]Redback(config-ctx)#tacacs+ max-retries 5
[local]Redback(config-ctx)#tacacs+ timeout 30
[local]Redback(config-ctx)#tacacs+ strip-domain
```

## Command Descriptions

This section describes the syntax and usage guidelines for the commands used to configure TACACS+. The commands are presented in alphabetical order.

**tacacs+ deadtime**  
**tacacs+ max-retries**  
**tacacs+ server**

**tacacs+ strip-domain**  
**tacacs+ timeout**

## tacacs+ deadtime

**tacacs+ deadtime** *interval*

**no tacacs+ deadtime**

**default tacacs+ deadtime**

### Purpose

Modifies the interval during which the SmartEdge OS is to treat a nonresponsive Terminal Access Controller Access Control System Plus (TACACS+) server as “dead,” and instead, try to reach another server if one is configured.

### Command Mode

context configuration

### Syntax Description

*interval*                      Deadtime interval in minutes. The range of values is 0 to 65,535; the default value is 5.

### Default

The SmartEdge OS waits five minutes after a timeout occurs before considering the affected server to be eligible to accept TACACS+ requests again.

### Usage Guidelines

Use the **tacacs+ deadtime** command to modify the interval during which the SmartEdge OS is to treat a nonresponsive TACACS+ server as “dead”, and try, instead, to reach another configured server.

If a server fails to respond to a TACACS+ request within the configured TACACS+ timeout window, which configured with the **tacacs+ timeout** command (in context configuration mode), it is declared dead. No TACACS+ requests are sent to a dead server until the server deadtime (the value of the *interval* argument) expires, at which time the server is again considered eligible for new TACACS+ requests and resumes its original priority. However, if all servers are currently considered dead, and there is an unprocessed TACACS+ request, one of the dead servers is chosen in round-robin fashion to be the target of the request, even though the deadtime has not elapsed.

Use the **no** form of this command or specify a value of 0 for the *interval* argument to disable the deadtime feature, which means that the server is never considered ineligible for TACACS+ requests.

Use the **default** form of this command to reset the number of retransmission attempts to five minutes.

### Examples

The following example specifies a deadtime interval of 10 minutes:

```
[local]Redback(config-ctx)#tacacs+ deadtime 10
```

## Related Commands

**tacacs+ max-retries**

**tacacs+ server**

**tacacs+ timeout**

## tacacs+ max-retries

**tacacs+ max-retries** *retries*

**no tacacs+ max-retries**

**default tacacs+ max-retries**

### Purpose

Modifies the number of retransmission attempts the SmartEdge router will make to open a Transmission Control Protocol (TCP) connection to the Terminal Access Controller Access Control System Plus (TACACS+) server in the event that no response is received from the server within the timeout period.

### Command Mode

context configuration

### Syntax Description

*retries*                Number of retransmission attempts. The range of values is 0 to 255; the default value is 3.

### Default

The SmartEdge OS makes three attempts to open a TCP connection to the TACACS+ server.

### Usage Guidelines

Use the **tacacs+ max-retries** command to modify the number of retransmission attempts the SmartEdge Router will make to open a TCP connection to the TACACS+ server in the event that no response is received from the server within the timeout period.

The timeout period is configured through the **tacacs+ timeout** command (in context configuration mode).

If no acknowledgment is received, all configured TACACS+ servers in the context are tried (moving from the last server back to the first, if necessary) until the maximum number of retransmission attempts have been made for each configured server.

Use the **no** form of this command or specify a value of 0 for the *retries* argument to disable the retransmission completely.

Use the **default** form of this command to reset the number of retransmission attempts to 3.

### Examples

The following example modifies the retry count to allow the SmartEdge OS to make up to 5 attempts to open a TCP connection to the TACACS+ server in the event that no response is received from the server within the timeout period:

```
[local]Redback(config-ctx)#tacacs+ max-retries 5
```

## Related Commands

`tacacs+ deadtime`  
`tacacs+ server`  
`tacacs+ timeout`

## tacacs+ server

**tacacs+ server** {*ip-addr* | *hostname*} **key** *key* [**port** *tcp-port*]

**no tacacs+ server** {*ip-addr* | *hostname*} **key** *key* [**port** *tcp-port*]

### Purpose

Configures the IP address or hostname for a Terminal Access Controller Access Control System Plus (TACACS+) server.

### Command Mode

context configuration

### Syntax Description

|                             |                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>              | IP address of the TACACS+ server.                                                                                                                                          |
| <i>hostname</i>             | Hostname of the TACACS+ server.                                                                                                                                            |
| <b>key</b> <i>key</i>       | Alphanumeric string indicating the authentication key that must be shared with the TACACS+ server.                                                                         |
| <b>port</b> <i>tcp-port</i> | Optional. TACACS+ server Transmission Control Protocol (TCP) port. The range of values is 1 to 65,536. If no port is specified, TCP port number 49 is used as the default. |

### Default

None

### Usage Guidelines

Use the **tacacs+ server** command to configure the IP address or hostname for a TACACS+ server. The SmartEdge OS can support up to five TACACS+ servers in each context. The servers are assigned priority based on the order configured. The first configured server is used first. If the first server becomes unavailable or unreachable, the second server is used, and so on.

In order for the *hostname* argument to take effect, Domain Name System (DNS) resolution must be enabled; for more information, see Chapter 6, “DNS Configuration,” for information.

Use the **no** form of this command to delete a previously configured TACACS+ server.

### Examples

The following example defines a TACACS+ server with an IP address, 10.43.32.56, and the key, Secretkey, for authentication:

```
[local]Redback(config-ctx)#tacacs+ server 10.43.32.56 key Secretkey port 53
```



## Related Commands

`tacacs+ max-retries`

`tacacs+ timeout`

## tacacs+ strip-domain

**tacacs+ strip-domain**

**{no | default} tacacs+ strip-domain**

### Purpose

Specifies that the domain portion of a structured username be removed before relaying an authentication, authorization, or accounting request to a Terminal Access Controller Access Control System Plus (TACACS+) server.

### Command Mode

context configuration

### Syntax Description

This command has no keywords or arguments.

### Default

The SmartEdge OS sends entire structured username, including the domain name, to the TACACS+ server.

### Usage Guidelines

Use the **tacacs+ strip-domain** command to specify that the domain portion of a structured username be removed before relaying an authentication, authorization, or accounting request to a TACACS+ server. For example, subscriber name joe is sent rather than joe@local. The domain portion can be stripped, even if custom structured username formats have been defined using the **aaa username-format** command (in global configuration mode).

The decision to strip the domain name depends on whether or not subscriber and administrator records are defined with or without the domain name in the TACACS+ server configuration.

Use the **no** or **default** form of this command to disable the stripping of the domain portion of the structured username.

### Examples

The following example prevents the domain portion of the structured username from being sent to the TACACS+ server:

```
[local]Redback(config-ctx)#tacacs+ strip-domain
```

### Related Commands

**aaa username-format**

## tacacs+ timeout

**tacacs+ timeout** *seconds*

**default tacacs+ timeout**

### Purpose

Modifies the maximum amount of time the SmartEdge OS waits for a response from a Terminal Access Controller Access Control System Plus (TACACS+) server before assuming that a packet is lost or that the TACACS+ server is unreachable.

### Command Mode

context configuration

### Syntax Description

*seconds*                      Timeout period in seconds. The range of values is 1 to 65,535; the default value is 10.

### Default

The timeout interval is 10 seconds.

### Usage Guidelines

Use the **tacacs+ timeout** command to modify the maximum amount of time that the SmartEdge OS waits for a response from a TACACS+ server before assuming that a packet is lost or that the TACACS+ server is unreachable.

The timeout value is displayed in the output of the **show tacacs+ server** command.

Use the **default** form of this command to return the timeout to the default value of 10 seconds.

### Examples

The following example sets the TACACS+ timeout to 60 seconds:

```
[local]Redback(config-ctx)#tacacs+ timeout 60
```

### Related Commands

**tacacs+ deadtime**  
**tacacs+ max-retries**  
**tacacs+ server**



# Key Chain Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS key chain features.

For information about the commands used to monitor, troubleshoot, and administer key chains, see the “Key Chain Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

Key chains allow you to control authentication keys used by various routing protocols in the system. The SmartEdge OS supports the use of key chains with the Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) routing protocols. Enabling the use of key chains by a routing protocol is part of the configuration process for the protocol; for information about configuring routing protocols, see the *Routing Protocols Configuration Guide* for the SmartEdge OS.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure key chains, perform the tasks described in the following sections:

- Configure a Key Chain Name and Description (Optional)
- Configure a Key Chain Name and ID
- Configure a Key String

- Limit the Lifespan of a Key
- Enable Key Chain Authentication with Routing Protocols

## Configure a Key Chain Name and Description (Optional)

To configure a key chain name and description, perform the task described in Table 18-1.

**Table 18-1 Configure a Key Chain Name and Description (Optional)**

| Task                                        | Root Command                 | Notes                                                                                                                                                                |
|---------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure a key chain name and description. | <b>key-chain description</b> | Enter this command in context configuration mode.<br>The description is displayed in the output of the <b>show configuration</b> and <b>show key-chain</b> commands. |

## Configure a Key Chain Name and ID

To configure a key chain name and ID, perform the task described in Table 18-2.

**Table 18-2 Configure a Key Chain Name and ID**

| Task                                                                        | Root Command            | Notes                                             |
|-----------------------------------------------------------------------------|-------------------------|---------------------------------------------------|
| Configure a key chain name and ID, and access key chain configuration mode. | <b>key-chain key-id</b> | Enter this command in context configuration mode. |

## Configure a Key String

To configure a key string (a password), perform the task described in Table 18-3.

**Table 18-3 Configure a Key String**

| Task                    | Root Command      | Notes                                               |
|-------------------------|-------------------|-----------------------------------------------------|
| Configure a key string. | <b>key-string</b> | Enter this command in key chain configuration mode. |

## Limit the Lifespan of a Key

To limit the lifespan of a key, perform one or more of the tasks described in Table 18-4; enter all commands in key chain configuration mode.

**Table 18-4 Limit the Lifespan of a Key**

| Task                                                                                                                    | Root Command           | Notes                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Specify a date and time at which to start sending the key, and optionally, a time at which to stop sending the key.     | <b>send-lifetime</b>   | If you do not issue the <b>send-lifetime</b> command, the key is sent starting immediately and continues to be sent indefinitely.           |
| Specify a date and time at which to start accepting the key, and optionally, a time at which to stop accepting the key. | <b>accept-lifetime</b> | If you do not issue the <b>accept-lifetime</b> command, the key is accepted starting immediately and continues to be accepted indefinitely. |

## Enable Key Chain Authentication with Routing Protocols

To enable key chain authentication with OSPF, IS-IS, or VRRP, perform the task described in Table 18-5.

**Table 18-5 Enable Key Chain Authentication with Routing Protocols**

| Task                                                    | Root Command          | Notes                                                                                                                                                |
|---------------------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable key chain authentication with routing protocols. | <b>authentication</b> | Enter this command in OSPF interface, IS-IS router, IS-IS interface, or VRRP configuration mode, depending on the routing protocol being configured. |

For information about configuring routing protocols and the **authentication** command (in any of the modes listed in Table 18-5), see the “OSPF Configuration,” “IS-IS Configuration,” or “VRRP Configuration” chapter in the *Routing Protocols Configuration Guide* for the SmartEdge OS.

## Configuration Examples

The following example configures a rollover period on Feb 2, 2002 from 12:00 a.m to 2:00 a.m. During this period, both keys will be accepted. Starting at 1:00 a.m., the new key will be sent.

```
[local]Redback(config-ctx)#key-chain ospf-keychain key-id 1
[local]Redback(config-key-chain)#key-string redback
[local]Redback(config-key-chain)#accept-lifetime 2001:02:02:00:00:00
2001:02:02:02:00:00
[local]Redback(config-key-chain)#send-lifetime 2001:02:02:01:00:00 2002:02:02:01:00:00
[local]Redback(config-key-chain)#key-chain ospf-keychain key-id 2
[local]Redback(config-key-chain)#key-string se800
[local]Redback(config-key-chain)#accept-lifetime 2002:02:02:00:00:00
2003:02:02:02:00:00
[local]Redback(config-key-chain)#send-lifetime 2002:02:02:01:00:00 2003:02:02:01:00:00
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#router ospf 1
[local]Redback(config-ospf)#area 0
[local]Redback(config-ospf-area)#interface fa4/1
[local]Redback(config-ospf-if)#authentication md5 ospf-keychain
```

## Command Descriptions

This section describes the syntax and usage guidelines for the commands used to configure key chains. The commands are presented in alphabetical order.

**accept-lifetime**  
**key-chain description**  
**key-chain key-id**

**key-string**  
**send-lifetime**

## accept-lifetime

**accept-lifetime** *start-datetime* [**duration** *seconds* | **infinite** | *stop-datetime*]

**no accept-lifetime** *start-datetime* [**duration** *seconds* | **infinite** | *stop-datetime*]

### Purpose

Establishes a start date and time for accepting the key, and optionally, a stop time for accepting the key.

### Command Mode

key chain configuration

### Syntax Description

|                                |                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>start-datetime</i>          | Date and time to start accepting the key being configured. Must be in the format <i>yyyy:mm:dd:hh:mm[:ss]</i> . See the “Usage Guidelines” section for more information about the format of this argument.          |
| <b>duration</b> <i>seconds</i> | Optional. Number of seconds to continue accepting the key. The range of values is 1 to 2,147,483,646.                                                                                                               |
| <b>infinite</b>                | Optional. Specifies that the key is to be accepted indefinitely.                                                                                                                                                    |
| <i>stop-datetime</i>           | Optional. Date and time to stop accepting the key being configured. Must be in the format <i>yyyy:mm:dd:hh:mm[:ss]</i> . See the “Usage Guidelines” section for more information about the format of this argument. |

### Default

If you do not issue this command, the key is accepted starting immediately and continues to be accepted indefinitely. If you do not specify a duration when issuing this command, the key is accepted indefinitely.

### Usage Guidelines

Use the **accept-lifetime** command to specify when the key being configured is to be accepted. The format of the *start-datetime* and *stop-datetime* arguments is *yyyy:mm:dd:hh:mm[:ss]* and is defined as follows:

- *yyyy* = The year in four digits (for example, 2003).
- *mm* = The month of the year in two digits (for example, 01). The range of values is 1 to 12.
- *dd* = The day of the month in two digits (for example, 24). The range of values is 1 to 31.
- *hh* = The hour of the day in two digits (for example, 23). The range of values is 0 to 23.
- *mm* = The minute of the hour in two digits (for example, 59). The range of values is 0 to 59.
- *ss* = Optional. The second of the minute in two digits (for example, 55). The range of values is 0 to 59.

If you issue the **accept-lifetime** command without any optional constructs, the key is accepted starting with the date and time that you specify and continues to be accepted indefinitely. You can replace an existing accept lifetime value by issuing the **accept-lifetime** command again and specifying new values.

Use the **no** form of this command to specify that the key is no longer to be accepted.



## Examples

The following example establishes a lifetime acceptance of January 25, 2002 at one minute and one second after 4:00 a.m. The key continues to be accepted indefinitely.

```
[local]Redback(config-key-chain)#accept-lifetime 2002:01:25:04:01:01
```

The following example establishes a lifetime acceptance of January 25, 2002 at exactly midnight, and specifies that the key is to be accepted for 30 minutes (1800 seconds):

```
[local]Redback(config-key-chain)#accept-lifetime 2002:01:25:00:00 duration 1800
```

## Related Commands

**send-lifetime**

## key-chain description

**key-chain** *key-chain-name* **description** *text*

**no key-chain** *key-chain-name* [**description** *text*]

### Purpose

Configures a key chain name and description.

### Command Mode

context configuration

### Syntax Description

|                       |                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------|
| <i>key-chain-name</i> | Name of the key chain.                                                                                      |
| <i>text</i>           | Alphanumeric text description to be associated with the key chain. Optional only when deleting a key chain. |

### Default

No key chains are created.

### Usage Guidelines

Use the **key-chain description** command to configure a key chain name and description.

Only one description can be associated with a single key chain. To update a description, issue this command with the new description; the old description is overwritten.

Use the **no** form of this command with the **description text** construct to remove a description from the key chain configuration. Use the **no** form of this command without the optional construct to delete the entire key chain.

### Examples

The following example configures key01 with a text description specifying 3 keys ospf only:

```
[local]Redback(config-ctx)#key-chain key01 description 3 keys ospf only
```

### Related Commands

**key-chain** *key-id*

## key-chain key-id

**key-chain** *key-chain-name* **key-id** *key-id*  
**no key-chain** *key-chain-name* [**key-id** *key-id*]

### Purpose

Creates a new key chain with a key, or creates a key within an existing key chain, and enters key chain configuration mode.

### Command Mode

context configuration

### Syntax Description

|                       |                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>key-chain-name</i> | Name of the key chain.                                                                                                                                             |
| <i>key-id</i>         | Identification number of a key within the chain. The range of values is 1 to 65,535. Must be unique within the key chain. Optional only when deleting a key chain. |

### Default

No key chains are created.

### Usage Guidelines

Use the **key-chain key-id** command to create a new key chain with a key, or to create a key within an existing key chain, and to enter key chain configuration mode.

Key chains allow you to control authentication keys used by various routing protocols in the system. Currently, the SmartEdge OS supports the use of key chains with the Open Shortest Path First (OSPF), intermediate-system-to-intermediate-system (IS-IS), and Virtual Router Redundancy Protocol (VRRP) routing protocols.

For information about the **authentication** command used in conjunction with the **key-chain key-id** command, see the “OSPF Configuration,” “IS-IS Configuration,” or VRRP Configuration” chapter in the *Routing Protocols Configuration Guide* for the SmartEdge OS.

Use the **no** form of this command with the **key-id key-id** construct to remove a key from the key chain configuration. Use the **no** form of this command without the optional construct to remove the entire key chain.

### Examples

The following example creates a new key chain, superkeychain, and creates three keys within it (IDs 200, 201, 202), each with its own string and lifetime:

```
[local]Redback(config-ctx)#key-chain superkeychain key-id 200
[local]Redback(config-key-chain)#key-string di492jffs
[local]Redback(config-key-chain)#accept-lifetime 2001:01:01:01:01 duration 10000
```

```
[local]Redback(config-key-chain)#send-lifetime 2001:01:01:01:01 infinite
[local]Redback(config-key-chain)#key-chain superkeychain key-id 201
[local]Redback(config-key-chain)#key-string 7744kkciao
[local]Redback(config-key-chain)#accept-lifetime 2001:01:01:01:01 infinite
[local]Redback(config-key-chain)#send-lifetime 2001:01:01:01:01
[local]Redback(config-key-chain)#key-chain superkeychain key-id 202
[local]Redback(config-key-chain)#key-string secret222
[local]Redback(config-key-chain)#accept-lifetime 2001:01:01:01:01 2002:01:01:00:00
[local]Redback(config-key-chain)#send-lifetime 2001:01:01:01:01 infinite
```

**Note** In this example, it is not necessary to exit from key chain configuration mode to enter the **key-chain** command, because commands from the next highest mode in the hierarchy (context configuration mode, in this case) are accepted in any configuration mode.

## Related Commands

- accept-lifetime**
- key-chain description**
- key-string**
- send-lifetime**

# key-string

**key-string** *string*

**no key-string** *string*

## Purpose

Configures a string for the specified key.

## Command Mode

key chain configuration

## Syntax Description

*string*                      Alphanumeric string.

## Default

No key string is configured.

## Usage Guidelines

Use the **key-string** command to configure a string for the specified key. A string is equivalent to a password. The string is encrypted in the output of the **show configuration** command. In the output of the **show key-chain** command, the key string is shown both encrypted and unencrypted.

You can replace an existing key string by using the **key-string** command again, specifying a new string.

Use the **no** form of this command to remove the key string from the configuration.

## Examples

The following example configures 7744kkciao as the string for the key chain, secretkeychain:

```
[local]Redback(config-ctx)#key-chain secretkeychain key-id 200  
[local]Redback(config-key-chain)#key-string 7744kkciao
```

## Related Commands

**key-chain description**

**key-chain key-id**

## send-lifetime

**send-lifetime** *start-datetime* [**duration** *seconds* | **infinite** | *stop-datetime*]

**no send-lifetime** *start-datetime* [**duration** *seconds* | **infinite** | *stop-datetime*]

### Purpose

Establishes a start date and time for sending the key, and optionally, a stop date and time for sending the key.

### Command Mode

key chain configuration

### Syntax Description

|                                |                                                                                                                                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>start-datetime</i>          | Date and time to start sending the key being configured. Must be in the format <i>yyyy:mm:dd:hh:mm[:ss]</i> . See the “Usage Guidelines” section for more information about the format of this argument.          |
| <b>duration</b> <i>seconds</i> | Optional. Number of seconds to continue sending the key. The range of values is 1 to 2,147,483,646.                                                                                                               |
| <b>infinite</b>                | Optional. Specifies that the key is to be sent indefinitely.                                                                                                                                                      |
| <i>stop-datetime</i>           | Optional. Date and time to stop sending the key being configured. Must be in the format <i>yyyy:mm:dd:hh:mm[:ss]</i> . See the “Usage Guidelines” section for more information about the format of this argument. |

### Default

If you do not use this command, the key is sent starting immediately and continues to be sent indefinitely.  
If you do not specify a duration when using this command, the key is sent indefinitely.

### Usage Guidelines

Use the **send-lifetime** command to specify when the key being configured is to be sent. The format of the *start-datetime* and *stop-datetime* arguments is *yyyy:mm:dd:hh:mm[:ss]* and is defined as follows:

- *yyyy* = The year in four digits (for example, 2001).
- *mm* = The month of the year in two digits (for example, 01). The range of values is 1 to 12.
- *dd* = The day of the month in two digits (for example, 24). The range of values is 1 to 31.
- *hh* = The hour of the day in two digits (for example, 23). The range of values is 0 to 23.
- *mm* = The minute of the hour in two digits (for example, 59). The range of values is 0 to 59.
- *ss* = The second of the minute in two digits (for example, 55). The range of values is 0 to 59.

If you issue the **send-lifetime** command without any optional constructs, the key is sent starting with the date and time that you specify and continues to be sent indefinitely.

You can replace an existing send lifetime value by issuing the **send-lifetime** command again, and specifying new parameters.

Use the **no** form of this command to specify that the key is no longer to be sent.

## Examples

The following example establishes a send lifetime of January 25, 2002 at one minute and one second after 4:00 a.m. The key continues to be accepted indefinitely.

```
[local]Redback(config-key-chain)#send-lifetime 2002:25:04:01:01
```

The following example establishes a send lifetime of January 25, 2002 at exactly midnight, and specifies that the key is to be sent for 30 minutes (1800 seconds):

```
[local]Redback(config-key-chain)#send-lifetime 2002:25:00:00 duration 1800
```

## Related Commands

**accept-lifetime**





# Lawful Intercept Configuration

---

This chapter describes the tasks and commands used to configure SmartEdge® OS lawful intercept (LI) features.

For information about tasks and commands used to monitor, troubleshoot, and administer LI features, see the “Lawful Intercept Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

This chapter contains the following sections:

- Overview
- Configuration Tasks
- Configuration Examples
- Command Descriptions

## Overview

---

LI enables service providers to mirror subscriber packets and send them to a mediation device (MD), which can be anywhere in the network. The SmartEdge OS can mirror packets from any circuit in the system, at the ingress or egress point, and send the mirrored packets to the MD using a User Datagram Protocol (UDP)/IP session.

## Configuration Tasks

---

**Note** In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the “Command Descriptions” section.

To configure and activate LI features, perform the tasks described in the following sections:

- Configure an LI Profile
- Configure Circuits for LI
- Activate an Intercept

## Configure an LI Profile

To configure an LI profile, perform the tasks described in Table 19-1; enter all commands in LI profile configuration mode, unless otherwise noted.

**Table 19-1 Configure an LI Profile**

| #  | Task                                                                     | Root Command         | Notes                                            |
|----|--------------------------------------------------------------------------|----------------------|--------------------------------------------------|
| 1. | Create or select an LI profile and access LI profile configuration mode. | <b>li-profile</b>    | Enter this command in global configuration mode. |
| 2. | Specify the type of intercept.                                           | <b>type</b>          |                                                  |
| 3. | Define the transport data section for this LI profile to use UDP/IP.     | <b>transport udp</b> |                                                  |
| 4. | Define the specified field in the LI profile header.                     | <b>header</b>        | Enter this command for each field in the header. |
| 5. | Enable pending intercept requests.                                       | <b>pending</b>       |                                                  |

## Configure Circuits for LI

To configure circuits on which you can activate intercepts, perform the tasks described in Table 19-2.

**Table 19-2 Configure a Circuit for LI**

| #  | Task                                                      | Root Command | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|-----------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Configure the context.                                    |              | For information about configuring contexts, see the "Context Configuration" chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS.                                                                                                                                                                                                                                                                                                                                           |
| 2. | Configure the interfaces for the circuits and MD.         |              | For information about configuring interfaces, see the "Interface Configuration" chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS.                                                                                                                                                                                                                                                                                                                                       |
| 3. | Configure the subscribers.                                |              | For information about configuring subscribers, see the "Subscriber Configuration" chapter in the <i>Basic System Configuration Guide</i> for the SmartEdge OS.                                                                                                                                                                                                                                                                                                                                     |
| 4. | Configure the circuits.                                   |              | For information about configuring ports and circuits, see the "ATM, Ethernet, and POS Ports Configuration," "Clear-Channel and Channelized Ports and Channels Configuration," and "Circuits Configuration" chapters in the <i>Ports, Circuits, and Tunnels Configuration Guide</i> for the SmartEdge OS. For information about binding port, channels, and circuits, see the "Bindings Configuration" chapter in the <i>Ports, Circuits, and Tunnels Configuration Guide</i> for the SmartEdge OS. |
| 5. | Configure one or more IP ACLs to use with the intercepts. |              | For information about configuring IP ACLs, see Chapter 8, "ACL Configuration."                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Activate an Intercept

To activate an intercept perform one of the tasks described in Table 19-3; enter all commands in exec mode. These command are described in the “Lawful Intercept Operations” chapter in the *IP Services and Security Operations Guide* for the SmartEdge OS.

**Table 19-3 Activate an Intercept**

| Task                                               | Root Command                     | Notes                                         |
|----------------------------------------------------|----------------------------------|-----------------------------------------------|
| Start or stop an intercept on a specified circuit. | <b>intercept circuit</b>         | Use the <b>no</b> form to stop the intercept. |
| Start or stop an intercept for a remote agent.     | <b>intercept remote-agent-id</b> | Use the <b>no</b> form to stop the intercept. |
| Start or stop an intercept for a subscriber.       | <b>intercept subscriber</b>      | Use the <b>no</b> form to stop the intercept. |

## Configuration Examples

The following example configures the context, interfaces, an ACL, and an LI profile; it then configures the ports and starts an intercept:

```
!Configure the context and interfaces for subscriber traffic
[local]Redback(config)#context isp1
[local]Redback(config-ctx)#interface subs multibind
[local]Redback(config-if)#ip address 10.1.1.1/24
[local]Redback(config-if)#ip pool 10.1.1.0/24
[local]Redback(config-if)#exit

[local]Redback(config-ctx)#interface egress
[local]Redback(config-if)#ip address 5.1.1.1/21
[local]Redback(config-if)#exit

!Configure the interface to the MD system
[local]Redback(config-ctx)#interface toMD
[local]Redback(config-if)#ip address 1.1.1.1/21
[local]Redback(config-if)#exit

!Configure authentication and a default profile for subscribers
[local]Redback(config-ctx)#aaa authentication subscriber none
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#ip address pool
[local]Redback(config-sub)#exit

!Create a subscriber record
[local]Redback(config-ctx)#subscriber usr5
[local]Redback(config-sub)#exit

!Create an ACL for the intercepts
[local]Redback(config-ctx)#ip access list acl-both
[local]Redback(config-access-list)#seq 10 permit ip any 5.0.0.0 0.255.255.255
[local]Redback(config-access-list)#seq 20 permit ip 100.1.1.0 0.0.0.255 any
[local]Redback(config-access-list)#seq 30 deny ip any 200.0.0.0 0.255.255.255
```

```
[local]Redback(config-access-list)#seq 40 deny ip 201.1.1.0 0.0.0.255 any
[local]Redback(config-access-list)#exit

!Configure the LI profile
[local]Redback(config)#li-profile li-001
[local]Redback(config-liprofile)#type ip-datagrams
[local]Redback(config-liprofile)#transport udp destination 1.1.1.2 4000 context isp1
source 1.1.1.1 5000
[local]Redback(config-liprofile)#header li-id
[local]Redback(config-liprofile)#header seq-no
[local]Redback(config-liprofile)#header session-id
[local]Redback(config-liprofile)#header label "Redback SE800"
[local]Redback(config-liprofile)#pending
[local]Redback(config-liprofile)#exit

!Configure the ports for subscriber traffic
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind subscriber usr5@isp1 password pass
[local]Redback(config-port)#exit

[local]Redback(config)#port ethernet 5/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface egress isp1
[local]Redback(config-port)#exit

!Configure the port for MD traffic
[local]Redback(config)#port ethernet 14/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface toMD isp1
[local]Redback(config-port)#exit

!Activate a subscriber intercept for both incoming and outgoing traffic on port 5/1
[local]Redback#intercept subscriber usr5@isp1 li-profile li-001 li-id 001 label usr5
traffic acl acl-both

!Activate a circuit intercept (instead of the subscriber intercept) for both incoming
and outgoing traffic on port 5/1
[local]Redback#intercept circuit 5/1 li-profile li-001 li-id 001 label port 5/1 traffic
acl acl-both
```

## Command Descriptions

---

This section describes the syntax and usage guidelines for the commands used to configure and activate LI features. The commands are presented in alphabetical order.

**header**  
**li-profile**  
**pending**

**transport udp**  
**type**

## header

**header** {*label description* | **li-id** | **seq-no** | **session-id**}

**no header** {*label* | **li-id** | **seq-no** | **session-id**}

### Purpose

Defines the specified field in the header for this lawful intercept (LI) profile.

### Command Mode

LI profile configuration (15, authorized LI administrator only)

### Syntax Description

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>label</b> <i>description</i> | Description for this profile. An alphanumeric string with 0 to 15 characters; if more than one word, enclose it in quotation marks (" "). The <i>description</i> argument is not entered in the <b>no</b> form. |
| <b>li-id</b>                    | Specifies a placeholder for the identifier that you assign to an intercept when you start it using this LI profile.                                                                                             |
| <b>seq-no</b>                   | Specifies a placeholder for a system-assigned packet sequence number.                                                                                                                                           |
| <b>session-id</b>               | Specifies a placeholder for the system-assigned session identifier.                                                                                                                                             |

### Default

The header is undefined.

### Usage Guidelines

Use the **header** command to define the specified field in the header for this LI profile.

Use the **no** form of this command to delete the specified field from the header configuration.

### Examples

The following example creates a header for the MD-001 LI profile:

```
[local]Redback(config)#li-profile MD-001
[local]Redback(config-liprofile)#header li-id
[local]Redback(config-liprofile)#header seq-no
[local]Redback(config-liprofile)#header session-id
[local]Redback(config-liprofile)#header label "Redback SE800"
```

### Related Commands

**li-profile**  
**pending**

**transport udp**  
**type**

## li-profile

**li-profile** *name*

**no li-profile** *name*

### Purpose

Creates or selects a lawful intercept (LI) profile and accesses LI profile configuration mode.

### Command Mode

global configuration (15, authorized LI administrator only)

### Syntax Description

*name*                                      Name of the LI profile to be created or selected.

### Default

No LI profiles are created.

### Usage Guidelines

Use the **li-profile** command to create or select an LI profile and access LI profile configuration mode.

Use the **no** form of this command to delete the specified profile.

### Examples

The following example creates an LI profile, `li-001`, and accesses LI profile configuration mode:

```
[local]Redback(config)#li-profile li-001
[local]Redback(config-liprofile)#
```

### Related Commands

**header**  
**pending**  
**transport udp**  
**type**

# pending

**pending**

**no pending**

## Purpose

Enables pending intercept requests.

## Command Mode

LI profile configuration (15, authorized LI administrator only)

## Syntax Description

This command has no keywords or arguments.

## Default

The system rejects an intercept request if the subscriber circuit to which this profile is attached is down.

## Usage Guidelines

Use the **pending** command to enable pending intercept requests.

Use the **no** form of this command to specify the default condition (intercept requests are rejected for subscriber circuits that are down).

## Examples

The following example enables pending intercept requests for the `li-001` profile:

```
[local]Redback(config)#li-profile li-001  
[local]Redback(config-liprofile)#pending
```

## Related Commands

**header**  
**li-profile**  
**transport udp**  
**type**

## transport udp

**transport udp destination** *md-ip-addr md-udp-port* **context** *ctx-name*  
**source** *src-ip-addr src-udp-port* [**dscp** *dscp-class* | **tos** *tos-value*]

### Purpose

Defines the transport data section for this lawful intercept (LI) profile to use the User Datagram Protocol (UDP) over IP (UDP/IP).

### Command Mode

LI profile configuration (15, authorized LI administrator only)

### Syntax Description

|                                |                                                                                                                                                                                                                                                            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>destination</b>             | Specifies the destination address for the mediation device (MD) to which the SmartEdge OS sends the mirrored traffic.                                                                                                                                      |
| <i>md-ip-addr</i>              | IP address for the MD.                                                                                                                                                                                                                                     |
| <i>md-udp-port</i>             | UDP port number for the MD. The range of values is 1 to 65,535.                                                                                                                                                                                            |
| <b>context</b> <i>ctx-name</i> | Name of the context in which the interface is configured with the destination IP address.                                                                                                                                                                  |
| <b>source</b>                  | Specifies the source address of the mirrored traffic.                                                                                                                                                                                                      |
| <i>src-ip-addr</i>             | Source IP address of the mirrored traffic.                                                                                                                                                                                                                 |
| <i>src-udp-port</i>            | Source UDP port number of the mirrored traffic. The range of values is 1 to 65,535.                                                                                                                                                                        |
| <b>dscp</b> <i>dscp-class</i>  | Optional. Differentiated Services Code Point (DSCP) priority for which the traffic is mirrored. Values can be: <ul style="list-style-type: none"> <li>An integer from <b>0</b> to <b>63</b>.</li> <li>One of the keywords listed in Table 19-4.</li> </ul> |
| <b>tos</b> <i>tos-value</i>    | Optional. Type of service (TOS) for which the traffic is mirrored. The range of values is 0 to 255.                                                                                                                                                        |

### Default

The transport section is undefined.

### Usage Guidelines

Use the **transport udp** command to define the transport data section for this LI profile to use UDP/IP.

Use the **destination** keyword with the *md-ip-addr* and *md-udp-port* arguments to specify the IP address and UDP port for the MD to which the SmartEdge OS sends the intercepted traffic.



Use the **context** *ctx-name* construct to specify the context in which you have configured an interface with the destination IP address.

Use the **source** keyword with the *src-ip-addr* and *src-udp-port* arguments to specify the IP address and UDP port for the IP address and UDP port for the traffic to be intercepted.

If you do not specify the **dscp** *dscp-class* or **tos** *tos-value* construct, the field defaults to the DSCP class af41.

Table 19-4 lists the keywords for the *dscp-class* argument.

**Table 19-4 DSCP Class Keywords**

| DSCP Class                                         | Keyword     | DSCP Class                                    | Keyword                         |
|----------------------------------------------------|-------------|-----------------------------------------------|---------------------------------|
| Assured Forwarding (AF) Class 1 /Drop precedence 1 | <b>af11</b> | Class Selector 0 (same as default forwarding) | <b>cs0</b> (same as <b>df</b> ) |
| AF Class 1/Drop precedence 2                       | <b>af12</b> | Class Selector 1                              | <b>cs1</b>                      |
| AF Class 1/Drop precedence 3                       | <b>af13</b> | Class Selector 2                              | <b>cs2</b>                      |
| AF Class 2/Drop precedence 1                       | <b>af21</b> | Class Selector 3                              | <b>cs3</b>                      |
| AF Class 2/Drop precedence 2                       | <b>af22</b> | Class Selector 4                              | <b>cs4</b>                      |
| AF Class 3/Drop precedence 3                       | <b>af23</b> | Class Selector 5                              | <b>cs5</b>                      |
| AF Class 3/Drop precedence 1                       | <b>af31</b> | Class Selector 6                              | <b>cs6</b>                      |
| AF Class 3/Drop precedence 2                       | <b>af32</b> | Class Selector 7                              | <b>cs7</b>                      |
| AF Class 3/Drop precedence 3                       | <b>af33</b> | Default Forwarding (same as Class Selector 0) | <b>df</b> (same as <b>cs0</b> ) |
| AF Class 4/Drop precedence 1                       | <b>af41</b> | Expedited Forwarding                          | <b>ef</b>                       |
| AF Class 4/Drop precedence 2                       | <b>af42</b> |                                               |                                 |
| AF Class 4/Drop precedence 3                       | <b>af43</b> |                                               |                                 |

## Examples

The following example defines the transport data section in the **li-001** profile:

```
[local]Redback(config)#li-profile li-001
[local]Redback(config-liprofile)#transport udp destination 10.1.1.1 2001 context local
source 10.1.1.2 3001 dscp af41
```

## Related Commands

**header**  
**li-profile**  
**pending**  
**type**

# type

**type ip-datagrams**

## Purpose

Defines the type of intercept for this lawful intercept (LI) profile.

## Command Mode

LI profile configuration (15, authorized LI administrator only)

## Syntax Description

**ip-datagrams**      Specifies that IP datagrams are to be intercepted.

## Default

None

## Usage Guidelines

Use the **type** command to define the type of intercept for this LI profile.

Use the **no** form of this command to erase the type of intercept from this LI profile.

## Examples

The following example defines IP datagrams as the type of traffic to be intercepted:

```
[local]Redback(config)#li-profile li-0001  
[local]Redback(config-liprofile)#type ip-datagrams
```

## Related Commands

**li-profile**

# Appendixes

---

This part describes attributes used with Remote Authentication Dial-In User Service (RADIUS) and attribute-value pairs (AVPs) used with Terminal Access Controller Access Control System Plus (TACACS+), and consists of the following appendixes:

- Appendix A, “RADIUS Attributes”
- Appendix B, “TACACS+ Attribute-Value Pairs”



# RADIUS Attributes

---

This appendix describes standard Remote Authentication Dial-In User Service (RADIUS) and vendor-specific attributes (VSAs) supported by the SmartEdge® OS.

For information about configuring RADIUS features, see Chapter 16, “RADIUS Configuration.”

For more information about RADIUS attributes, see the following documents:

- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*

This appendix contains the following sections:

- Overview
- Supported Standard RADIUS Attributes
- Redback VSAs

## Overview

---

Internet Engineering Task Force (IETF) RADIUS attributes are the original set of 255 standard attributes used to communicate authentication, authorization, and accounting (AAA) information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known so that all clients and servers can exchange AAA information. RADIUS VSAs are derived from one IETF RADIUS attribute 26, Vendor-Specific, which enables a vendor, in this case, Redback Networks, to create an additional 255 attributes.

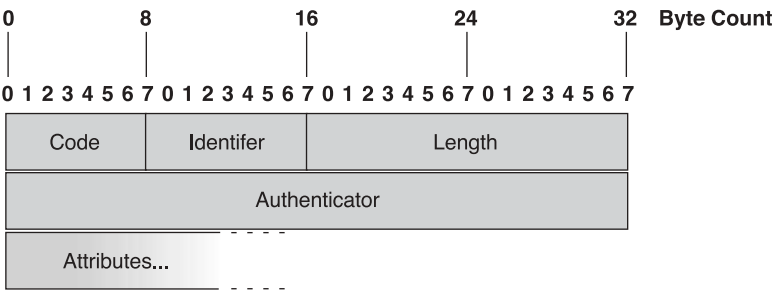
RADIUS packets and files are described further in the following sections:

- RADIUS Packet Format
- Packet Types
- RADIUS Files

# RADIUS Packet Format

Figure A-1 illustrates the format of a RADIUS packet.

Figure A-1 RADIUS Packet Format)



0797

Table A-1 describes the fields contained in a RADIUS packet.

Table A-1 RADIUS Packet Fields

| Field         | Description                                                                                                                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Code          | Identifies the RADIUS packet type. The type can be one of the following: <ul style="list-style-type: none"><li>• Access-Request (1)</li><li>• Access-Accept (2)</li><li>• Access-Reject (3)</li><li>• Accounting-Request (4)</li><li>• Accounting-Response (5)</li></ul>                                                                                      |
| Identifier    | Helps the RADIUS server match request and responses and detect duplicate requests.                                                                                                                                                                                                                                                                            |
| Length        | Specifies the length of the entire packet.                                                                                                                                                                                                                                                                                                                    |
| Authenticator | Authenticates the reply from the RADIUS server. There are two types of authenticators: <ul style="list-style-type: none"><li>• Request-Authentication (available in Access-Request and Accounting-Request packets)</li><li>• Response-Authentication (available in Access-Accept, Access Reject, Access-Challenge, and Accounting-Response packets)</li></ul> |

## Packet Types

Table A-2 describes RADIUS packet types.

Table A-2 RADIUS Packet Types

| Type           | Description                                                                                                                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access-Request | Sent from a client to a RADIUS server. The RADIUS server uses the packet to determine whether to allow access to a specific network access server (NAS), which permits subscriber access. Subscribers performing authentication must submit an Access-Request packet. When an Access-Request packet is received, the RADIUS server must forward a reply. |
| Access-Accept  | Upon receiving an Access-Request packet, the RADIUS server sends an Access-Accept packet if all attribute values in the Access-Request packet are acceptable.                                                                                                                                                                                            |
| Access-Reject  | Upon receiving an Access-Request packet, the RADIUS server sends an Access-Reject packet if any of the attribute values are not acceptable.                                                                                                                                                                                                              |

**Table A-2 RADIUS Packet Types** (*continued*)

| Type                | Description                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access-Challenge    | Upon receiving an Access-Request packet, the RADIUS server can send the client an Access-Challenge packet, which requires a response. If the client does not know how to respond, or if the packets are invalid, the RADIUS server discards the packets. If the client responds to the packet, a new Access-Request packet is sent with the original Access-Request packet. |
| Accounting-Request  | Sent from a client to a RADIUS accounting server. If the RADIUS accounting server successfully records the Accounting-Request packet, it must submit an Accounting-Response packet.                                                                                                                                                                                         |
| Accounting-Response | Sent by the RADIUS accounting server to the client to acknowledge that the Accounting-Request has been received and recorded successfully.                                                                                                                                                                                                                                  |

## RADIUS Files

RADIUS files communicate AAA information between a client and server. These files are described in the following sections:

- RADIUS Dictionary File
- RADIUS Clients Files
- Subscriber Files

### RADIUS Dictionary File

Table A-3 describes the information contained in a RADIUS dictionary file.

**Table A-3 RADIUS Dictionary File**

| Name                                                        | ID                                                                                    | Value Type                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASCII string name of the attribute; for example, User-Name. | Numerical identification of the attribute; for example, the User-Name attribute is 1. | Each attribute can be specified through one of the following value types: <ul style="list-style-type: none"> <li>• binary—0 to 254 octets.</li> <li>• date—32-bit value in big endian order; for example, seconds since 00:00:00 GMT, JAN. 1, 1970.</li> <li>• ipadd—4 octets in network byte order.</li> <li>• integer—32-bit value in big endian order (high byte first).</li> <li>• string—0 to 253 octets.</li> </ul> |

An integer can be expanded to represent a string. The following example is an integer-based attribute and its corresponding string values. In this example, the values for VSA 144, Acct-Reason, describe the reason for sending subscriber accounting packets to the RADIUS server. Each value is represented by an integer.

```
#
ATTRIBUTE    Acct-Reason    144                Integer
VALUE        AAA_LOAD_ACCT_SESSION_UP        1
VALUE        AAA_LOAD_ACCT_SESSION_DOWN      2
VALUE        AAA_LOAD_ACCT_PERIODIC           3
.
.
.
```

### RADIUS Clients Files

A clients file contains a list of RADIUS clients allowed to send authentication and accounting requests to the RADIUS server. To receive authentication, the client name and authentication key sent to the RADIUS server must be an exact match with the data contained in the clients file; see the following example:

```
#
Client Name      Key
10.1.1.1         test
nas-1            secret
```

### Subscriber Files

A subscriber file contains an entry for each subscriber that the RADIUS server will authenticate. The first line in any subscriber file is a “user access” line; that is, the server must check the attributes on the first line before it can grant access to the user.

The following example allows the subscriber to access five tunnel attributes:

```
#
redback.com Password="redback" Service-Type Outbound
Tunnel-Type = :1:L2TP
Tunnel-Medium-Type = :1:IP
Tunnel-Server-Endpoint = :1:10.0.0.1
Tunnel-Password = :1:"welcome"
Tunnel-Assignment-ID = :1:"nas"
```

## Supported Standard RADIUS Attributes

---

Table A-4 describes the standard RADIUS attributes supported by the SmartEdge OS.

**Table A-4 Standard RADIUS Attributes Supported by the SmartEdge OS**

| # | Attribute Name | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                       |
|---|----------------|------------------------|----------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | User-Name      | Yes                    | Yes                  | No                            | String. Name of the user to be authenticated; only used in Access-Request packets.                                                                                                                                                                                                          |
| 2 | User-Password  | Yes                    | No                   | No                            | String. Sent unless using the CHAP-Password attribute.                                                                                                                                                                                                                                      |
| 3 | CHAP-Password  | Yes                    | No                   | No                            | String. Sent in Access-Request packet unless using the User-Password attribute.                                                                                                                                                                                                             |
| 4 | NAS-IP-Address | Yes                    | Yes                  | No                            | IP address. Specifies an IP source address for RADIUS packets sent by the SmartEdge router.<br><br>This attribute is not sent unless explicitly enabled through the <b>radius attribute nas-ip-address</b> command (in context configuration mode); see Chapter 16, “RADIUS Configuration.” |
| 5 | NAS-Port       | Yes                    | Yes                  | No                            | Integer. This attribute is sent using the <b>slot-port</b> format. For details on this format or to modify the format in which this attribute is sent, see the <b>radius attribute nas-port</b> command in Chapter 16, “RADIUS Configuration.”                                              |



Table A-4 Standard RADIUS Attributes Supported by the SmartEdge OS (*continued*)

| #  | Attribute Name    | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|-------------------|------------------------|----------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6  | Service-Type      | Yes                    | Yes                  | Yes                           | Integer. Type of service requested or provided. Values are: <ul style="list-style-type: none"> <li>• 2=Framed</li> <li>• 5=Outbound</li> <li>• 6=Administrative</li> <li>• 7=NAS Prompt</li> </ul>                                                                                                                                                                                                                                                                              |
| 7  | Framed-Protocol   | Yes                    | Yes                  | Yes                           | Integer. The value indicates the framing to be used for framed access. This attribute must not be used in a user profile designed for RFC 1483 and RFC 1490 bridged or routed circuits, or for Telnet sessions. This value is sent only for Point-to-Point Protocol (PPP) service types. The value for PPP is 1.                                                                                                                                                                |
| 8  | Framed-IP-Address | Yes                    | Yes                  | Yes                           | IP address. In Accounting-Request packets, returns the IP address assigned to the subscriber either dynamically or statically. In Access-Accept packets, a return value of 255.255.255.254 or 0.0.0.0 causes the SmartEdge OS to assign the subscriber an address from an IP address pool. This attribute is received in Access-Response messages and is sent in Access-Request messages conditioned by the <b>aaa hint ip address</b> command (in context configuration mode). |
| 9  | Framed-IP-Netmask | No                     | Yes                  | Yes                           | IP address. Assigns a range of addresses to a subscriber circuit—it is not a netmask in the conventional sense of determining which address bits are host vs. prefix, and so on.                                                                                                                                                                                                                                                                                                |
| 11 | Filter-Id         | No                     | Yes                  | Yes                           | String. Specifies that inbound or outbound traffic be filtered. Use the <b>in:&lt;name&gt;</b> and <b>out:&lt;name&gt;</b> format.                                                                                                                                                                                                                                                                                                                                              |
| 12 | Framed-MTU        | No                     | Yes                  | Yes                           | Integer. Maximum transmission unit (MTU) to be configured for the user when it is not negotiated by some other means (such as Point-to-Point Protocol [PPP]). It is only used in Access-Accept packets.                                                                                                                                                                                                                                                                         |
| 18 | Reply-Message     | No                     | No                   | Yes                           | String. Text that can be displayed to the user. Multiple Reply-Message attributes can be included. If any are displayed, they must be displayed in the same order as they appear in the packet.                                                                                                                                                                                                                                                                                 |
| 22 | Framed-Route      | No                     | Yes                  | Yes                           | IP address. The format is <i>h.h.h.hnn g.g.g.g n</i> where: <ul style="list-style-type: none"> <li>• <i>h.h.h.h</i>=IP address of destination host or network.</li> <li>• <i>nn</i>=optional netmask size in bits (if not present, defaults to 32).</li> <li>• <i>g.g.g.g</i>=IP address of gateway.</li> <li>• <i>n</i>=Number of hops for this route.</li> </ul>                                                                                                              |
| 25 | Class             | No                     | Yes                  | Yes                           | String. If received, this information must be sent on, without interpretation, in all subsequent packets sent to the RADIUS accounting server for that subscriber session.                                                                                                                                                                                                                                                                                                      |
| 26 | Vendor-Specific   | Yes                    | Yes                  | No                            | String. Allows Redback Networks to support its own VSAs. embedded with the Vendor-Id attribute set to 2352. See Table A-6 for the VSAs supported by the SmartEdge OS.                                                                                                                                                                                                                                                                                                           |

Table A-4 Standard RADIUS Attributes Supported by the SmartEdge OS (*continued*)

| #  | Attribute Name     | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|--------------------|------------------------|----------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 27 | Session-Timeout    | No                     | Yes                  | Yes                           | Integer. Sets the maximum number of seconds of service allowed the subscriber before termination of the session. Corresponds to the SmartEdge OS <b>timeout</b> command (in subscriber configuration mode) with the <b>absolute</b> keyword, except that the attribute requires seconds instead of minutes. The value 0 indicates that the timeout is disabled.                                                                                                                                                    |
| 28 | Idle-Timeout       | No                     | Yes                  | Yes                           | Integer. Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session. Corresponds to the SmartEdge OS <b>timeout idle</b> command (in subscriber configuration mode), except that the attribute calls for seconds instead of minutes.                                                                                                                                                                                                                  |
| 30 | Called-Station-Id  | Yes                    | No                   | No                            | String. The telephone number that the call came from.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 31 | Calling-Station-Id | Yes                    | Yes                  | No                            | Dependent on the type of subscriber terminated in the SmartEdge router: <ul style="list-style-type: none"> <li>• CLIPS subscribers: GIADDR (gateway IP address) for the CLIPS session; the address is received via a Dynamic Host Configuration Protocol (DHCP) relay network.</li> <li>• PPP subscribers: this attribute is not sent unless explicitly enabled through the <b>radius attribute calling-station-id</b> command (in context configuration mode); see Chapter 16, "RADIUS Configuration."</li> </ul> |
| 32 | NAS-Identifier     | Yes                    | Yes                  | No                            | String. Value for the system hostname.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 40 | Acct-Status-Type   | No                     | Yes                  | No                            | Integer. Values can be: <ul style="list-style-type: none"> <li>• 1=Start</li> <li>• 2 =Stop</li> <li>• 3=Interim-Updated</li> <li>• 7=Accounting-On</li> <li>• 8=Accounting-Off</li> <li>• 9=Tunnel Start</li> <li>• 10=Tunnel Stop</li> <li>• 12=Link Start</li> <li>• 13=Link Stop</li> <li>• 15=Reserved for failed</li> </ul>                                                                                                                                                                                  |
| 41 | Acct-Delay-Time    | No                     | Yes                  | No                            | Integer. Time, in seconds, for which the client has been trying to send the record.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 42 | Acct-Input-Octets  | No                     | Yes                  | No                            | Integer. Number of octets that have been received from the port over the course of this service being provided. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.                                                                                                                                                                                                                                                                                   |
| 43 | Acct-Output-Octets | No                     | Yes                  | No                            | Integer. Number of octets that have been sent to the port in the course of delivering this service. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.                                                                                                                                                                                                                                                                                               |

Table A-4 Standard RADIUS Attributes Supported by the SmartEdge OS (continued)

| #  | Attribute Name        | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------|------------------------|----------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 44 | Acct-Session-Id       | Yes                    | Yes                  | No                            | String. Unique accounting ID to match start and stop records for in a log file. The start and stop records for a given subscriber session have the same Acct-Session-Id attribute value. The format is <i>cct_handle timestamp</i> .<br>By default, this attribute is sent in Accounting-Request packets. To send this attribute in Access-Request packets, you must use the <b>radius attribute acct-session-id</b> command (in context configuration mode); see Chapter 16, "RADIUS Configuration." |
| 45 | Acct-Authentic        | No                     | Yes                  | No                            | String. Values are RADIUS and local.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 46 | Acct-Session-Time     | No                     | Yes                  | No                            | Integer. Number of seconds for which the user has received service. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.                                                                                                                                                                                                                                                                                                                  |
| 47 | Acct-Input-Packets    | No                     | Yes                  | No                            | Integer. Number of packets that have been received from the port over the course of this service being provided to a framed user. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.                                                                                                                                                                                                                                                    |
| 48 | Acct-Output-Packets   | No                     | Yes                  | No                            | Integer. Number of packets that have been sent to the port in the course of delivering this service to a Framed User. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.                                                                                                                                                                                                                                                                |
| 49 | Acct-Terminate-Cause  | No                     | Yes                  | No                            | Integer. Value represents the cause of session termination. Values are: <ul style="list-style-type: none"> <li>• 1=User request</li> <li>• 2=Lost carrier</li> <li>• 3=Lost service</li> <li>• 4=Idle timeout</li> <li>• 5=Session timeout</li> <li>• 6=Admin reset</li> <li>• 8=Port error</li> <li>• 9=NAS error</li> <li>• 10=NAS request</li> <li>• 15=Service unavailable</li> <li>• 17=User error</li> </ul>                                                                                    |
| 52 | Acct-Input-Gigawords  | No                     | Yes                  | No                            | Integer. Value represents the number of times the Acct-Input-Octets counter has wrapped around $2^{32}$ in the course of providing this service. This attribute can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Interim-Update.                                                                                                                                                                                                              |
| 53 | Acct-Output-Gigawords | No                     | Yes                  | No                            | Integer. Value represents the number of times the Acct-Output-Octets counter has wrapped around $2^{32}$ in the course of delivering this service. This attribute can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Interim-Update.                                                                                                                                                                                                            |
| 55 | Event-Timestamp       | No                     | Yes                  | No                            | Integer. Value represents the time this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.                                                                                                                                                                                                                                                                                                                                                                                       |

Table A-4 Standard RADIUS Attributes Supported by the SmartEdge OS (*continued*)

| #  | Attribute Name         | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|------------------------|------------------------|----------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 61 | NAS-Port-Type          | Yes                    | Yes                  | No                            | <p>Integer. The default value is either 0 or 5, indicating an asynchronous connection through a console port or a connection through a transport protocol, respectively, depending on how the subscriber is connected to its authenticating NAS. The range of values is 0 to 255. Values 0 to 19 are as follows:</p> <ul style="list-style-type: none"> <li>• 0—async</li> <li>• 1—sync</li> <li>• 2—ISDN (sync)</li> <li>• 3—ISDN (async V120)</li> <li>• 4—ISDN (async V110)</li> <li>• 5—Virtual</li> <li>• 6—PIAFS (wireless ISDN used in Japan)</li> <li>• 7—HDLC (clear-channel)</li> <li>• 8—X.25</li> <li>• 9—X.75</li> <li>• 10—G3_Fax (G.3 Fax)</li> <li>• 11—SDSL (Symmetric DSL)</li> <li>• 12—ADSL_CAP (Asymmetric DSL, Carrierless Amplitude Phase Modulation)</li> <li>• 13—ADSL_DMT (Asymmetric DSL, Discrete Multi-Tone)</li> <li>• 14—IDSL (ISDN Digital Subscriber Line)</li> <li>• 15—Ethernet</li> <li>• 16—xDSL (Digital Subscriber Line of unknown type)</li> <li>• 17—Cable</li> <li>• 18—Wireless (Wireless - Other)</li> <li>• 19—Wireless_802_11 (Wireless - IEEE 802.11)</li> </ul> <p>You can also modify the value of this attribute through the <b>radius attribute nas-port-type</b> command (in context configuration mode); see Chapter 16, “RADIUS Configuration.”</p> |
| 62 | Port-Limit             | No                     | Yes                  | Yes                           | Integer. Maximum number of sessions a particular subscriber can have active at one time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 64 | Tunnel-Type            | No                     | Yes                  | Yes                           | Integer. Value indicates the tunneling protocol to be used. The supported value is 3, which indicates the Layer 2 Tunneling Protocol (L2TP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 65 | Tunnel-Medium-Type     | No                     | Yes                  | Yes                           | Integer. Value represents the transport medium to use when creating an L2TP tunnel for protocols that can operate over multiple transports. The supported value is 1, which indicates IPv4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 66 | Tunnel-Client-Endpoint | No                     | Yes                  | Yes                           | String. Fully qualified domain name or IP address of the initiator end of an L2TP tunnel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 67 | Tunnel-Server-Endpoint | No                     | Yes                  | Yes                           | String. Fully qualified domain name or IP address of the server end of an L2TP tunnel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 68 | Acct-Tunnel-Connection | No                     | Yes                  | No                            | String. Unique accounting ID to easily match start and stop records in a log file for L2TP sessions. The start and stop records for a given session will have the same Acct-Tunnel-Connection attribute value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 69 | Tunnel-Password        | No                     | No                   | Yes                           | String. Password. Only used in Access-Accept packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table A-4 Standard RADIUS Attributes Supported by the SmartEdge OS (*continued*)

| #   | Attribute Name        | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|-----------------------|------------------------|----------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 77  | Connect-Info          | Yes                    | Yes                  | No                            | String containing either: <ul style="list-style-type: none"> <li>An ATM or Frame Relay profile name being sent to the RADIUS server.</li> <li>The values from L2TP attribute-value pairs (AVPs) 24 and 38 in the tx/rx format. Speeds are provided in bits-per-second.</li> </ul>                                                                                                                                                                                                                                                          |
| 82  | Tunnel-Assignment-ID  | No                     | Yes                  | Yes                           | String. Used to distinguish between different peers with configurations that use the same IP address. If no Tunnel-Client-Endpoint or Tunnel-Server-Endpoint attribute is supplied with this tag, and if the Tunnel-Assignment-ID matches the name of a locally configured peer, the session will be tunneled to that peer.                                                                                                                                                                                                                |
| 83  | Tunnel-Preference     | No                     | No                   | Yes                           | String. If more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator, this attribute should be included in all sets to indicate the preference assigned to each set; the lower the value for a set, the more preferable it is.                                                                                                                                                                                                                                                                    |
| 87  | NAS-Port-Id           | Yes                    | Yes                  | No                            | String. By default, this attribute is sent in RADIUS packets. The default format is:<br><code>slot/port [vpi-vci vpi vci  <br/> vlan-id [tunl-vlan-id:]pvc-vlan-id] [pppoe sess-id  <br/> clips sess-id]</code> .<br>For example, 4/1 vpi-vci 207 138 pppoe 5.<br>Use the <b>radius attribute nas-port-id</b> command (in context configuration mode) to specify another format for this attribute. This command is described in Chapter 16, "RADIUS Configuration."                                                                       |
| 90  | Tunnel-Client-Auth-ID | No                     | Yes                  | Yes                           | String. Defines the local hostname provided to remote tunnel peer (used during tunnel setup). The behavior is identical to Redback VSA 16, Tunnel-Local-Name.                                                                                                                                                                                                                                                                                                                                                                              |
| 91  | Tunnel-Server-Auth-ID | No                     | Yes                  | Yes                           | String. Defines an alias for the remote peer name. The value of this attribute must match the value of the hostname AVP that the peer sends in the SCCRQ or SCCRQ message (depending on the tunnel initiator).                                                                                                                                                                                                                                                                                                                             |
| 242 | Ascend-Data-Filter    | No                     | Yes                  | Yes                           | Multivalued attribute. An Access-Accept packet contains multiple binary strings each representing a rule in an IP access control list (ACL). The rules are interpreted in the order they are received from the RADIUS server. If the RADIUS server returns both the SmartEdge OS Filter-Id and Ascend-Data-Filter attributes for the same subscriber in the same direction, the Ascend-Data-Filter attribute is ignored, the SmartEdge OS Filter-Id attribute is applied in that direction, and an event message to that effect is logged. |

Table A-5 lists the standard RADIUS attributes that are reauthorized when you enter the **reauthorize** command (in exec mode).

**Table A-5 Standard RADIUS Attributes Supported by Reauthorization**

| #  | Attribute Name  | Description                                                                                                                                                                                        |
|----|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11 | Filter-Id       | Filters inbound or outbound traffic through an access control list (ACL).                                                                                                                          |
| 25 | Class           | Forwards the information sent by the RADIUS server to the SmartEdge router, without interpretation, in subsequent accounting messages to the RADIUS accounting server for that subscriber session. |
| 27 | Session-Timeout | Sets the in-service time allowed before termination of the session.                                                                                                                                |
| 28 | Idle-Timeout    | Sets the idle time allowed before termination of the session.                                                                                                                                      |
| 62 | Port-Limit      | Sets the maximum number of ports to be provided to the user by the NAS.                                                                                                                            |

## Redback VSAs

Table A-6 lists the Redback VSAs supported by the SmartEdge OS.

**Table A-6 Redback VSAs Supported by the SmartEdge OS**

| #  | VSA Name           | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                               |
|----|--------------------|------------------------|----------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Client-DNS-Pri     | No                     | No                   | Yes                           | IP address of the primary DNS server for this subscriber's connection.                                                                                                                                              |
| 2  | Client-DNS-Sec     | No                     | No                   | Yes                           | IP address of the secondary DNS server for this subscriber's connection.                                                                                                                                            |
| 3  | DHCP-Max-Leases    | No                     | Yes                  | Yes                           | Integer. Maximum number of DHCP addresses this subscriber can allocate to hosts. The range of values is 1 to 255.                                                                                                   |
| 4  | Context-Name       | No                     | Yes                  | Yes                           | Binds the subscriber session to specified context, overriding the structured username. This information is only interpreted when global AAA is enabled.                                                             |
| 14 | Source-Validation  | No                     | Yes                  | Yes                           | Integer. Enables source validation for subscriber, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=TRUE</li> <li>• 0=FALSE</li> </ul>                                          |
| 15 | Tunnel-Domain      | No                     | No                   | Yes                           | Integer. Binds the subscriber to a tunnel based on the domain name portion of the username, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=TRUE</li> <li>• 0=FALSE</li> </ul> |
| 16 | Tunnel-Local-Name  | No                     | No                   | Yes                           | String. Defines the local hostname provided to the remote peer during tunnel setup.                                                                                                                                 |
| 17 | Tunnel-Remote-Name | No                     | No                   | Yes                           | String. Defines an alias for the remote peer name.                                                                                                                                                                  |

**Table A-6 Redback VSAs Supported by the SmartEdge OS** *(continued)*

| #  | VSA Name            | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|---------------------|------------------------|----------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18 | Tunnel-Function     | No                     | Yes                  | Yes                           | Integer. Determines this tunnel configuration as a LAC-only endpoint or an LNS endpoint, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=LAC only</li> <li>• 2=LNS only</li> </ul>                                                                                                                                                                                    |
| 21 | Tunnel-Max-Sessions | No                     | Yes                  | Yes                           | Integer. Limits the number of sessions per tunnel using this tunnel configuration.                                                                                                                                                                                                                                                                                                                         |
| 22 | Tunnel-Max-Tunnels  | No                     | Yes                  | Yes                           | Integer. Limits the number of tunnels that can be initiated using this tunnel configuration.                                                                                                                                                                                                                                                                                                               |
| 23 | Tunnel-Session-Auth | No                     | No                   | Yes                           | Integer. Specifies the authentication method to use during PPP authentication, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=CHAP</li> <li>• 2=PAP</li> <li>• 3=CHAP-PAP</li> </ul>                                                                                                                                                                                 |
| 24 | Tunnel-Window       | No                     | No                   | Yes                           | Integer. Configures the receive window size for incoming L2TP messages.                                                                                                                                                                                                                                                                                                                                    |
| 25 | Tunnel-Retransmit   | No                     | No                   | Yes                           | Integer. Specifies the number of times the SmartEdge router retransmits a control message.                                                                                                                                                                                                                                                                                                                 |
| 26 | Tunnel-Cmd-Timeout  | No                     | No                   | Yes                           | Integer. Specifies the number of seconds for the timeout interval between control message retransmissions.                                                                                                                                                                                                                                                                                                 |
| 27 | PPPOE-URL           | No                     | Yes                  | Yes                           | String in PPPoE URL format. Defines the PPPoE URL that is sent to the remote PPPoE client via the PADM packet.                                                                                                                                                                                                                                                                                             |
| 28 | PPPOE-MOTM          | No                     | Yes                  | Yes                           | String. Defines the PPPoE MOTM message that is sent to the remote PPPoE client via the PADM packet.                                                                                                                                                                                                                                                                                                        |
| 31 | Tunnel-Algorithm    | No                     | No                   | Yes                           | Integer. Specifies the session distribution algorithm used to choose between the peer configurations in the RADIUS response. This VSA instructs the SmartEdge OS on how to interpret standard RADIUS attribute 83, Tunnel-Preference, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=Priority</li> <li>• 2=Load-Balance</li> <li>• 3=Weighted round-robin</li> </ul> |
| 32 | Tunnel-Deadtime     | No                     | No                   | Yes                           | Integer. Specifies the number of minutes during which no sessions are attempted to an L2TP peer when the peer is down.                                                                                                                                                                                                                                                                                     |
| 33 | Mcast-Send          | No                     | Yes                  | Yes                           | Integer. Defines whether or not the subscriber can send multicast packets, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=NO SEND</li> <li>• 2=SEND</li> <li>• 3=UNSOLICITED SEND</li> </ul>                                                                                                                                                                         |

Table A-6 Redback VSAs Supported by the SmartEdge OS (*continued*)

| #  | VSA Name                | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|-------------------------|------------------------|----------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34 | Mcast-Receive           | No                     | Yes                  | Yes                           | Integer. Defines whether or not the subscriber can receive multicast packets, according to one of the following values: <ul style="list-style-type: none"> <li>• 1=NO RECEIVE</li> <li>• 2=RECEIVE</li> </ul>                                                                                                                                                                                                                                      |
| 35 | Mcast-MaxGroups         | No                     | Yes                  | Yes                           | Integer. Specifies the maximum number of multicast groups of which the subscriber can be a member.                                                                                                                                                                                                                                                                                                                                                 |
| 36 | Ip-Address-Pool-Name    | No                     | Yes                  | Yes                           | String. Name of the interface or IP pool used to assign an IP pool address to the subscriber.                                                                                                                                                                                                                                                                                                                                                      |
| 38 | Medium-Type             | Yes                    | Yes                  | No                            | Integer. Contains the medium type of the circuit as configured by the administrator in the ATM profile or the Ethernet port configuration, according to one of the following values: <ul style="list-style-type: none"> <li>• 11=DSL</li> <li>• 12=Cable</li> <li>• 13=Wireless</li> <li>• 14=Satellite</li> </ul>                                                                                                                                 |
| 39 | PVC-Encapsulation-Type  | No                     | No                   | Yes                           | Integer. Encapsulation type to be applied to the circuit: <ul style="list-style-type: none"> <li>• 2 = Routed 1483</li> <li>• 4 = ATM multi</li> <li>• 5 = Bridged 1483</li> <li>• 6 = ATM PPP</li> <li>• 7 = ATM PPP serial</li> <li>• 8 = ATM PPP NLPID</li> <li>• 9 = ATM PPP auto</li> <li>• 10 = ATM PPPoE</li> <li>• 12 = ATM PPP LLC</li> <li>• 22 = Ethernet IPoE</li> <li>• 23 = Ethernet PPPoE</li> <li>• 24 = Ethernet dot1q</li> </ul> |
| 40 | PVC-Profile-Name        | No                     | No                   | Yes                           | String. Name of the ATM profile that is assigned to the subscriber record, a named profile, or the default profile, using the <b>shaping profile</b> command (in subscriber configuration mode), to use for this circuit.                                                                                                                                                                                                                          |
| 42 | Bind-Type               | No                     | No                   | Yes                           | Integer. Binding type to be applied to this circuit: <ul style="list-style-type: none"> <li>• 1 = authentication</li> <li>• 3 = interface</li> <li>• 4 = subscriber</li> </ul>                                                                                                                                                                                                                                                                     |
| 43 | Bind-Auth-Protocol      | No                     | No                   | Yes                           | Integer. Authentication protocol to use for this circuit: <ul style="list-style-type: none"> <li>• 1 = PAP</li> <li>• 2 = CHAP</li> <li>• 4 = CHAP PAP</li> <li>• 6 = PAP CHAP</li> </ul>                                                                                                                                                                                                                                                          |
| 63 | Tunnel-Session-Auth-Ctx | No                     | Yes                  | Yes                           | String. L2TP peer parameter that specifies the name of the context in which all incoming PPP over L2TP sessions should be authenticated, regardless of the domain specified in the username.                                                                                                                                                                                                                                                       |



Table A-6 Redback VSAs Supported by the SmartEdge OS (continued)

| #  | VSA Name                | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-------------------------|------------------------|----------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 71 | PPPoE-IP-Route-Add      | No                     | Yes                  | Yes                           | String. Allows the PPPoE subscriber routing table to be populated in terms of what routes to be installed if multiple PPPoE sessions exist. A more granular set of routes can be achieved when multiple sessions are active to the client. The format is <i>h.h.h.h nn g.g.g.g m</i> where: <ul style="list-style-type: none"> <li>• <i>h.h.h.h</i>=IP address of destination host or network.</li> <li>• <i>nn</i>=optional netmask size in bits (if not present, defaults to 32).</li> <li>• <i>g.g.g.g</i>=IP address of gateway.</li> <li>• <i>m</i>=Number of hops for this route.</li> </ul>                                |
| 87 | Qos-Policy-Policing     | No                     | Yes                  | Yes                           | String. Attaches a QoS policing policy to the subscriber session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 88 | Qos-Policy-Metering     | No                     | Yes                  | Yes                           | String. Attaches a QoS metering policy to the subscriber session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 89 | Qos-Policy-Queuing      | No                     | Yes                  | Yes                           | String. Attaches a QoS queuing (scheduling) policy to the subscriber session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 90 | Igmp-Service-Profile-Id | No                     | Yes                  | Yes                           | String. Name of the IGMP service profile that is applied to the subscriber session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 91 | Sub-Profile-Name        | No                     | Yes                  | Yes                           | Name of the subscriber profile that is applied to the subscriber session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 92 | Forward-Policy          | No                     | Yes                  | Yes                           | String. Attaches an in or out forward policy to the subscriber session. The forward policy is in the following format:<br><b>in:</b> <i>forward-policy-name</i><br><b>out:</b> <i>forward-policy-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 93 | Remote-Port-String      | No                     | Yes                  | No                            | String.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 94 | Reauth-String           |                        |                      |                               | String. The format is:<br><b>ID-type;subID;attr-num;attr-value;attr-num;attr-value...</b><br>When the ID-type is 1, the subID is read as a RADIUS accounting session ID. When the ID-type is 2, the subID is read as a name.<br>The semicolon ( ; ) acts as a delimiter.<br>Attr - num is an integer that identifies a RADIUS attribute. For example, standard RADIUS attribute 11 (Filter-Id) for an access control list (ACL) or Redback VSA 87 (Qos-Policy-Policing) for a QoS policing policy. (Redback VSAs include the Redback prefix, 2352.)<br>Attr - value is the value of the RADIUS attribute specified by attr - num. |
| 95 | Reauth-More             |                        |                      |                               | Integer. 0 or 1 (False or True).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Table A-6 Redback VSAs Supported by the SmartEdge OS (*continued*)

| #   | VSA Name                   | Sent in Access-Request | Sent in Acct-Request               | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|----------------------------|------------------------|------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 96  | Remote-Agent-Id            | Yes                    | Yes                                | No                            | String. Used for two types of subscriber sessions: <ul style="list-style-type: none"> <li>Incoming CLIPS sessions to the SmartEdge router from a DHCP relay network. This is suboption 2 in a DHCP option 82 packet.</li> <li>PPPoE sessions. Sent by the PPP client in the PADR.</li> </ul> This attribute can also be set through the <b>radius attribute calling-station-id</b> and <b>radius attribute nas-port-id</b> commands in context configuration mode; see Chapter 16, "RADIUS Configuration." |
| 97  | Agent-Circuit-Id           | Yes                    | Yes                                | No                            | String. Used for two types of subscriber sessions: <ul style="list-style-type: none"> <li>CLIPS sessions coming into the SmartEdge via a DHCP relay network. This is suboption 1 in a DHCP option 82 packet.</li> <li>PPPoE sessions. Sent by the PPP client in the PADR.</li> </ul> This attribute can also be set through the <b>radius attribute calling-station-id</b> and <b>radius attribute nas-port-id</b> commands in context configuration mode; see Chapter 16, "RADIUS Configuration."         |
| 98  | Platform-Type              | Yes                    | Yes                                | No                            | Integer. Indicates the Redback product family from which the RADIUS access request is sent. The supported values are: <ul style="list-style-type: none"> <li>2=PLATFORM_TYPE_SE800</li> <li>3=PLATFORM_TYPE_SE400</li> </ul>                                                                                                                                                                                                                                                                               |
| 99  | RB-Client-NBNS-Pri         | No                     | Yes                                | Yes                           | IP address. Configures the IP address of a primary NetBios Name Server (NBNS) that the subscriber must use.                                                                                                                                                                                                                                                                                                                                                                                                |
| 100 | RB-Client-NBNS-Sec         | No                     | Yes                                | Yes                           | IP address. Configures the IP address of a secondary NBNS that the subscriber must use.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 101 | Shaping-Profile-Name       | No                     | Yes                                | Yes                           | String. Name of the ATM shaping profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 102 | Bridge-Profile-Name        | No                     | Yes                                | Yes                           | String. Name of the bridge profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 104 | IP-Interface-Name          | No                     | Yes                                | Yes                           | String. Interface name. Binds a subscriber to the specified interface. This VSA is used in conjunction with VSA 3, DHCP-Max-Leases. <p>This attribute can also be set through the <b>ip interface name</b> command (in subscriber configuration mode); see Chapter 5, "DHCP Configuration."</p>                                                                                                                                                                                                            |
| 105 | NAT-Policy-Name            | No                     | Yes                                | Yes                           | String. NAT policy name. Attaches the specified NAT policy to a subscriber.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 107 | HTTP-Redirect-Profile-Name | No                     | Yes (alive/ and stop records only) | Yes                           | String of up to 32 characters. HTTP redirect profile name.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 111 | Circuit-Protocol-Encap     | No                     | Yes                                | Yes                           | Integer. Circuit encapsulation for CCOD child circuit. The only supported value is 27 for PPPoE encapsulation.                                                                                                                                                                                                                                                                                                                                                                                             |
| 112 | OS-Version                 | Yes                    | Yes                                | No                            | String. Software version number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table A-6 Redback VSAs Supported by the SmartEdge OS (continued)

| #   | VSA Name                  | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|---------------------------|------------------------|----------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 113 | Session-Traffic-Limit     | No                     | Yes                  | Yes                           | String. Specifies that inbound or outbound traffic be limited. Use the <b>in:</b> <limit> and <b>out:</b> <limit> format where limits are independent and in Kbytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 114 | QoS-Reference             | No                     | Yes                  | Yes                           | String. Specifies the node name, the node-name index, the group name, and the group-name index. A : separates the node-name index from the group name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 125 | DHCP-Vendor-Class-Id      | Yes                    | Yes                  | No                            | String. DHCP option 60 value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 127 | DHCP-Vendor-Encap-Option  | No                     | Yes                  | Yes                           | String. DHCP option 43 value. The format is:<br><i>code:value:code:value ....</i><br>where: <ul style="list-style-type: none"> <li>• <i>code</i> = DHCP vendor-encapsulation option number</li> <li>• <i>value</i> = option data in one of the following formats: <ul style="list-style-type: none"> <li>• IP address type = dot notation</li> <li>• Number = decimal integer</li> <li>• ASCII string = ASCII characters without quotation marks</li> <li>• Binary string = Hex values of bytes separated by commas (",")</li> </ul> </li> </ul> See Table 5-6 to Table 5-12 in Chapter 5, "DHCP Configuration," for descriptions of the vendor-encapsulated options found in RFC 2132, <i>DHCP Options and BOOTP Vendor Extensions</i> . |
| 128 | Acct-Input-Octets-64      | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Input-Octets standard attribute per RFC 2139.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 129 | Acct-Output-Octets-64     | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Output-Octets standard attribute per RFC 2139.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 130 | Acct-Input-Packets-64     | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Input-Packets standard attribute per RFC 2139.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 131 | Acct-Output-Packets-64    | No                     | Yes                  | No                            | Integer. 64-bit value for Acct-Output-Packets attribute per RFC 2139.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 132 | Assigned-IP-Address       | No                     | Yes                  | No                            | IP address. Reports IP addresses assigned to a subscriber via IP pools or DHCP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 133 | Acct-Mcast-In-Octets-64   | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Mcast-In-Octets attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 134 | Acct-Mcast-Out-Octets-64  | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Mcast-Out-Octets attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 135 | Acct-Mcast-In-Packets-64  | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Mcast-In-Packets attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 136 | Acct-Mcast-Out-Packets-64 | No                     | Yes                  | No                            | Integer. 64-bit value for the Acct-Mcast-Out-Packets attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 142 | Session-Error-Code        | No                     | Yes                  | No                            | Integer. 32 bits. Stop record only. Communicates specific error code information between Redback devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 143 | Session-Error-Msg         | No                     | Yes                  | No                            | String. Stop record only. Describes how the session terminated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Table A-6 Redback VSAs Supported by the SmartEdge OS** *(continued)*

| #   | VSA Name               | Sent in Access-Request | Sent in Acct-Request | Receivable in Access-Response | Notes                                                                                                                                                                                                                                                                                                       |
|-----|------------------------|------------------------|----------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 145 | Mac-Addr               | Yes                    | Yes                  | No                            | String. MAC address. The format is 17 octets in hex. The MAC address is sent for all subscriber PPPoE sessions. Supported media includes ATM PVCs, 802.1Q PVCs (tagged or untagged VLANs), and Ethernet ports.                                                                                              |
| 146 | Vlan-Id                | No                     | Yes                  | No                            | String. Sent only for PPPoE sessions over an 802.1Q PVC. The format is ab/c:d where: <ul style="list-style-type: none"> <li>• a = "E", "A", or "F" for Ethernet, ATM or Frame Relay, respectively</li> <li>• b = slot number</li> <li>• c = port number</li> <li>• d = VLAN ID of the 802.1Q PVC</li> </ul> |
| 147 | Acct-Mcast-In-Octets   | No                     | Yes                  | No                            | Integer. Number of inbound multicast octets.                                                                                                                                                                                                                                                                |
| 148 | Acct-Mcast-Out-Octets  | No                     | Yes                  | No                            | Integer. Number of outbound multicast octets.                                                                                                                                                                                                                                                               |
| 149 | Acct-Mcast-In-Packets  | No                     | Yes                  | No                            | Integer. Number of inbound multicast packets.                                                                                                                                                                                                                                                               |
| 150 | Acct-Mcast-Out-Packets | No                     | Yes                  | No                            | Integer. Number of outbound multicast packets.                                                                                                                                                                                                                                                              |
| 151 | Reauth-Session-Id      | No                     | No                   | Yes                           | String. Identifies the reauthorize session request. The value in this attribute is a string of attributes and values for the identified subscriber.                                                                                                                                                         |

Table A-7 lists the Redback VSAs that are reauthorized when you enter the **reauthorize** command (in exec mode). For details about these VSAs, see Table A-6.

**Table A-7 Redback VSA Attributes Supported by Reauthorization**

| #   | VSA Name                   | Description                                                                               |
|-----|----------------------------|-------------------------------------------------------------------------------------------|
| 3   | DHCP-Max-Leases            | Specifies the maximum number of DHCP addresses this subscriber can allocate to hosts.     |
| 33  | Mcast-Send                 | Defines whether or not the subscriber can send multicast packets.                         |
| 34  | Mcast-Receive              | Defines whether or not the subscriber can receive multicast packets.                      |
| 35  | Mcast-MaxGroups            | Specifies the maximum number of multicast groups of which the subscriber can be a member. |
| 87  | QoS-Policy-Policing        | Attaches a QoS policing policy to the subscriber session.                                 |
| 88  | QoS-Policy-Metering        | Attaches a QoS metering policy to the subscriber session.                                 |
| 89  | QoS-Policy-Queuing         | Attaches a QoS queuing service profile to the subscriber session.                         |
| 90  | Igmp-Service-Profile       | Applies an IGMP service profile to the subscriber session.                                |
| 92  | Forward-Policy             | Attaches an in or out forward policy to the subscriber session.                           |
| 101 | Shaping-Profile-Name       | Indicates the name of the ATM shaping profile.                                            |
| 102 | Bridge-Profile-Name        | Indicates the name of the bridge profile.                                                 |
| 107 | HTTP-Redirect-Profile-Name | Indicates the name of the HTTP redirect profile.                                          |
| 113 | Session-Traffic-Limit      | Specifies that inbound or outbound traffic be limited.                                    |

# TACACS+ Attribute-Value Pairs

Terminal Access Controller Access Control System Plus (TACACS+) attribute-value (AV) pairs are used to define specific administrator and command-line interface (CLI) command authentication, authorization, and accounting (AAA) elements for user profiles that are stored on a TACACS+ server.

For information about configuring TACACS+ features, see Chapter 17, “TACACS+ Configuration.”

This appendix contains the following sections:

- TACACS+ Authentication and Authorization AV Pairs
- TACACS+ Administrator Accounting AV Pairs
- TACACS+ Command Accounting AV Pairs

## TACACS+ Authentication and Authorization AV Pairs

Table B-1 describes TACACS+ authentication and authorization AV pairs supported by the SmartEdge<sup>®</sup> OS.

**Table B-1 TACACS+ Authentication and Authorization AV Pairs**

| Attribute  | Description                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cmd=x      | Administrator shell command. Indicates the command name for the command to be issued. This attribute can only be specified if service=shell.                                                         |
| cmd-arg=x  | Argument used with an administrator shell command. Indicates the argument name to be used with the command. Multiple cmd-arg attributes can be specified and cmd-arg attributes are order dependent. |
| priv-lvl=x | When received in an administrator authorization response from the server, sets the starting privilege level for the administrator.                                                                   |
| service=x  | Service used by the administrator.                                                                                                                                                                   |

## TACACS+ Administrator Accounting AV Pairs

---

Table B-2 describes the TACACS+ administrator accounting AV pairs supported by the SmartEdge OS.

**Table B-2 TACACS+ Administrator Accounting AV Pairs**

| Attribute     | Description                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| service=shell | Service used by the administrator.                                                                                                 |
| start_time=x  | Time at which the administrator logged onto the SmartEdge OS. The format is in number of seconds since 12:00 a.m. January 1, 1970. |
| stop_time=x   | Time at which the administrator logged off the SmartEdge OS. The format is in number of seconds since 12:00 a.m., January 1, 1970. |
| task_id=x     | Start and stop records for the same event must have matching (unique) task ID numbers.                                             |
| timezone=x    | Time zone abbreviation for all time stamps included in this packet.                                                                |

## TACACS+ Command Accounting AV Pairs

---

Table B-3 describes the TACACS+ command accounting AV pairs supported by the SmartEdge OS.

**Table B-3 TACACS+ Command Accounting AV Pairs**

| Attribute     | Description                                                                            |
|---------------|----------------------------------------------------------------------------------------|
| cmd=x         | Command issued by the administrator. Includes all supported CLI commands.              |
| priv-lvl=x    | Privilege level associated with the command being issued.                              |
| start_time=x  | Time at which the command is issued.                                                   |
| service=shell | Service used by the administrator.                                                     |
| task_id=x     | Start and stop records for the same event must have matching (unique) task ID numbers. |
| timezone=x    | Time zone abbreviation for all timestamps included in this packet.                     |

## A

AAA (authentication, authorization, and accounting)

administrator

accounting, 15-13

authentication, 15-7

assigning preferred IP addresses, 15-8

CLI commands

accounting, 15-12

authorization, 15-11

examples

subscriber authentication, 15-16

subscriber reauthorization, 15-17

L2TP accounting

context-specific, 15-15

global, 15-15

two-stage, 15-15

L2TP peer authorization, 15-11

structured username formats, 15-7

subscriber accounting

context-specific, 15-14

global, 15-13

two-stage, 15-14

subscriber authentication

disabling, 15-10

last-resort context, 15-10

local configuration, 15-9

RADIUS, context-specific, 15-9

RADIUS, context-specific, then global, 15-9

RADIUS, followed by SmartEdge OS, 15-10

RADIUS, global, 15-8

subscriber circuits, assigning IP addresses, 15-8

subscriber circuits, assigning routes, 15-6

subscriber reauthorization, configuring, 15-11

subscriber sessions, limiting number of, 15-6

access control list configuration mode, described, 1-13

Acct-Authentic attribute, A-7

Acct-Delay-Time attribute, A-6

Acct-Input-Gigawords attribute, A-7

Acct-Input-Octets-64 VSA, A-15

Acct-Input-Octets attribute, A-6

Acct-Input-Packets-64 VSA, A-15

Acct-Input-Packets attribute, A-7

Acct-Mcast-In-Octets-64 VSA, A-15

Acct-Mcast-In-Octets VSA, A-16

Acct-Mcast-In-Packets-64 VSA, A-15

Acct-Mcast-In-Packets VSA, A-16

Acct-Mcast-Out-Octets-64 VSA, A-15

Acct-Mcast-Out-Octets VSA, A-16

Acct-Mcast-Out-Packets-64 VSA, A-15

Acct-Mcast-Out-Packets VSA, A-16

Acct-Output-Gigawords attribute, A-7

Acct-Output-Octets-64 VSA, A-15

Acct-Output-Octets attribute, A-6

Acct-Output-Packets-64 VSA, A-15

Acct-Output-Packets attribute, A-7

Acct-Session-Id attribute, A-7

Acct-Session-Time attribute, A-7

Acct-Status-Type attribute, A-6

Acct-Terminate-Cause attribute, A-7

Acct-Tunnel-Connection attribute, A-8

ACL condition configuration mode, described, 1-13

ACLs (access control lists)

enabling ACL counters for subscribers, 8-7

examples

attaching an IP ACL to an interface, 8-11

configuring a forward policy ACL, 8-12

configuring a NAT policy ACL, 8-12

configuring a QoS policy ACL, 8-11

modifying an IP ACL, 8-9

resequencing statements in an IP ACL, 8-9

ACLs (access control lists), IP ACLs

absolute conditions

creating, 8-6

modifying in real time, 8-7

applying to

a context, 8-6

an interface, 8-6

a subscriber, 8-6

---

- conditions, creating, 8-6
- creating or selecting, 8-6
- deny statements, creating, 8-6
- described, 8-1
- description, creating, 8-6
- periodic conditions
  - creating, 8-6
  - modifying in real time, 8-7
- permit statements, creating, 8-6
- resequencing statements, 8-6

ACLs (access control lists), policy ACLs

- absolute conditions
  - creating, 8-7
  - modifying in real time, 8-8
- applying to
  - a forward policy, 9-3
  - a NAT policy with dynamic translations, 10-7
  - a QoS metering policy, 12-9
  - a QoS policing policy, 12-9
- condition ID, creating, 8-7
- creating or selecting, 8-7
- described, 8-3
- description, creating, 8-7
- periodic conditions
  - creating, 8-7
  - modifying in real time, 8-8
- permit statements, creating, 8-7
- resequencing statements, 8-7

Agent-Circuit-Id VSA, A-14

ARP (Address Resolution Protocol)

- disabling, 2-2
- enabling
  - ARP, 2-2
  - proxy ARP, 2-2
  - secured ARP, 2-2
- examples, 2-4
- table entries
  - creating static, 2-3
  - deleting expired, 2-3
  - incomplete, setting a maximum, 2-3
  - modifying the lifespan of, 2-3

Ascend-Data-Filter attribute, A-9

Assigned-IP-Address VSA, A-15

ATM DS-3 configuration mode, described, 1-13

ATM OC configuration mode, described, 1-13

ATM profile configuration mode, described, 1-13

ATM PVC configuration mode, described, 1-13

ATMWFQ policy configuration mode, described, 1-13

attributes

- standard RADIUS, A-4
- vendor-specific Redback, A-10

autonomous address configuration flag, specifying, 3-12

AV (attribute-value) pairs, TACACS+, B-1

## B

- Bind-Auth-Protocol VSA, A-12
- Bind-Type VSA, A-12
- Bridge-Profile-Name attribute, A-14

## C

- Called-Station-Id attribute, A-6
- Calling-Station-Id attribute, A-6
- CHAP-Password attribute, A-4
- characters, in command syntax, xxiii
- Circuit-Protocol-Id VSA, A-14
- Class attribute, A-5
- CLI (command-line interface) syntax, 1-13
- Client-DNS-Pri VSA, A-10
- Client-DNS-Sec VSA, A-10
- CLIPS PVC configuration mode, described, 1-13
- command modes, xxii
- command privilege, xxii
- command syntax
  - conventions, xxii
  - special characters, xxiii
  - terminology, xxii
  - text formats, xxiii
- congestion map configuration mode, described, 1-13
- Connect-Info attribute, A-9
- context configuration mode, described, 1-13
- Context-Name VSA, A-10
- conventions, used in this guide
  - command modes, xxii
  - command privilege, xxii
  - command syntax, xxii

## D

DHCP (Dynamic Host Configuration Protocol)

- described, 5-1
- examples
  - IP source address, 5-19
  - proxy, dynamic, 5-15
  - proxy, static, 5-17
  - RADIUS, 5-18
- external server
  - adding options to packets, 5-5
  - assigning to server group, 5-4
  - configuring subscriber circuits to use, 5-6
  - forwarding all, 5-4
  - hostname, assigning, 5-4
  - IP address for, 5-4
  - maximum hops, 5-4
  - minimum wait, 5-4
  - NAK suppression, 5-5
  - retries, 5-5
  - standby, forwarding to, 5-4



- 
- interfaces
    - external proxy server, 5-5
    - external relay server, 5-5
    - IP address for the giaddr field, 5-5
    - IP source address for external server, 5-5
  - internal server
    - assigning subnet IP addresses, 5-4
    - creating static mapping between subnet and vendor class ID, 5-3
    - creating static mapping for IP address, 5-4
    - creating static mapping with MAC address, 5-4
    - creating subnet, 5-3
    - default lease time, specifying global setting, 5-3
    - default lease time, specifying subnet setting, 5-4
    - enabling context for, 5-3
    - enabling interface for, 5-3
    - maximum lease time, specifying global setting, 5-3
    - offer lease time, specifying global setting, 5-3
    - options, specifying global setting, 5-3
    - specifying boot loader image file, 5-3
    - specifying global settings, 5-3
    - specifying maximum number of IP addresses, 5-4
    - specifying server for boot loader image file, 5-3
    - specifying subnet settings, 5-4
  - DHCP giaddr configuration mode, described, 1-13
  - DHCP-Max-Leases VSA, A-10
  - DHCP relay server configuration mode, described, 1-13
  - DHCP server configuration mode, described, 1-13
  - DHCP subnet configuration mode, described, 1-13
  - DHCP-Vendor-Class-Id VSA, A-15
  - DHCP-Vendor-Encap-Option VSA, A-15
  - DNS (Domain Name System)
    - creating domain names, 6-2
    - described, 6-1
    - enabling, 6-2
    - examples, 6-3
    - host table, creating static entries, 6-3
    - specifying server IP addresses for, 6-2
    - subscribers, 6-2
  - dot1q profile configuration mode, described, 1-13
  - dot1q PVC configuration mode, described, 1-13
  - dropping packets
    - associated with a class, 9-4
    - not associated with a class, 9-3
  - DS-0 group configuration mode, described, 1-13
  - DS-1 configuration mode, described, 1-13
  - DS-3 configuration mode, described, 1-13
  - DSCP (Differentiated Services Code Point)
    - marking incoming packets
      - conforming, 12-8
      - exceeding, 12-8
      - priority assignment, 12-8
      - violating, 12-8
    - marking outgoing packets
      - conforming, 12-7
      - exceeding, 12-7
      - priority assignment, 12-7
      - violating, 12-7
  - propagating
    - IP and L2TP, 14-17
    - IP and MPLS, 14-17
    - IP from Ethernet, 14-12
    - IP to ATM, 14-11
    - IP to Ethernet, 14-12
- E**
- E1 configuration mode, described, 1-13
  - E3 configuration mode, described, 1-13
  - EDRR policy configuration mode, described, 1-13
  - EPD (early packet discard) parameters, ATMWFQ policies, 13-10
  - Event-Timestamp attribute, A-7
  - examples, conventions used in this guide, xxiii
  - exec mode, described, 1-13
- F**
- Filter-Id attribute, A-5
  - forwarding all, 5-4
  - forward policies
    - applying a policy ACL, 9-3
    - classifying packets, 9-3
    - creating or selecting, 9-3
    - destination port, specifying, 9-3
  - dropping packets
    - associated with a class, 9-4
    - not associated with a class, 9-3
  - examples
    - combination of mirror, redirect, and drop, 9-11
    - dropping packets, 9-9
    - mirroring packets, 9-4
    - redirecting packets, 9-7
  - mirroring packets
    - associated with a class, 9-4
    - not associated with a class, 9-3
  - redirecting packets
    - associated with a class, 9-4
    - not associated with a class, 9-3
  - forward policy configuration mode, described, 1-13
  - Forward-Policy VSA, A-13
  - Framed-IP-Address attribute, A-5
  - Framed-IP-Netmask attribute, A-5
  - Framed-MTU attribute, A-5
  - Framed-Protocol attribute, A-5
  - Framed-Route attribute, A-5
  - Frame Relay PVC configuration mode, described, 1-13

---

## G

global configuration mode, described, 1-13

GRE tunnel configuration mode, described, 1-13

## H

hierarchical node configuration mode, described, 1-13

hierarchical node group configuration mode,  
described, 1-13

HTTP redirect

attaching

a forward policy to a subscriber circuit, 7-4

the redirect profile to a subscriber, 7-3

configuring

forward policy, 7-4

IP ACL for subscriber access, 7-2

policy ACL, 7-4

redirect profile, 7-3

subscriber access, 7-2

subscriber authentication, 7-2

subscriber reauthorization, 7-2

URL, 7-3

described, 7-1

examples, 7-5

server

enabling, 7-2

port number, modifying, 7-2

HTTP redirect profile mode, described, 1-13

HTTP-Redirect-Profile-Name VSA, A-14

HTTP redirect server configuration mode, described, 1-14

## I

Idle-Timeout attribute, A-6

Igmp-Service-Profile VSA, A-13

interface configuration mode, described, 1-14

Ip-Address-Pool-Name VSA, A-12

IP-Interface attribute, A-14

## K

key chain configuration mode, described, 1-14

key chains

creating a description, 18-2

enabling for use with

IS-IS, 18-3

OSPF, 18-3

VRRP, 18-3

examples, 18-3

specifying

key ID, 18-2

key string, 18-2

send lifetime, 18-2

## L

L2TP (Layer 2 Tunneling Protocol)

accounting

context-specific, 15-15

global, 15-15

two-stage, 15-15

propagating QoS, 14-17

l2tp peer configuration mode, described, 1-14

LI (lawful intercept)

configuring circuits for

contexts, 19-2

interfaces, 19-2

subscribers, 19-2

described, 19-1

examples, 19-3

profiles

creating, 19-2

defining header fields, 19-2

defining transport data section, 19-2

enabling pending intercept requests, 19-2

specifying intercept type, 19-2

starting a circuit intercept, 19-3

starting a subscriber intercept, 19-3

stopping a circuit intercept, 19-3

stopping a subscriber intercept, 19-3

link group configuration mode, described, 1-14

LI profile configuration mode, described, 1-14

## M

Mac-Addr VSA, A-16

maximum hops, external DHCP server, 5-4

maximum lease time, specifying subnet setting, 5-4

Mcast-MaxGroups VSA, A-12

Mcast-Receive VSA, A-12

Mcast-Send VSA, A-11

Medium-Type VSA, A-12

metering policy configuration mode, described, 1-14

minimum wait, external DHCP server, 5-4

mirroring packets

associated with a class, 9-4

not associated with a class, 9-3

MPLS (Multiprotocol Label Switching)

propagating QoS, 14-17

using only DSCP for queuing, 14-18

MPLS router configuration mode, described, 1-14

## N

NAK suppression, external DHCP server, 5-5

NAS-Identifier attribute, A-6

NAS-IP-Address attribute, A-4

NAS-Port attribute, A-4

NAS-Port-Id attribute, A-9

NAS-Port-Type attribute, A-8

---

## NAT (Network Address Translation) policies

- described, 10-1

- dynamic translations

- applying a policy ACL, 10-7
  - attaching a policy, 10-6
  - configuration tasks, 10-6
  - creating or selecting a policy, 10-6
  - creating or selecting a pool, 10-6
  - dropping a class of packets, 10-7
  - dropping or ignoring packets, 10-6
  - ignoring a class of packets, 10-7
  - specifying a class, 10-7
  - specifying a pool, 10-6
  - specifying IP addresses for a pool, 10-6
  - specifying the class timeout, 10-7
  - specifying the pool for a class of packets, 10-7
  - specifying timeout, 10-6

- examples

- combination of all translation types, 10-10
  - dynamic translations, 10-9
  - NAPT with dynamic translations, 10-9
  - NAPT with static translations, 10-8
  - static translations, 10-7

- order of application to packets, 10-4

- static translations, configuring, 10-5

- using policy ACLs with, described, 10-3

- NAT policy configuration mode, described, 1-14

- NAT-Policy-Name attribute, A-14

- NAT pool configuration mode, described, 1-14

- ND (Neighbor Discovery) protocol

- examples, 3-4

- ND router

- configuring global settings for, 3-3
  - creating, 3-3
  - creating interface for, 3-2
  - creating or selecting context for, 3-2
  - specifying IPv6 interface address for, 3-2

- ND router interface

- configuring interface settings for, 3-3
  - configuring prefixes for, 3-3
  - selecting context for, 3-3
  - selecting interface for, 3-3
  - selecting ND router for, 3-3
  - specifying static neighbors for, 3-3

- Preferred Lifetime, 3-10

- prefixes, configuring, 3-12

- RA messages

- configuration flags, 3-14
  - Reachable Time, 3-16
  - Router Lifetime, 3-14

- Retrans Timer, 3-8

- Valid Lifetime, 3-19

- ND router configuration mode, described, 1-14

- ND router interface configuration mode, described, 1-14

## NTP (Network Time Protocol)

- accessing NTP configuration mode, 4-2

- configuring

- peer synchronization, 4-2
  - server synchronization, 4-2

- enabling slowsync, 4-2

- examples, 4-3

- NTP configuration mode, described, 1-14

- num-queues configuration mode, described, 1-14

## O

- offer lease time, specifying subnet setting, 5-4

- on-link flag, specifying, 3-12

- options, specifying subnet setting, 5-4

- organization, of this guide, xxi

- OS-Version VSA, A-14

## P

- Platform-Type VSA, A-14

- policing policy configuration mode, described, 1-14

- policy ACL class configuration mode, described, 1-14

- policy ACL configuration mode, described, 1-14

- policy class rate configuration mode, described, 1-14

- policy rate configuration mode, described, 1-14

- port configuration mode, described, 1-14

- Port-Limit attribute, A-8

- PPPoE-IP-Route-Add VSA, A-13

- PPPOE-MOTM VSA, A-11

- PPPOE-URL VSA, A-11

- PQ policy configuration mode, described, 1-14

- Preferred Lifetime, specifying, 3-10

- Prefix Information option, configuring

- autonomous address configuration flag, 3-12

- on-link flag, prefix specific, 3-12

- Preferred Lifetime, 3-13

- Valid Lifetime

- interfaces, 3-13

- ND router, 3-19

- priority groups

- customizing queue maps for, 13-8

- described, 12-2

- propagating QoS

- IP from Ethernet, 14-12

- IP from MPLS, 14-17

- IP to ATM, 14-11

- IP to Ethernet, 14-12

- IP to MPLS, 14-17

- L2TP

- inbound packets, downstream direction, 14-17

- inbound packets, to an LAC, 14-17

- inbound packets, to an LNS, 14-17

- inbound packets, upstream direction, 14-17

---

- outbound packets, from an LNS, 14-17
- outbound packets, upstream direction, 14-17
- propagating QoS, described
  - IP and Ethernet, 14-6
  - IP and L2TP, 14-8
  - IP and MPLS, 14-7
  - IP to ATM, 14-6
  - types of settings, 14-5
- proxy ARP, enabling, 2-2
- PVC-Encapsulation-Type VSA, A-12
- PVC-Profile-Name VSA, A-12

## Q

### QoS (quality of service)

- classifying packets using ACLs, described, 12-2
- classifying traffic with priority groups
  - Ethernet circuits, 14-12
  - PDH circuits, 14-15
  - POS circuits, 14-15
- congestion avoidance, described, 13-5
- congestion avoidance maps
  - creating or selecting, 13-9
  - setting exponential weight for, 13-9
  - setting RED parameters for, 13-9
- congestion management, described, 13-5
- DSCP bits, marking incoming packets
  - conforming, 12-8
  - exceeding, 12-8
  - priority, 12-8
  - violating, 12-8
- DSCP bits, marking outgoing packets
  - conforming, 12-7
  - exceeding, 12-7
  - priority, 12-7
  - violating, 12-7
- EDRR algorithm mode, defining for
  - Ethernet circuits, 14-12
  - first-generation ATM PVCs, 14-11
  - PDH circuits, 14-15
  - POS circuits, 14-15
  - subscriber circuits, 14-16
- marking, described, 12-3
- order of application to inbound packets, 12-6
- policy ACLs, described, 12-2
- priority groups
  - customizing queue maps for, 13-8
  - described, 12-2
- propagating
  - described, 14-5
  - IP from Ethernet, 14-12
  - IP to ATM, 14-11
  - IP to Ethernet, 14-12
- queue depth, described, 13-7

- queue maps
  - creating, 13-8
  - described, 13-2
  - mapping priority groups to queues, 13-8
  - specifying the number of queues for, 13-8
- queue rates, described, 13-7
- rate-limiting, described, 12-3
- setting the rate for outgoing traffic, 14-12
- QoS (quality of service), examples
  - ATMWFQ policy, 13-13
  - congestion avoidance map, 13-13
  - EDRR policy
    - attaching, 14-20
    - configuring, 13-13
  - hierarchical scheduling, 14-20
  - hierarchical shaping, 14-20
  - metering policies, attaching
    - cross-connected circuits, 14-18
    - PVCs, 14-18
    - subscribers, 14-19
  - policing policies
    - circuit-based marking, 12-10
    - circuit-based rate-limiting, 12-10
    - class and rate-limiting, 12-10
    - rate-limiting and marking, 12-12
  - PQ policies
    - attaching, 14-19
    - backbone application, 13-15
    - rate-limiting, 13-14
  - PWFQ policies
    - attaching to node, 14-20
    - attaching to port and PVC, 14-20
    - configuring, 13-17
    - ports, 14-20
  - QoS propagation, 14-21
  - queue maps, 13-12
  - RED parameters, 13-14
- QoS (quality of service), hierarchical scheduling, configuring
  - ports
    - attaching PWFQ policy, 14-13
    - scheduling algorithm for, 14-13
    - setting rates for, 14-13
  - tunnels and PVCs
    - attaching PWFQ policy, 14-13
    - scheduling algorithm, 14-13
    - setting rates for, 14-13
- QoS (quality of service), hierarchical shaping, configuring
  - node groups
    - creating, 14-13
    - for subscriber circuits, 14-13
    - scheduling algorithm for, 14-14
    - setting rates for, 14-14

- 
- nodes
    - attaching PWFQ policy, 14-14
    - creating, 14-14
    - for subscriber circuits, 14-13
    - scheduling algorithm for, 14-14
    - setting rates for, 14-14
  - ports
    - scheduling algorithm for, 14-13
    - setting rates for, 14-13
  - subscriber circuits, creating reference to node, 14-16
  - QoS (quality of service), policies
    - ATMWFQ policies
      - assigning a congestion avoidance map to, 13-9
      - assigning a queue map to, 13-9
      - attaching to second-generation ATM PVCs, 14-11
      - creating the name of, 13-9
      - defining the algorithm mode for, 13-9
      - described, 13-4
      - setting EPD parameters for, 13-10
      - specifying the number of queues for, 13-9
      - specifying the traffic weight for, 13-9
    - congestion avoidance maps, specifying the queue depth for, 13-9
    - EDRR policies
      - assigning a queue priority map to, 13-10
      - creating the name of, 13-10
      - described, 13-3
      - modifying the traffic weight for, 13-10
      - setting a rate limit for, 13-10
      - specifying RED parameters for, 13-10
      - specifying the depth of each queue, 13-10
      - specifying the number of queues for, 13-10
    - metering policies
      - applying a policy ACL, 12-9
      - creating or selecting, 12-7
      - described, 12-2
      - marking outgoing packets, 12-7
      - rate-limiting outgoing packets, 12-7
    - metering policies, attaching to
      - cross-connected circuits, 14-16
      - Ethernet circuits, 14-12
      - first-generation ATM PVCs, 14-11
      - PDH circuits, 14-15
      - POS circuits, 14-15
      - second-generation ATM PVCs, 14-11
      - subscriber circuits, 14-16
    - policing policies
      - applying a policy ACL, 12-9
      - creating or selecting, 12-8
      - described, 12-2
      - marking incoming packets, 12-8
      - rate-limiting incoming packets, 12-8
    - policing policies, attaching to
      - cross-connected circuits, 14-16
      - Ethernet circuits, 14-12
      - first-generation ATM PVCs, 14-11
      - PDH circuits, 14-15
      - POS circuits, 14-15
      - second-generation ATM PVCs, 14-11
      - subscriber circuits, 14-16
    - PQ policies
      - assigning a queue map to, 13-11
      - creating the name of, 13-11
      - described, 13-3
      - setting a rate limit per queue, 13-11
      - specifying RED parameters for, 13-11
      - specifying the number of queues for, 13-11
      - specifying the queue depth for, 13-11
    - PWFQ policies
      - assigning a congestion avoidance map to, 13-11
      - assigning a queue map to, 13-11
      - creating the name of, 13-11
      - defining the algorithm mode for, 13-11
      - described, 13-4
      - setting rate and burst for priority groups, 13-11
      - setting rate limits, 13-11
      - setting relative weight, 13-11
      - specifying the number of queues for, 13-11
    - scheduling policies, attaching to
      - Ethernet circuits, 14-12
      - first-generation ATM PVCs, 14-11
      - PDH circuits, 14-15
      - POS circuits, 14-15
      - subscriber circuits, 14-16
    - scheduling policies, circuits supported, 14-3
    - scheduling policies, described
      - ATMWFQ, 13-4
      - EDRR, 13-3
      - PQ, 13-3
      - PWFQ, 13-4
    - Qos-Policy-Metering VSA, A-13
    - Qos-Policy-Policing VSA, A-13
    - Qos-Policy-Queuing VSA, A-13
    - QoS-Reference VSA, A-15
    - queue map configuration mode, described, 1-14

## R

    - RA (Router Advertisement) messages
      - Managed address configuration flag, 3-14
      - Other stateful configuration flag, 3-14
      - Reachable Time, 3-16
      - Router Lifetime, 3-14

---

---

## RADIUS (Remote Authentication Dial-In User Service)

- accounting servers
  - accounting messages, sending, 16-3
  - configuring hostname or IP address, 16-2
  - configuring load balancing, 16-3
  - described, 16-1
  - modifying number of requests, 16-5
  - modifying number of retransmissions, 16-4
  - timeout, deadtime, 16-4
  - timeout, lost packet, 16-4
  - timeout, server dead, 16-4
  - timeout, server unreachable, 16-4
- account termination error code, remapping, 16-7
- attributes, Filter-Id, 16-6
- attributes, Redback prefix for VSAs, A-5
- attributes, sending in request packets
  - Acct-Delay-Time, 16-6
  - Acct-Session-Id, 16-6
  - Calling-Station-Id, 16-6
  - NAS-IP-Address attribute, 16-6
  - NAS-Port, 16-6
  - NAS-Port-ID, 16-6
  - NAS-Port-Type, 16-6
- attributes, specifying separator character, 16-6
- attributes, standard, A-4
- attributes, VSA, A-10
- authentication servers
  - configuring hostname or IP address, 16-2
  - configuring load balancing, 16-3
  - described, 16-1
- described, 16-1
- examples, 16-7
- increasing number of server ports, 16-5
- policies
  - assigning to a context, 16-5
  - creating or modifying, 16-5
  - specifying attributes to be dropped, 16-5
- servers
  - modifying number of requests, 16-5
  - modifying number of retransmissions, 16-4
  - timeout, dead time, 16-4
  - timeout, lost packet, 16-4
  - timeout, server dead, 16-4
  - timeout, server unreachable, 16-4
- source address, configuring, 16-3
- stripping domain from username, 16-5

RADIUS policy configuration mode, described, 1-14

RB-Client-NBNS-Pri VSA, A-14

RB-Client-NBNS-Sec VSA, A-14

Reauth-More attribute, A-13

Reauth-Session-Id VSA, A-16

Reauth-String attribute, A-13

## RED (random early detection) parameters

- ATMWFQ policies, 13-9
- EDRR policies, 13-10
- PQ policies, 13-11
- PWFQ policies, 13-11

redirecting packets

- associated with a class, 9-4
- not associated with a class, 9-3

Remote-Agent-Id VSA, A-14

Remote-Port-String attribute, A-13

Reply-Message attribute, A-5

Retrans Timer, 3-8

retries, external DHCP server, 5-5

## S

secured ARP, enabling, 2-2

server group, assigning external DHCP server to, 5-4

service policies

- attaching to subscriber sessions, 11-2
- configuring
  - allowable contexts or domains, 11-2
  - policy name, 11-2
- described, 11-1
- examples, 11-3

service policy configuration mode, described, 1-14

Service-Type attribute, A-5

Session-Error-Code VSA, A-15

Session-Error-Msg VSA, A-15

Session-Timeout attribute, A-6

Session-Traffic-Limit VSA, A-15

Shaping-Profile-Name attribute, A-14

Source-Validation VSA, A-10

special characters, in command syntax, xxii

standby server, forwarding to, 5-4

Sub-Profile-Name VSA, A-13

subscriber configuration mode, described, 1-14

## T

TACACS+ (Terminal Access Controller Access Control System Plus)

- AV pairs, B-1
- configuring IP address or hostname, 17-2
- described, 17-1
- examples, 17-3
- modifying deadtime interval, 17-2
- modifying number of maximum retries, 17-3
- modifying timeout, 17-2
- source address, configuring, 17-3
- stripping the domain portion of a username, 17-3

terminate error cause configuration mode, described, 1-14

text formats, in command syntax, xxiii

traffic cards, listed, 14-3

---

Tunnel-Algorithm VSA, A-11  
Tunnel-Assignment-Id attribute, A-9  
Tunnel-Client-Auth-Id attribute, A-9  
Tunnel-Client-Endpoint attribute, A-8  
Tunnel-Cmd-Timeout VSA, A-11  
Tunnel-Deadtime VSA, A-11  
Tunnel-Domain VSA, A-10  
Tunnel-Function VSA, A-11  
Tunnel-Local-Name VSA, A-10  
tunnel map configuration mode, described, 1-14  
Tunnel-Max-Sessions VSA, A-11  
Tunnel-Max-Tunnels VSA, A-11  
Tunnel-Medium-Type attribute, A-8  
Tunnel-Password attribute, A-8  
Tunnel-Preference attribute, A-9  
Tunnel-Remote-Name VSA, A-10  
Tunnel-Retransmit VSA, A-11  
Tunnel-Server-Auth-Id, A-9  
Tunnel-Server-Endpoint attribute, A-8  
Tunnel-Session-Auth-Ctx VSA, A-12  
Tunnel-Session-Auth VSA, A-11  
Tunnel-Type attribute, A-8  
Tunnel-Window VSA, A-11

## U

URL, HTTP redirect, 7-3  
User-Name attribute, A-4  
User-Password attribute, A-4

## V

Vendor-Specific attribute, A-5  
VSAs (vendor-specific attributes), Redback  
    listed, A-10  
    prefix for, A-5





# Commands

---

## A

- aaa accounting administrator, 15-18
- aaa accounting commands, 15-19
- aaa accounting event, 15-21
- aaa accounting l2tp, 15-23
- aaa accounting reauthorization subscriber, 15-25
- aaa accounting subscriber, 15-27
- aaa accounting suppress-acct-on-fail, 15-29
- aaa authentication administrator, 15-31
- aaa authentication subscriber, 15-34
- aaa authorization commands, 15-37
- aaa authorization tunnel, 15-39
- aaa global accounting event, 15-40
- aaa global accounting l2tp-session, 15-41
- aaa global accounting reauthorization subscriber, 15-42
- aaa global accounting subscriber, 15-44
- aaa global authentication subscriber, 15-45
- aaa global maximum subscriber, 15-46
- aaa global update subscriber, 15-48
- aaa hint ip-address, 15-50
- aaa last-resort, 15-52
- aaa maximum subscriber, 15-54
- aaa provision binding-order, 15-56
- aaa provision route, 15-58
- aaa reauthorization bulk, 15-59
- aaa update subscriber, 15-61
- aaa username-format, 15-63
- absolute, 8-14
- accept-lifetime, 18-4
- access-group, 8-16
- access-list, 8-18
- address, 10-11
- admin-access-group, 8-19
- allow, 11-5
- attribute, 16-9

## B

- bootp-filename, 5-21
- boot-siaddr, 5-22

## C

- class, 8-21
- clpbit propagate qos to atm, 14-22
- condition, 8-23
- conform mark dscp, 12-13
- conform mark precedence, 12-16
- conform mark priority, 12-18
- conform no-action, 12-20
- congestion-map, 13-19

## D

- default-lease-time, 5-23
- deny, 8-25
- description, 8-34
- dhcp max-addr, 5-24
- dhcp proxy, 5-26
- dhcp relay, 5-28
- dhcp relay option, 5-30
- dhcp relay server, 5-32
- dhcp relay server retries, 5-34
- dhcp relay suppress-nak, 5-35
- dhcp server, 5-36
- dhcp server policy, 5-38
- dns, 6-4
- drop
  - forward policies, 9-14
  - NAT policies, 10-13

## E

- egress prefer dscp-qos, 14-24
- exceed drop, 12-21
- exceed mark dscp, 12-23
- exceed mark precedence, 12-25
- exceed mark priority, 12-27
- exceed no-action, 12-29

---

## F

- forward-all, 5-39
- forward output, 9-16
- forward policy, 9-18
- forward policy in, 9-19
- forward policy out, 9-21

## H

- header, 19-5
- http-redirect profile, 7-7
- http-redirect server, 7-9

## I

- ignore, 10-14
- interface, 3-5
- ip access-group, 8-35
- ip access-list, 8-37
- ip arp, 2-5
- ip arp arpa, 2-6
- ip arp delete-expired, 2-7
- ip arp maximum incomplete-entries, 2-8
- ip arp proxy-arp, 2-9
- ip arp secured-arp, 2-11
- ip arp timeout, 2-13
- ip dmz, 10-15
- ip domain-lookup, 6-5
- ip domain-name, 6-6
- ip host, 6-7
- ip interface, 5-40
- ip name-servers, 6-8
- ip nat, 10-16
- ip nat pool, 10-17
- ip static in, 10-18
- ip static out, 10-20
- ip subscriber arp, 2-15
- ipv6 host, 6-9
- ipv6 name-servers, 6-10

## K

- key-chain description, 18-6
- key-chain key-id, 18-7
- key-string, 18-9

## L

- li-profile, 19-6

## M

- mac-address, 5-42
- mark dscp, 12-31
- mark precedence, 12-33
- mark priority, 12-35
- max-hops, 5-43

- max-lease-time, 5-44
- min-wait, 5-45
- mirror destination, 9-23
- modify ip access-list, 8-39
- modify policy access-list, 8-41

## N

- nat policy, 10-22
- nat policy-name, 10-23
- neighbor, 3-7
- ns-interval, 3-8
- ntp mode, 4-4
- ntp peer, 4-5
- ntp server, 4-7
- num-queues, 13-20

## O

- offer-lease-time, 5-46
- option, 5-47
- option-82, 5-53
- out, 16-49

## P

- pending, 19-7
- periodic, 8-43
- permit, 8-45
- policy access-list, 8-54
- pool, 10-24
- port, 7-10
- preferred-lifetime, 3-10
- prefix, 3-12
- propagate qos from ethernet, 14-25
- propagate qos from l2tp, 14-26
- propagate qos from-mpls, 14-27
- propagate qos from subscriber, 14-28
- propagate qos to ethernet, 14-30
- propagate qos to l2tp, 14-31
- propagate qos to-mpls, 14-33

## Q

- qos congestion-avoidance-map, 13-22
- qos hierarchical mode, 14-34
- qos mode, 14-36
- qos node, 14-38
- qos node-group, 14-40
- qos node-reference, 14-41
- qos policy atmwfq, 13-24
- qos policy edrr, 13-26
- qos policy metering
  - attaching, 14-42
  - creating or selecting, 12-37

---

- qos policy policing
  - attaching, 14-44
  - creating or selecting, 12-38
- qos policy pq, 13-28
- qos policy pwfq, 13-30
- qos policy queuing, 14-46
- qos priority, 14-49
- qos queue-map, 13-31
- qos rate, 14-51
- qos weight, 14-53
- queue 0 mode, 13-40
- queue congestion epd, 13-33
- queue depth, 13-35
- queue exponential-weight, 13-37
- queue-map, 13-39
- queue priority, 13-41
- queue priority-group, 13-44
- queue rate, 13-46
- queue red, 13-47
- queue weight, 13-52

## R

- ra, 3-14
- radius accounting algorithm, 16-11
- radius accounting deadtime, 16-12
- radius accounting max-outstanding, 16-13
- radius accounting max-retries, 16-14
- radius accounting send-acct-on-off, 16-15
- radius accounting server, 16-17
- radius accounting server-timeout, 16-19
- radius accounting timeout, 16-20
- radius algorithm, 16-21
- radius attribute acct-delay-time, 16-22
- radius attribute acct-session-id, 16-23
- radius attribute acct-terminate-remap, 16-24
- radius attribute calling-station-id, 16-25
- radius attribute filter-id, 16-28
- radius attribute nas-ip-address, 16-30
- radius attribute nas-port, 16-31
- radius attribute nas-port-id, 16-33
- radius attribute nas-port-type, 16-36
- radius attribute vendor-specific, 16-38
- radius deadtime, 16-39
- radius max-outstanding, 16-40
- radius max-retries, 16-41
- radius policy, 16-42
- radius server, 16-44
- radius server-timeout, 16-46
- radius source-port, 16-47
- radius strip-domain, 16-48
- radius timeout, 16-49
- range, 5-55
- rate

- EDRR and PWFQ policies, 13-54
- metering and policing policies, 12-40
- policy ACLs, 12-40
- rate percentage, 12-42
- rbak-term-ec, 16-50
- reachable-time, 3-16
- redirect destination circuit, 9-25
- redirect destination local, 7-11
- redirect destination next-hop, 9-26
- resequence ip access-list, 8-56
- resequence policy access-list, 8-57
- router nd, 3-18

## S

- send-lifetime, 18-10
- server-group, 5-56
- service-policy, 11-6
- slowsync, 4-9
- standby, 5-57
- subnet, 5-58

## T

- tacacs+ deadtime, 17-4
- tacacs+ max-retries, 17-6
- tacacs+ server, 17-8
- tacacs+ strip-domain, 17-10
- tacacs+ timeout, 17-11
- timeout, 10-25
- transport udp, 19-8
- type, 19-10

## U

- url, 7-12
- user-class-id, 5-60

## V

- valid-lifetime, 3-19
- vendor-class, 5-62
- vendor-class-id, 5-64
- violate drop, 12-44
- violate mark dscp, 12-46
- violate mark precedence, 12-49
- violate mark priority, 12-51
- violate no-action, 12-53

## W

- weight, 13-56



## A

access control list configuration mode

condition, 8-23

deny, 8-25

description, 8-34

permit, 8-45

ACL condition configuration mode

absolute, 8-14

periodic, 8-43

ATM DS-3 configuration mode

forward policy in, 9-19

forward policy out, 9-21

qos policy metering, 14-42

qos policy policing, 14-44

qos policy queuing, 14-46

qos priority, 14-49

ATM OC configuration mode

forward policy in, 9-19

forward policy out, 9-21

qos mode, 14-36

qos policy metering, 14-42

qos policy policing, 14-44

qos policy queuing, 14-46

qos priority, 14-49

ATM profile configuration mode

clpbit propagate qos to atm, 14-22

radius attribute nas-port-type, 16-36

ATM PVC configuration mode

forward policy in, 9-19

forward policy out, 9-21

qos policy metering, 14-42

qos policy policing, 14-44

qos policy queuing, 14-46

qos priority, 14-49

ATMWfq policy configuration mode

num-queues, 13-20

queue 0 mode, 13-40

queue congestion epd, 13-33

queue-map, 13-39

queue weight, 13-52

## C

congestion map configuration mode

queue depth, 13-35

queue exponential-weight, 13-37

queue red, 13-47

context configuration mode

aaa accounting administrator, 15-18

aaa accounting commands, 15-19

aaa accounting event, 15-21

aaa accounting l2tp, 15-23

aaa accounting reauthorization subscriber, 15-25

aaa accounting subscriber, 15-27

aaa accounting suppress-acct-on-fail, 15-29

aaa authentication administrator, 15-31

aaa authentication subscriber, 15-34

aaa authorization commands, 15-37

aaa authorization tunnel, 15-39

aaa hint ip-address, 15-50

aaa maximum subscriber, 15-54

aaa provision binding-order, 15-56

aaa provision route, 15-58

aaa reauthorization bulk, 15-59

aaa update subscriber, 15-61

admin-access-group, 8-19

dhcp relay option, 5-30

dhcp relay server, 5-32

dhcp relay server retries, 5-34

dhcp relay suppress-nak, 5-35

dhcp server policy, 5-38

http-redirect profile, 7-7

ip access-list, 8-37

ip arp, 2-5

ip arp maximum incomplete-entries, 2-8

ip domain-lookup, 6-5

ip domain-name, 6-6

ip host, 6-7

---

- ip name-servers, 6-8
- ip nat pool, 10-17
- ipv6 host, 6-9
- ipv6 name-servers, 6-10
- key-chain description, 18-6
- key-chain key-id, 18-7
- nat policy, 10-22
- policy access-list, 8-54
- radius accounting algorithm, 16-11
- radius accounting deadtime, 16-12
- radius accounting max-outstanding, 16-13
- radius accounting max-retries, 16-14
- radius accounting send-acct-on-off, 16-15
- radius accounting server, 16-17
- radius accounting server-timeout, 16-19
- radius accounting timeout, 16-20
- radius algorithm, 16-21
- radius attribute acct-delay-time, 16-22
- radius attribute acct-session-id, 16-23
- radius attribute calling-station-id, 16-25
- radius attribute filter-id, 16-28
- radius attribute nas-ip-address, 16-30
- radius attribute nas-port, 16-31
- radius attribute nas-port-id, 16-33
- radius attribute nas-port-type, 16-36
- radius attribute vendor-specific, 16-38
- radius deadtime, 16-39
- radius max-outstanding, 16-40
- radius max-retries, 16-41
- radius policy, 16-42
- radius server, 16-44
- radius server-timeout, 16-46
- radius strip-domain, 16-48
- radius timeout, 16-49
- resequence ip access-list, 8-56
- resequence policy access-list, 8-57
- router nd, 3-18
- subnet, 5-58
- tacacs+ deadtime, 17-4
- tacacs+ max-retries, 17-6
- tacacs+ server, 17-8
- tacacs+ strip-domain, 17-10
- tacacs+ timeout, 17-11

## D

- DHCP giaddr configuration mode
  - user-class-id, 5-60
  - vendor-class-id, 5-64
- DHCP relay server configuration mode
  - forward-all, 5-39
  - max-hops, 5-43
  - min-wait, 5-45

- server-group, 5-56
- standby, 5-57
- DHCP server configuration mode
  - bootp-filename, 5-21
  - boot-siaddr, 5-22
  - default-lease-time, 5-23
  - max-lease-time, 5-44
  - offer-lease-time, 5-46
  - option, 5-47
  - vendor-class, 5-62
- DHCP subnet configuration mode
  - mac-address, 5-42
  - max-lease-time, 5-44
  - offer-lease-time, 5-46
  - option, 5-47
  - option-82, 5-53
  - range, 5-55
- dot1q profile configuration mode
  - propagate qos from ethernet, 14-25
  - propagate qos to ethernet, 14-30
  - radius attribute nas-port-type, 16-36
- dot1q PVC configuration mode
  - forward policy in, 9-19
  - forward policy out, 9-21
  - qos policy metering, 14-42
  - qos policy policing, 14-44
  - qos policy queuing, 14-46
  - qos priority, 14-49
  - qos rate, 14-51
  - qos weight, 14-53
- DS-0 group configuration mode
  - forward policy in, 9-19
  - forward policy out, 9-21
  - qos mode, 14-36
  - qos policy metering, 14-42
  - qos policy policing, 14-44
  - qos policy queuing, 14-46
  - qos priority, 14-49
- DS-1 configuration mode
  - forward policy in, 9-19
  - forward policy out, 9-21
  - qos mode, 14-36
  - qos policy metering, 14-42
  - qos policy policing, 14-44
  - qos policy queuing, 14-46
  - qos priority, 14-49
- DS-3 configuration mode
  - forward policy in, 9-19
  - forward policy out, 9-21
  - qos mode, 14-36
  - qos policy metering, 14-42
  - qos policy policing, 14-44
  - qos policy queuing, 14-46
  - qos priority, 14-49

---

## E

### E1 configuration mode

- forward policy in, 9-19
- forward policy out, 9-21
- qos mode, 14-36
- qos policy metering, 14-42
- qos policy policing, 14-44
- qos policy queuing, 14-46
- qos priority, 14-49

### E3 configuration mode

- forward policy in, 9-19
- forward policy out, 9-21
- qos mode, 14-36
- qos policy metering, 14-42
- qos policy policing, 14-44
- qos policy queuing, 14-46
- qos priority, 14-49

### EDRR policy configuration mode

- num-queues, 13-20
- queue depth, 13-35
- queue-map, 13-39
- queue red, 13-47
- queue weight, 13-52
- rate, 13-54

### exec mode

- modify ip access-list, 8-39
- modify policy access-list, 8-41

## F

### forward policy configuration mode

- access-group, 8-16
- drop, 9-14
- mirror destination, 9-23
- redirect destination circuit, 9-25
- redirect destination local, 7-11
- redirect destination next-hop, 9-26

### Frame Relay PVC configuration mode

- forward output, 9-16
- forward policy in, 9-19
- forward policy out, 9-21
- qos policy metering, 14-42
- qos policy policing, 14-44
- qos policy queuing, 14-46
- qos priority, 14-49

## G

### global configuration mode

- aaa global accounting event, 15-40
- aaa global accounting l2tp-session, 15-41
- aaa global accounting reauthorization subscriber, 15-42
- aaa global accounting subscriber, 15-44
- aaa global authentication subscriber, 15-45
- aaa global maximum subscriber, 15-46

- aaa global update subscriber, 15-48
  - aaa last-resort, 15-52
  - aaa username-format, 15-63
  - forward policy, 9-18
  - http-redirect server, 7-9
  - li-profile, 19-6
  - ntp mode, 4-4
  - ntp peer, 4-5
  - ntp server, 4-7
  - qos congestion-avoidance-map, 13-22
  - qos policy atmwfq, 13-24
  - qos policy edrr, 13-26
  - qos policy metering, 12-37
  - qos policy policing, 12-38
  - qos policy pq, 13-28
  - qos policy pwfq, 13-30
  - qos queue-map, 13-31
  - radius attribute acct-terminate-cause remap, 16-24
  - radius policy, 16-42
  - radius source-port, 16-47
  - service-policy, 11-6
- ### GRE tunnel configuration mode
- forward output, 9-16

## H

### hierarchical node configuration mode

- qos hierarchical mode, 14-34
- qos policy queuing, 14-46
- qos rate, 14-51
- qos weight, 14-53

### hierarchical node group configuration mode

- qos hierarchical mode, 14-34
- qos node, 14-38
- qos rate, 14-51
- qos weight, 14-53

### HTTP redirect profile configuration mode

- url, 7-12

### HTTP redirect server configuration mode

- port, 7-10

## I

### interface configuration mode

- dhcp proxy, 5-26
- dhcp relay, 5-28
- dhcp server, 5-36
- ip access-group, 8-35
- ip arp arpa, 2-6
- ip arp delete-expired, 2-7
- ip arp proxy-arp, 2-9
- ip arp secured-arp, 2-11
- ip arp timeout, 2-13
- ip nat, 10-16

---

## K

key chain configuration mode  
  accept-lifetime, 18-4  
  key-string, 18-9  
  send-lifetime, 18-10

## L

L2TP peer configuration mode  
  propagate qos from l2tp, 14-26  
  propagate qos from subscriber, 14-28  
  propagate qos to l2tp, 14-31  
link group configuration mode  
  qos mode, 14-36  
  qos policy metering, 14-42  
  qos policy policing, 14-44  
  qos policy queuing, 14-46  
  qos priority, 14-49  
LI profile configuration mode  
  header, 19-5  
  pending, 19-7  
  transport udp, 19-8  
  type, 19-10

## M

metering policy configuration mode  
  mark dscp, 12-31  
  mark precedence, 12-33  
  mark priority, 12-35  
  rate, 12-40  
MPLS router configuration mode  
  egress prefer dscp-qos, 14-24  
  propagate qos from-mpls, 14-27  
  propagate qos to-mpls, 14-33

## N

NAT policy configuration mode  
  access-group, 8-16  
  drop, 10-13  
  ignore, 10-14  
  ip dmz, 10-15  
  ip static in, 10-18  
  ip static out, 10-20  
  pool, 10-24  
  timeout, 10-25  
NAT pool configuration mode  
  address, 10-11  
ND router configuration mode  
  interface, 3-5  
  ns-interval, 3-8  
  preferred-lifetime, 3-10  
  ra, 3-14  
  reachable-time, 3-16  
  valid-lifetime, 3-19

ND router interface configuration mode  
  neighbor, 3-7  
  ns-interval, 3-8  
  preferred-lifetime, 3-10  
  prefix, 3-12  
  ra, 3-14  
  reachable-time, 3-16  
  valid-lifetime, 3-19  
NTP configuration mode  
  slowsync, 4-9  
num-queues configuration mode  
  queue priority, 13-41

## P

policing policy configuration mode  
  mark dscp, 12-31  
  mark precedence, 12-33  
  mark priority, 12-35  
  rate, 12-40  
policy ACL class configuration mode  
  drop  
    forward policies, 9-14  
    NAT policies, 10-13  
  ignore, 10-14  
  mark dscp, 12-31  
  mark precedence, 12-33  
  mark priority, 12-35  
  mirror destination, 9-23  
  pool, 10-24  
  rate, 12-40  
  rate percentage, 12-42  
  redirect destination circuit, 9-25  
  redirect destination local, 7-11  
  redirect destination next-hop, 9-26  
  timeout, 10-25  
policy ACL configuration mode  
  class, 8-21  
policy class rate configuration mode  
  conform mark dscp, 12-13  
  conform mark precedence, 12-16  
  conform mark priority, 12-18  
  conform no-action, 12-20  
  exceed drop, 12-21  
  exceed mark dscp, 12-23  
  exceed mark precedence, 12-25  
  exceed mark priority, 12-27  
  exceed no-action, 12-29  
  violate drop, 12-44  
  violate mark dscp, 12-46  
  violate mark precedence, 12-49  
  violate mark priority, 12-51  
  violate no-action, 12-53



---

- policy rate configuration mode
  - conform mark dscp, 12-13
  - conform mark precedence, 12-16
  - conform mark priority, 12-18
  - conform no-action, 12-20
  - exceed drop, 12-21
  - exceed mark dscp, 12-23
  - exceed mark precedence, 12-25
  - exceed mark priority, 12-27
  - exceed no-action, 12-29
  - violate drop, 12-44
  - violate mark dscp, 12-46
  - violate mark precedence, 12-49
  - violate mark priority, 12-51
  - violate no-action, 12-53
- port configuration mode
  - forward output, 9-16
  - forward policy in, 9-19
  - forward policy out, 9-21
  - qos hierarchical mode, 14-34
  - qos mode, 14-36
  - qos node-group, 14-40
  - qos policy metering, 14-42
  - qos policy policing, 14-44
  - qos policy queuing, 14-46
  - qos priority, 14-49
  - qos rate, 14-51
  - radius attribute nas-port-type, 16-36
- PQ policy configuration mode
  - num-queues, 13-20
  - queue depth, 13-35
  - queue-map, 13-39
  - queue rate, 13-46
  - queue red, 13-47
- PWFQ policy
  - weight, 13-56
- PWFQ policy configuration mode
  - congestion-map, 13-19
  - num-queues, 13-20
  - queue-map, 13-39
  - queue priority, 13-41
  - queue priority-group, 13-44
  - rate, 13-54

## Q

- QoS metering policy configuration mode
  - access-group, 8-16
- QoS policing policy configuration mode
  - access-group, 8-16
- queue map configuration mode
  - num-queues, 13-20

## R

- RADIUS policy configuration mode
  - attribute, 16-9

## S

- service policy configuration mode
  - allow, 11-5
- subscriber configuration mode
  - access-list, 8-18
  - dhcp max-addrs, 5-24
  - dns, 6-4
  - forward policy in, 9-19
  - forward policy out, 9-21
  - http-redirect profile, 7-7
  - ip access-group, 8-35
  - ip interface, 5-40
  - ip subscriber arp, 2-15
  - nat policy-name, 10-23
  - qos node-reference, 14-41
  - qos policy metering, 14-42
  - qos policy policing, 14-44
  - qos policy queuing, 14-46

## T

- terminate error cause configuration mode
  - rbak-term-ec, 16-50

