

RS Switch Router Command Line Interface Reference

Release 8.0

36-008-07 Rev. 0A



River
STONE
NETWORKS™

COPYRIGHT NOTICES

© 2001 by Riverstone Networks, Inc. All rights reserved.

Riverstone Networks, Inc.
5200 Great America Parkway
Santa Clara, CA 95054

Printed in the United States of America

This product includes software developed by the University of California, Berkeley, and its contributors.

© 1979 – 1994 by The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley, and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Changes

Riverstone Networks, Inc., and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Riverstone Networks, Inc., to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

Disclaimer

IN NO EVENT SHALL RIVERSTONE NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF RIVERSTONE NETWORKS HAS BEEN ADVISED, KNOWN, OR SHOULD HAVE KNOWN, OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks

Riverstone Networks, Riverstone, RS, and IA are trademarks of Riverstone Networks, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

REGULATORY COMPLIANCE INFORMATION

This product complies with the following:

SAFETY

UL 1950; CSA C22.2, No. 950; 73/23/EEC; EN 60950; IEC 950

ELECTROMAGNETIC

FCC Part 15; CSA C108.8; 89/336/EEC; EN 55022; EN 61000-3-2

COMPATIBILITY (EMC)

EN 61000-3-3; EN 50082-1, AS/NZS 3548; VCCI V-3

REGULATORY COMPLIANCE STATEMENTS



Note

Complies with Part 68, FCC rules.
FCC Registration Number 6TGUSA-46505-DE-N
Riverstone Networks, Inc.
Model WICT1-12
Made in U.S.A.

FCC COMPLIANCE STATEMENT

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



Note

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 uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

**Warning**

Changes or modifications made to this device that are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

INDUSTRY CANADA COMPLIANCE STATEMENT

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational, and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

VCCI COMPLIANCE STATEMENT

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

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。

SAFETY INFORMATION: CLASS 1 LASER TRANSCEIVERS

This product may use Class 1 laser transceivers. Read the following safety information before installing or operating this product.

The Class 1 laser transceivers use an optical feedback loop to maintain Class 1 operation limits. This control loop eliminates the need for maintenance checks or adjustments. The output is factory set and does not allow any user adjustment. Class 1 laser transceivers comply with the following safety standards:

- 21 CFR 1040.10 and 1040.11, U.S. Department of Health and Human Services (FDA)
- IEC Publication 825 (International Electrotechnical Commission)
- CENELEC EN 60825 (European Committee for Electrotechnical Standardization)

When operating within their performance limitations, laser transceiver output meets the Class 1 accessible emission limit of all three standards. Class 1 levels of laser radiation are not considered hazardous.

LASER RADIATION AND CONNECTORS

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6 dBm or $55 \times 10^{-6} \text{ watts}$.

Removing the optical connector from the transceiver allows laser radiation to emit directly from the optical port. The maximum radiance from the optical port (under worst case conditions) is 0.8 W cm^{-2} or $8 \times 10^3 \text{ W m}^{-2} \text{ sr}^{-1}$.

Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

SAFETY INFORMATION: WICT1-12 T1 CARD



Warning

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

CONSUMER INFORMATION AND FCC REQUIREMENTS

1. This equipment complies with Part 68 of the FCC rules, FCC Registration Number 6TGUSA-46505-DE-N Riverstone Networks Inc. Model WICT1-12 Made in the USA. On the DS1/E1 WAN Module of this equipment is a label that contains, among other information, the FCC registration number and Ringer Equivalence Number (REN) for this equipment. If requested, provide this information to your telephone company.
2. The REN is useful to determine the quantity of devices you may connect to your telephone and still have all those devices ring when your number is called. In most, but not all areas, the sum of the REN's of all devices should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should call your local telephone company to determine the maximum REN for your calling area.
3. If your DS1/E1 WAN Module causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.
4. Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice so as to give you an opportunity to maintain uninterrupted service.
5. If you experience trouble with this equipment DS1/E1 WAN Module, please contact Riverstone Networks Inc., 5200 Great America Parkway, Santa Clara, CA 95054, 408 878-6500, for repair/warranty information. The Telephone Company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.
6. There are no repairs that can be made by the customer to the DS1/E1WAN Module.
7. This equipment may not be used on coin service provided by the Telephone Company. Connection to party lines is subject to state tariffs. (Contact your state public utility commission or corporation commission for information).

EQUIPMENT ATTACHMENT LIMITATIONS NOTICE

The Industry Canada label identifies certified equipment. This certification means that the equipment meets the telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

RIVERSTONE NETWORKS, INC.
STANDARD SOFTWARE LICENSE AGREEMENT

IMPORTANT: BEFORE UTILIZING THE PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is a legal agreement ("Agreement") between You, the end user, and Riverstone Networks, Inc. ("Riverstone"). BY USING THE ENCLOSED SOFTWARE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THE RIVERSTONE STANDARD LIMITED WARRANTY, WHICH IS INCORPORATED HEREIN BY REFERENCE. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED LICENSED MATERIALS, ALONG WITH THE HARDWARE PURCHASED IF PROVIDED ON SUCH HARDWARE, AND PROOF OF PAYMENT TO RIVERSTONE OR YOUR DEALER, IF ANY, WITHIN THIRTY (30) DAYS FROM THE DATE OF PURCHASE FOR A FULL REFUND.

The parties further agree that this Agreement is between You and Riverstone, and creates no obligations to You on the part of Riverstone's affiliates, subcontractors, or suppliers. You expressly relinquish any rights as a third party beneficiary to any agreements between Riverstone and such parties, and waive any and all rights or claims against any such third party.

- 1. GRANT OF SOFTWARE LICENSE.** Subject to the terms and conditions of this Agreement, Riverstone grants You the right on a non-exclusive, basis for internal purposes only and only as expressly permitted by this Agreement
 - a. to use the enclosed software program (the "Licensed Software") in object code form on a single processing unit owned or leased by You or otherwise use the software as embedded in equipment provided by Riverstone;
 - b. to use the Licensed Software on any replacement for that processing unit or equipment;
 - c. to use any related documentation (collectively with the Licensed Software the "Licensed Materials"), provided that You may not copy the documentation;
 - d. to make copies of the Licensed Software in only the amount necessary for backup or archival purposes, or to replace a defective copy; provided that You (i) have not more than two (2) total copies of the Licensed Software including the original media without Riverstone's prior written consent, (ii) You operate no more than one copy of the Licensed Software, (iii) and You retain all copyright, trademark and other proprietary notices on the copy.
- 2. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS.** All rights not expressly granted herein are reserved by Riverstone or its suppliers or licensors. Without limiting the foregoing You agree
 - a. to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You;
 - b. not to use, copy or modify the Licensed Materials, in whole or in part, except as expressly provided in this Agreement;
 - c. not to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language; provided that, if You are located within a Member State of the European community, then such activities shall be permitted solely to the extent, if any, permitted under Article 6 of the Council Directive of 14 May 1991 on the legal protection of computer programs, and implementing legislations thereunder.
- 3. TERM AND TRANSFER.** You may transfer the License Materials with a copy of this Agreement to another party only on a permanent basis in connection with the transfer to the same party of the equipment on which it is used, and only if the other party accepts the terms and conditions of this Agreement. Upon such transfer, You must transfer all accompanying written materials, and either transfer or destroy all copies of the Software. Any attempted transfer not permitted by this Agreement is void. You may not lease or rent the License Materials. This Agreement is effective until terminated. You may terminate the Agreement at any time by destroying or purging all copies of the Licensed Materials. This Agreement will terminate automatically without notice from Riverstone if You fail to comply with any provision of this Agreement. Upon such termination, You must destroy the Licensed Materials as set forth above. Sections 4, 5, 6, 7, 8, 9, and 10 shall survive termination of this Agreement for any reason.
- 4. TITLE AND PROPRIETARY RIGHTS.**
 - (a) The Licensed Materials are copyrighted works and/or trade secrets of Riverstone and are the sole and exclusive property of Riverstone, any company or a division thereof which Riverstone controls or is controlled by, or which may result from the merger or consolidation with Riverstone (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Material to You.
 - (b) You acknowledge that in the event of a breach of this Agreement, Riverstone shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You agree that in the event of a breach of this Agreement, Riverstone shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Riverstone.

5. **MAINTENANCE AND UPDATES.** Updates, upgrades, bug fixes, and maintenance and support services, if any, are provided to You pursuant to the terms of a Riverstone Service and Maintenance Agreement, and only if Riverstone and You enter into such an agreement. Except as specifically set forth in such agreement, Riverstone is under no obligation to provide any updates, upgrades, patches, bug fixes, modifications, enhancements, or maintenance or support services to You. Notwithstanding the foregoing, if you are provided or obtain any software or documentation of Riverstone, which is not otherwise provided under a license from Riverstone, then Your use of such materials shall be subject to the terms of this Riverstone Networks, Inc. Software License Agreement.
6. **EXPORT REQUIREMENTS.** Licensed Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. You agree to comply strictly with all such regulations and acknowledge that you have the responsibility to obtain licenses to export, re-export or import Licensed Materials.
7. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure of the Licensed Materials and accompanying documentation by the U.S. Government is subject to restrictions as set forth in this Agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DRAS 252.227-7013(c)(ii) (OCT 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable. Riverstone Networks, Inc.
8. **LIMITED WARRANTY.** The sole warranty provided under this Agreement and with respect to the Licensed Materials is set forth in Riverstone's Standard Limited Warranty, which is incorporated herein by reference. THE RIVERSTONE STANDARD LIMITED WARRANTY CONTAINS IMPORTANT LIMITS ON YOUR WARRANTY RIGHTS. THE WARRANTIES AND LIABILITIES SET FORTH IN THE STANDARD LIMITED WARRANTY ARE EXCLUSIVE AND ESTABLISH RIVERSTONE'S ONLY OBLIGATIONS AND YOUR SOLE RIGHTS WITH RESPECT TO THE LICENSED MATERIALS AND THIS AGREEMENT. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.
9. **LIMITATION OF LIABILITY.** Your exclusive remedy for any claim in connection with the Licensed Materials and the entire liability of Riverstone are set forth in the Riverstone Standard Limited Warranty. Except to the extent provided there, if any, IN NO EVENT WILL RIVERSTONE OR ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR ANY LOSS OF USE, INTERRUPTION OF BUSINESS, LOST PROFITS OR LOST DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF RIVERSTONE OR ITS AFFILIATE OR SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND WHETHER OR NOT ANY REMEDY PROVIDED SHOULD FAIL OF ITS ESSENTIAL PURPOSE. THE TOTAL CUMULATIVE LIABILITY TO YOU, FROM ALL CAUSES OF ACTION AND ALL THEORIES OF LIABILITY, WILL BE LIMITED TO AND WILL NOT EXCEED THE PURCHASE PRICE OF THE LICENSED MATERIALS PAID BY YOU. YOU ACKNOWLEDGE THAT THE AMOUNT PAID FOR THE LICENSED MATERIALS REFLECTS THIS ALLOCATION OF RISK.
10. **GENERAL.** The provisions of the Agreement are severable and if any one or more of the provisions hereof are illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto. Riverstone's waiver of any right shall not constitute waiver of that right in future. This Agreement (including the documents it incorporates) constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws of the State of California, excluding the UN Convention on Contracts for the International Sale of Goods and that body of law known as conflicts of laws. Any dispute in connection with the Licensed Materials will be resolved in state or federal courts located in Santa Clara County, California, U.S.A.. You consent to the personal jurisdiction of and waive any objections to venue in such courts.

STANDARD LIMITED WARRANTY

Limited Warranty

Riverstone Networks, Inc. (“Riverstone”) warrants that for a period of one (1) year from the date of shipment from Riverstone that the Riverstone hardware purchased by Customer (“Hardware”) will be free from defects in materials and workmanship under normal use. This limited warranty extends only to Customer as original purchaser. Customer’s sole and exclusive remedy and the entire liability of Riverstone, its suppliers and affiliates under this warranty is, at Riverstone’s option, either (i) repair of the Hardware, (ii) replacement of the Hardware, or (iii) refund of the purchase price of the Hardware (as evidenced by a copy of Customer’s purchase receipt), less any rebates or credits.

Riverstone warrants that for a period of one (1) year from the date of shipment from Riverstone that the media on which the Riverstone software purchased by Customer (“Software”) is furnished will be free from defects in materials and workmanship under normal use. This limited warranty extends only to Customer as original licensee. Customer’s sole and exclusive remedy and the entire liability of Riverstone, its suppliers and affiliates under this warranty is replacement of the media on which the Software is furnished. Riverstone makes no warranty with respect to the Software, and specifically disclaims any warranty that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.

Restrictions. No warranty will apply if the Hardware and/or Software (collectively, “Product”) (i) has been altered, except by Riverstone; (ii) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Riverstone; or (iii) has been subjected to abnormal physical, thermal or electrical stress, misuse, negligence, or accident. In addition, Products are not designed or intended for use in (i) the design, construction, operation or maintenance of any nuclear facility, (ii) navigating or operating aircraft; or (iii) operating life-support or life-critical medical equipment, and Riverstone disclaims any express or implied warranty of fitness for such uses.

Warranty Service Procedures

Customer must notify Riverstone of any defect in the Product within the applicable warranty period and provide dated proof of original purchase prior to the return of any defective Product. Within ten (10) business days of the date of notification, Riverstone will provide Customer with a Return Material Authorization (“RMA”) number and the location to which Customer must return the defective Product. Customer is responsible for proper packaging of Product returned to Riverstone, including description of the failure, shipment to Riverstone’s designated location, and return of Product within ten (10) days after issuance of the RMA number. In no event will Riverstone accept any returned Product which does not have a valid RMA number. Customer’s failure to return Product within thirty (30) days of its receipt of an RMA may result in cancellation of the RMA and/or the charge of the list price of any advanced replacement product. Riverstone does not accept responsibility for any Product lost in transit and recommends that the return be insured for the full value. Riverstone will use all reasonable efforts within thirty (30) days of receipt of defective Product to repair or replace such Product or refund Customer’s purchase price.

Transportation costs relating to warranty service and any applicable duties will be borne by Customer. If a warranty claim is invalid for any reason, Customer will be charged at Riverstone’s then-current standard rates for services performed and will be charged for all expenses incurred by Riverstone.

Replacement Products or replacement parts used in the repair of Products may be new or reconditioned.

Riverstone shall not be responsible for Customer’s or any third party’s software, firmware, information, or memory

data contained in, sorted on, or integrated with any Product returned to Riverstone, whether under warranty or not. Customer is responsible for backing up its programs and data to protect against loss or corruption.

Disclaimer. EXCEPT AS SPECIFIED ABOVE, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

Limitation of Liability. IN NO EVENT WILL RIVERSTONE OR ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR ANY LOSS OF USE, INTERRUPTION OF BUSINESS, LOST PROFITS, OR LOST DATA, OR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OF ANY KIND REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF RIVERSTONE OR ITS AFFILIATE OR SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND WHETHER OR NOT ANY REMEDY PROVIDED SHOULD FAIL OF ITS ESSENTIAL PURPOSE. THE TOTAL CUMULATIVE LIABILITY TO CUSTOMER, FROM ALL CAUSES OF ACTION AND ALL THEORIES OF LIABILITY, WILL BE LIMITED TO AND WILL NOT EXCEED THE PURCHASE PRICE OF THE PRODUCT PAID BY CUSTOMER.

DECLARATION OF CONFORMITY ADDENDUM

Application of Council Directive(s)	89/336/EEC 73/23/EEC
Manufacturer's Name	Riverstone Networks, Inc.
Manufacturer's Address	5200 Great America Parkway Santa Clara, CA 95054
Conformance to Directive(s)/Product Standards	EC Directive 89/336/EEC EC Directive 73/23/EEC EN 55022 EN 50082-1 EN 60950
Equipment Type/Environment	Networking equipment for use in a commercial or light-industrial environment

TABLE OF CONTENTS

1	Preface	1-1
1.1	How to Use This Manual	1-1
1.2	Related Documentation	1-1
1.3	CLI Parameter Types	1-2
1.4	<port-list> Syntax	1-4
1.5	Use of wan-encapsulation	1-7
2	acl Commands	2-1
2.1	Command Summary	2-1
	acl apply interface	2-3
	acl apply port	2-5
	acl apply service	2-7
	acl clearCounters	2-9
	acl permit deny icmp	2-10
	acl permit deny igmp	2-12
	acl permit deny ip	2-14
	acl permit deny ip-protocol	2-17
	acl permit deny ipx	2-19
	acl permit deny ipxgn	2-21
	acl permit deny ipxrip	2-23
	acl permit deny ipxsap	2-24
	acl permit deny ipxtype20	2-26
	acl permit deny tcp	2-27
	acl permit deny udp	2-29
	acl-policy enable external	2-31
	acl show	2-32
3	acl-edit Commands	3-1
3.1	Command Summary	3-1
	acl-edit	3-2
	acl permit deny*	3-3
	delete	3-4
	exit	3-5
	move	3-6
	save	3-7
	show	3-8
4	aging Commands	4-1
4.1	Command Summary	4-1
	aging l2 disable	4-2

	aging l2 set aging-timeout	4-3
	aging l2 show status	4-4
	aging l3 set timeout	4-5
	aging l3 set nat-flow-timeout	4-6
	aging l3 show status	4-7
5	arp Commands	5-1
5.1	Command Summary	5-1
	arp add	5-2
	arp clear	5-4
	arp set drop-unresolved	5-5
	arp set interface.	5-6
	arp set unresolve-threshold.	5-7
	arp set unresolve-timer	5-8
	arp show	5-9
6	atm Commands.	6-1
6.1	Command Summary	6-1
	atm add vcl	6-3
	atm apply service	6-5
	atm clear stats	6-7
	atm create vcgroup	6-8
	atm create vcl	6-9
	atm define service.	6-11
	atm ping	6-15
	atm restart ppp	6-16
	atm set cross-connect	6-17
	atm set peer-addr	6-18
	atm set port cell-mapping.	6-19
	atm set port oam-detect-down	6-20
	atm set port oam-detect-up.	6-21
	atm set port pdh-cell-scramble	6-22
	atm set port vpi-bits	6-23
	atm set vcgroup.	6-25
	atm set vcl.	6-26
	atm set vcl-buffering.	6-28
	atm set vcl-priority	6-30
	atm set vcl-qos	6-32
	atm show port-settings	6-34
	atm show ppp	6-37
	atm show service	6-40
	atm show stats.	6-42
	atm show vcgroup.	6-44
	atm show vcl.	6-46
	atm show vpl.	6-49
7	bgp Commands.	7-1
7.1	Command Summary	7-1
	bgp add peer-host	7-3
	bgp clear flap-statistics.	7-4

	bgp clear peer-host	7-5
	bgp create peer-group	7-6
	bgp set cluster-id	7-8
	bgp set compare-MED	7-9
	bgp set dampenflap	7-10
	bgp set default-localpref	7-12
	bgp set default-metric	7-13
	bgp set multipath	7-14
	bgp set peer-group	7-15
	bgp set peer-host	7-21
	bgp set preference	7-27
	bgp show aspath-regular-expression	7-28
	bgp show aspaths	7-30
	bgp show cidr-only	7-31
	bgp show community	7-32
	bgp show community-list	7-34
	bgp show flap-statistics	7-35
	bgp show neighbor	7-36
	bgp show peer-as	7-38
	bgp show peer-group-type	7-39
	bgp show peer-host	7-40
	bgp show regexp	7-42
	bgp show routes	7-43
	bgp show summary	7-45
	bgp show sync-tree	7-46
	bgp start stop	7-48
	bgp trace	7-49
8	cisco-hdlc Commands	8-1
8.1	Command Summary	8-1
	cisco-hdlc apply service	8-2
	cisco-hdlc clear stats-counter	8-3
	cisco-hdlc define service	8-4
	cisco-hdlc restart slarp	8-7
	cisco-hdlc set cisco-hdlc-encaps-bgd	8-8
	cisco-hdlc show	8-9
9	cli Commands.	9-1
9.1	Command Summary	9-1
	cli set command completion	9-2
	cli set history	9-3
	cli set terminal	9-4
	cli show history	9-5
	cli show terminal	9-6
	cli terminal monitor	9-8
10	cmts Commands	10-1
10.1	Command Summary	10-1
	cmts clear error-stats	10-4
	cmts clear flap-list	10-6

cmts clear map-stats	10-7
cmts clear misc-stats	10-8
cmts clear packet-stats	10-9
cmts reset ak	10-11
cmts reset modem	10-12
cmts reset tek	10-13
cmts set ak	10-14
cmts set cpe	10-15
cmts set dschannel	10-16
cmts set flapthresh	10-19
cmts set headend	10-21
cmts set ipc-local	10-24
cmts set ipc-main	10-25
cmts llc-ping	10-26
cmts set mac	10-27
cmts set modem	10-29
cmts set modulation	10-30
cmts set multicast-ip	10-32
cmts set multicast-sid	10-33
cmts set privacy	10-34
cmts set relay-agent	10-35
cmts set tek	10-36
cmts set uschannel	10-37
cmts show ak	10-39
cmts show dschannel	10-41
cmts show error-stats	10-43
cmts show flap-list	10-45
cmts show flap-thresh	10-46
cmts show headend	10-48
cmts show mac	10-50
cmts show map-stats	10-52
cmts show misc-stats	10-56
cmts show modem	10-57
cmts show modulation	10-59
cmts show multicast-ip	10-61
cmts show multicast-sid	10-62
cmts show packet-stats	10-63
cmts show privacy	10-64
cmts show qosprofile	10-66
cmts show qosproppermissions	10-68
cmts show signalquality	10-69
cmts show service	10-70
cmts show status	10-71
cmts show tek	10-73
cmts show uschannel	10-75
cmts-diag set 3033	10-77
11 comment Commands	11-1
11.1 Command Summary	11-1
comment out	11-2
comment in	11-3

	comment line	11-4
	comment move	11-5
12	configure Command	12-1
	configure	12-1
13	copy Command	13-1
	copy	13-1
14	dhcp Commands	14-1
14.1	Command Summary	14-1
	dhcp attach superscope	14-2
	dhcp define parameters	14-3
	dhcp define pool	14-5
	dhcp define static-ip	14-6
	dhcp flush	14-8
	dhcp global set commit-interval	14-9
	dhcp global set lease-database	14-10
	dhcp show binding	14-11
	dhcp show num-clients	14-12
15	diff Command	15-1
	diff	15-1
16	dvmrp Commands	16-1
16.1	Command Summary	16-1
	dvmrp accept route	16-2
	dvmrp advertise route	16-3
	dvmrp create tunnel	16-4
	dvmrp enable no-pruning	16-5
	dvmrp enable interface	16-6
	dvmrp set interface	16-8
	dvmrp show interface	16-10
	dvmrp show routes	16-12
	dvmrp show rules	16-16
	dvmrp start	16-17
17	enable Command	17-1
	enable	17-1
18	erase Command	18-1
	erase	18-1
19	exit Command	19-1
	exit	19-1

20	file Commands	20-1
20.1	Command Summary	20-1
	file copy	20-2
	file delete	20-3
	file dir	20-4
	file reformat	20-5
	file rename	20-6
	file type.	20-7
21	filters Commands	21-1
21.1	Command Summary	21-1
	filters add address-filter	21-3
	filters add port-address-lock	21-4
	filters add secure-port	21-5
	filters add static-entry	21-6
	filters show address-filter	21-8
	filters show port-address-lock	21-9
	filters show secure-port	21-10
	filters show static-entry	21-11
22	frame-relay Commands.	22-1
22.1	Command Summary	22-1
	frame-relay apply service	22-2
	frame-relay clear stats-counter	22-3
	frame-relay create vc	22-4
	frame-relay define service	22-5
	frame-relay set fr-encaps-bgd	22-8
	frame-relay set lmi	22-9
	frame-relay set payload-compress	22-11
	frame-relay set peer-addr	22-12
	frame-relay show service	22-13
	frame-relay show stats	22-14
	frame-relay show stats summary	22-16
23	garp Commands	23-1
23.1	Command Summary	23-1
	garp set timers.	23-2
	garp show timers.	23-3
24	gvrp Commands	24-1
24.1	Command Summary	24-1
	gvrp clear statistics	24-2
	gvrp enable dynamic-vlan-creation	24-3
	gvrp enable ports	24-4
	gvrp set applicant-status	24-5
	gvrp set registration-mode	24-6
	gvrp show applicant status	24-7
	gvrp show error-statistics	24-8

	gvrp show registration-mode	24-9
	gvrp show statistics	24-11
	gvrp show status	24-13
	gvrp start	24-14
25	hrt Command	25-1
25.1	Command Summary	25-1
	hrt enable	25-2
	hrt set icmp icmp-redirect-count	25-3
26	igmp Commands	26-1
26.1	Command Summary	26-1
	igmp enable interface	26-2
	igmp enable vlan	26-3
	igmp join group	26-4
	igmp set interface	26-5
	igmp set queryinterval	26-6
	igmp set responsetime	26-7
	igmp set vlan	26-8
	igmp show interfaces	26-9
	igmp show memberships	26-11
	igmp show timers	26-12
	igmp show vlans	26-14
	igmp start-snooping	26-16
27	interface Commands	27-1
27.1	Command Summary	27-1
	interface add ip	27-2
	interface add ipx	27-3
	interface create ip	27-5
	interface create ipx	27-9
	interface show ip	27-12
	interface show ipx	27-13
28	ip Commands	28-1
28.1	Command Summary	28-1
	ip add route	28-3
	ip apply custom-forwarding-mode	28-6
	ip bgp-accounting	28-7
	ip clear bgp-actg	28-9
	ip clear reverse-flows	28-10
	ip community-list	28-11
	ip define custom-forwarding-profile	28-12
	ip disable	28-14
	ip disable webcache-actg	28-16
	ip dos disable	28-17
	ip dos enable	28-19
	ip dos rate-limit	28-20
	ip enable bgp-actg-on	28-22

	ip enable custom-forwarding-mode	28-23
	ip enable directed-broadcast	28-24
	ip enable reverse-flow	28-25
	ip enable reverse-path-forwarding	28-26
	ip helper-address	28-27
	ip l3-deep-hashing	28-29
	ip l3-hash	28-30
	ip set data-receive-size control-receive-size	28-31
	ip set multipath-hash-variant	28-32
	ip set port forwarding-mode	28-33
	ip show community-list	28-35
	ip show connections	28-36
	ip show custom-forwarding-mode	28-37
	ip show custom-forwarding-profile	28-38
	ip show dos rate-limit	28-39
	ip show hash-variant	28-40
	ip show helper-address	28-42
	ip show mode	28-43
	ip show interfaces	28-44
	ip show reverse-flows	28-46
	ip show routes	28-47
	ip show stack-queues	28-49
29	ip-policy Commands	29-1
29.1	Command Summary	29-1
	ip-policy apply	29-2
	ip-policy clear	29-3
	ip-policy deny	29-4
	ip-policy permit	29-6
	ip-policy set load-policy	29-9
	ip-policy set pinger on	29-10
	ip-policy set pinger-options	29-11
	ip-policy show	29-13
30	ip-redundancy Commands	30-1
30.1	Command Summary	30-1
	ip-redundancy associate	30-2
	ip-redundancy clear vrrp-stats	30-3
	ip-redundancy create	30-4
	ip-redundancy set vrrp	30-5
	ip-redundancy show vrrp	30-7
	ip-redundancy start vrrp	30-10
	ip-redundancy trace	30-11
31	ip-router Commands	31-1
31.1	Command Summary	31-1
	ip-router authentication add key-chain	31-4
	ip-router authentication create key-chain	31-5
	ip-router clear dropped-route-stats	31-6
	ip-router find route	31-7

ip-router global add interface	31-8
ip-router global add martian	31-9
ip-router global set autonomous-system	31-10
ip-router global set confederation-id	31-11
ip-router global set install-lsp-routes	31-12
ip-router global set interface	31-13
ip-router global set max-bgjob-interval	31-14
ip-router global set memory-threshold	31-15
ip-router global set router-id	31-16
ip-router global set trace-level	31-17
ip-router global set trace-options	31-18
ip-router global set trace-state	31-19
ip-router global use provided_config	31-20
ip-router kernel set flash-inst-cnt	31-21
ip-router kernel set inst-cnt	31-22
ip-router kernel trace	31-23
ip-router policy add aspath-regular-expression	31-24
ip-router policy add community-list	31-26
ip-router policy add filter	31-28
ip-router policy add optional-attributes-list	31-30
ip-router policy aggr-gen destination	31-31
ip-router policy create aggr-export-source	31-33
ip-router policy create aggr-gen-dest	31-34
ip-router policy create aggr-gen-source	31-35
ip-router policy create aspath-export-source	31-37
ip-router policy create aspath-regular-expression	31-39
ip-router policy create bgp-export-destination	31-40
ip-router policy create bgp-export-source	31-42
ip-router policy create bgp-import-source	31-44
ip-router policy create community-list	31-46
ip-router policy create direct-export-source	31-47
ip-router policy create filter	31-48
ip-router policy create isis-export-destination	31-49
ip-router policy create isis-export-source	31-50
ip-router policy create optional-attributes-list	31-51
ip-router policy create ospf-export-destination	31-53
ip-router policy create ospf-export-source	31-54
ip-router policy create ospf-import-source	31-55
ip-router policy create rip-export-destination	31-56
ip-router policy create rip-export-source	31-57
ip-router policy create rip-import-source	31-58
ip-router policy create static-export-source	31-59
ip-router policy create tag-export-source	31-60
ip-router policy export destination	31-61
ip-router policy import source	31-63
ip-router policy redistribute	31-65
ip-router policy summarize route	31-68
ip-router show configuration file	31-70
ip-router show rib	31-71
ip-router show route	31-73
ip-router show route-preferences	31-75
ip-router show state	31-76

	ip-router show summary	31-77
32	ipx Commands	32-1
32.1	Command Summary	32-1
	ipx add route	32-2
	ipx add sap	32-3
	ipx find rip	32-4
	ipx find sap	32-5
	ipx l3-hash	32-6
	ipx set interface	32-7
	ipx set port	32-8
	ipx set rip buffers	32-9
	ipx set ripreq buffers	32-10
	ipx set sap buffers	32-11
	ipx set sapgns	32-12
	ipx set type20 propagation	32-13
	ipx show buffers	32-14
	ipx show hash-variant	32-15
	ipx show interfaces	32-17
	ipx show rib	32-18
	ipx show servers	32-19
	ipx show summary	32-20
33	isis Commands	33-1
33.1	Command Summary	33-1
	isis add area	33-3
	isis add interface	33-4
	isis add label-switched-path	33-5
	isis add summary-filt	33-6
	isis add summary-orig	33-7
	isis set area-key-chain	33-8
	isis set domain-key-chain	33-9
	isis set domain-wide	33-10
	isis set external-preference	33-11
	isis set igp-shortcuts	33-12
	isis set interface	33-13
	isis set level	33-17
	isis set overload-bit	33-18
	isis set preference	33-19
	isis set psn-interval	33-20
	isis set reference-bandwidth	33-21
	isis set require-snp-auth	33-22
	isis set spf-interval	33-23
	isis set system-id	33-24
	isis set traffic-engineering	33-25
	isis show adjacencies	33-26
	isis show all	33-28
	isis show circuits	33-29
	isis show export-policies	33-30
	isis show globals	33-31
	isis show lsp-database	33-32

	isis show timers	33-34
	isis start	33-36
	isis stop.	33-37
	isis trace	33-38
34	I2-tables Commands	34-1
34.1	Command Summary	34-1
	l2-tables show all-flows	34-2
	l2-tables show all-macs	34-3
	l2-tables show bridge-management	34-5
	l2-tables show igmp-mcast-registrations	34-6
	l2-tables show mac.	34-8
	l2-tables show mac-table-stats	34-9
	l2-tables show port-macs	34-10
	l2-tables show vlan-igmp-status.	34-12
35	lACP Commands	35-1
35.1	Command Summary	35-1
	lACP set aggregator	35-2
	lACP set port	35-3
	lACP set system	35-4
	lACP show aggregator	35-5
	lACP show keygroup	35-6
	lACP show lag	35-7
	lACP show port	35-8
36	ldp Commands	36-1
36.1	Command Summary	36-1
	ldp add export-filter	36-3
	ldp add import-filter	36-5
	ldp add interface.	36-7
	ldp add l2-fec	36-8
	ldp add prefix-filter	36-9
	ldp add remote-peer	36-11
	ldp clear	36-12
	ldp map ports	36-13
	ldp set egress-policy	36-14
	ldp set global	36-15
	ldp set interface	36-16
	ldp set l2-fec.	36-18
	ldp set md5-password.	36-20
	ldp set remote-peer.	36-21
	ldp set trace-level	36-22
	ldp set trace-options	36-23
	ldp show all	36-24
	ldp show database	36-26
	ldp show global	36-29
	ldp show interface	36-30
	ldp show l2-fec.	36-32
	ldp show neighbor	36-34

	ldp show session	36-36
	ldp show statistics	36-39
	ldp start	36-42
37	lfap Commands	37-1
37.1	Command Summary	37-1
	lfap set batch-interval	37-2
	lfap set batch-size	37-3
	lfap set lost-contact-interval	37-4
	lfap set poll-interval	37-5
	lfap set priority	37-6
	lfap set send	37-7
	lfap set send-queue-max-size	37-9
	lfap set server	37-10
	lfap set server-retry-interval	37-11
	lfap show all	37-12
	lfap show configuration	37-13
	lfap show servers	37-14
	lfap show statistics	37-15
	lfap show status	37-16
	lfap start	37-17
38	load-balance Commands	38-1
38.1	Command Summary	38-1
	load-balance add group-for-mirroring	38-3
	load-balance add host-to-group	38-4
	load-balance add host-to-vip-range	38-6
	load-balance allow access-to-servers	38-8
	load-balance create group-name	38-9
	load-balance create health-check-cluster	38-11
	load-balance create state-mirror-peer	38-12
	load-balance create vip-range-name	38-13
	load-balance set acv-file-size-limit	38-15
	load-balance set aging-for-src-maps	38-16
	load-balance set client-proxy-subnet	38-17
	load-balance set ftp-control-port	38-18
	load-balance set group-options	38-19
	load-balance set hash-variant	38-22
	load-balance set health-check-cluster-options	38-23
	load-balance set server-status	38-25
	load-balance set server-options	38-26
	load-balance set sipp-pat	38-29
	load-balance set vpn-dest-port	38-30
	load-balance set wildcard-lsnapt-range	38-31
	load-balance show acv-options	38-32
	load-balance show hash-stats	38-35
	load-balance show health-check-clusters	38-37
	load-balance show session-mirror-info	38-39
	load-balance show source-mappings	38-41
	load-balance show statistics	38-43
	load-balance show virtual-hosts	38-46

39	logout Command	39-1
	logout	39-1
40	mpls Commands	40-1
40.1	Command Summary	40-1
	mpls add interface	40-3
	mpls clear label-switched-paths	40-4
	mpls create admin-group	40-5
	mpls create l2-policy	40-6
	mpls create l2-static-path	40-8
	mpls create label-switched-path	40-9
	mpls create path	40-12
	mpls create policy	40-13
	mpls create static-path	40-16
	mpls set global	40-17
	mpls set interface	40-19
	mpls set l2-static-path	40-21
	mpls set label-switched-path	40-22
	mpls set path	40-25
	mpls set portlist	40-26
	mpls set static-path	40-28
	mpls set trace-level	40-30
	mpls set trace-options	40-31
	mpls show admin-groups	40-32
	mpls show all	40-33
	mpls show global	40-35
	mpls show hw-cam-tbl	40-37
	mpls show hw-ilm-err	40-39
	mpls show hw-ilm-tbl	40-41
	mpls show hw-ott-err	40-44
	mpls show hw-ott-tbl	40-46
	mpls show ilm-tbl	40-50
	mpls show interface	40-52
	mpls show l2-policy	40-56
	mpls show label-switched-paths	40-59
	mpls show ott-table	40-62
	mpls show paths	40-64
	mpls show policy	40-65
	mpls show static-paths	40-68
	mpls start	40-71
41	mtrace Command	41-1
	mtrace	41-1
42	multicast Commands	42-1
42.1	Command Summary	42-1
	multicast show interface	42-2
	multicast show mroutes	42-4

43	nat Commands	43-1
43.1	Command Summary	43-1
	nat clear-err-stats	43-2
	nat create dynamic	43-3
	nat create static	43-5
	nat flush-dynamic-binding	43-7
	nat set dns-session-timeout	43-9
	nat set dns-translation-state	43-10
	nat set dynamic-binding-timeout	43-11
	nat set ftp-control-port	43-12
	nat set ftp-session-timeout	43-13
	nat set interface	43-14
	nat set secure-plus	43-15
	nat set sipp-pat	43-16
	nat show	43-17
44	negate Command	44-1
	negate	44-1
45	no Command	45-1
	no	45-1
46	ntp Commands	46-1
46.1	Command Summary	46-1
	ntp set server	46-2
	ntp show all	46-4
	ntp synchronize server	46-5
47	ospf Commands	47-1
47.1	Command Summary	47-1
	ospf add interface	47-4
	ospf add label-switched-path	47-5
	ospf add nbma-neighbor	47-6
	ospf add network summary-range	47-7
	ospf add nssa-network	47-9
	ospf add pmp-neighbor	47-10
	ospf add stub-host	47-11
	ospf add summary-filters	47-12
	ospf add virtual-link	47-13
	ospf clear database	47-14
	ospf clear statistics	47-15
	ospf create area	47-16
	ospf create-monitor	47-17
	ospf monitor interfaces	47-18
	ospf monitor neighbors	47-19
	ospf monitor next-hop-list	47-20
	ospf monitor routes	47-22
	ospf monitor version	47-24
	ospf set advertise-subnet	47-25

	ospf set area	47-26
	ospf set ase-defaults	47-28
	ospf set authentication-method	47-30
	ospf set export-interval.	47-31
	ospf set export-limit	47-32
	ospf set hello-interval.	47-33
	ospf set igp-shortcuts	47-34
	ospf set interface	47-35
	ospf set monitor-auth-method	47-38
	ospf set opaque-capability	47-39
	ospf set poll-interval.	47-40
	ospf set preference	47-41
	ospf set priority	47-42
	ospf set ref-bwtdh.	47-43
	ospf set retransmit-interval.	47-44
	ospf set router-dead-interval	47-45
	ospf set spf-holdtime	47-46
	ospf set traffic-engineering	47-47
	ospf set transit-delay	47-48
	ospf set virtual-link	47-49
	ospf show adjacency-down-reason	47-51
	ospf show all	47-52
	ospf show areas	47-53
	ospf show as-external-lsdb.	47-55
	ospf show border-routes.	47-56
	ospf show database.	47-57
	ospf show export-policies	47-58
	ospf show globals.	47-59
	ospf show import-policies	47-61
	ospf show interfaces.	47-62
	ospf show lsa	47-63
	ospf show neighbor	47-65
	ospf show statistics.	47-66
	ospf show summary-asb.	47-68
	ospf show ted	47-69
	ospf show timers	47-70
	ospf show virtual-links.	47-71
	ospf start stop	47-72
48	ping Command	48-1
	ping.	48-1
49	port Commands	49-1
49.1	Command Summary	49-1
	port auto-negotiate	49-12
	port bert	49-13
	port bmon	49-15
	port clear per-vlan-stats	49-17
	port clear phy-errors.	49-18
	port description	49-19
	port disable.	49-20

	port enable 8021p	49-21
	port enable per-vlan-stats	49-22
	port enable wdm ports	49-23
	port flow-bridging	49-24
	port loopback	49-26
	port set	49-30
	port set cablelength.	49-36
	port set clock-source.	49-37
	port set crc	49-39
	port set fdl.	49-40
	port set framing.	49-42
	port set idle-code	49-46
	port set impedance	49-48
	port set international-bits	49-49
	port set invert-data	49-50
	port set lbo	49-51
	port set line-coding.	49-52
	port set national-bits	49-54
	port set remote-loopback-enable	49-55
	port set scrambling-mode	49-56
	port set speed-56 speed-64	49-57
	port set timeslots.	49-58
	port set ts16.	49-60
	port show 8021p	49-62
	port show autonegotiation	49-63
	port show autonegotiation-capabilities.	49-64
	port show bmon	49-66
	port show bridging-status	49-68
	port show description	49-69
	port show dsx-stats	49-70
	port show hash-mode	49-74
	port show MAU	49-75
	port show MAU-statistics.	49-76
	port show mirroring-status	49-77
	port show mtu.	49-78
	port show per-vlan-stats	49-79
	port show phy-errors.	49-81
	port show port-status	49-83
	port show pvst-info.	49-85
	port show serial-link-info	49-86
	port show stp-info.	49-97
	port show vlan-info.	49-98
	port testport.	49-99
50	port mirroring Command	50-1
	port mirroring	50-1
51	ppp Commands.	51-1
51.1	Command Summary	51-1
	ppp add-to-mlp	51-3
	ppp apply service	51-4

	ppp clear stats-counter	51-5
	ppp create-mlp	51-6
	ppp define service	51-7
	ppp restart lcp-ncp	51-11
	ppp set mlp-encaps-format	51-12
	ppp set mlp-frag-size	51-13
	ppp set mlp-fragq-depth	51-14
	ppp set mlp-orderq-depth	51-15
	ppp set mlp-preserv-pkt-order	51-16
	ppp set payload-compress	51-17
	ppp set payload-encrypt	51-18
	ppp set peer-addr	51-19
	ppp set ppp-encaps-bgd	51-20
	ppp show mlp	51-21
	ppp show service	51-22
	ppp show stats	51-23
52	pvst Commands	52-1
52.1	Command Summary	52-1
	pvst create spanningtree	52-2
	pvst enable port spanning-tree	52-3
	pvst set bridging spanning-tree	52-4
	pvst set port spanning-tree	52-6
	pvst show bridging-info spanning-tree	52-7
53	qos Commands	53-1
53.1	Command Summary	53-1
	qos apply priority-map	53-3
	qos create priority-map	53-4
	qos create one-p-overwrite-map	53-5
	qos overwrite tos-precedence-overwrite	53-7
	qos overwrite tos-byte-rewrite	53-8
	qos overwrite one-p-priority	53-9
	qos precedence ip	53-10
	qos precedence ipx	53-12
	qos priority-map off	53-14
	qos set ip	53-15
	qos set ip-acl	53-18
	qos set ipx	53-20
	qos set l2	53-22
	qos set queuing-policy	53-24
	qos set weighted-fair	53-25
	qos show ip	53-26
	qos show ipx	53-27
	qos show l2	53-28
	qos show one-p-priority-overwrite-with-tos	53-29
	qos show one-p-priority-overwrite-with-map	53-30
	qos show precedence	53-31
	qos show priority-map	53-32
	qos show tos-precedence-overwrite-with-1p	53-33
	qos show tos-precedence-overwrite-with-map	53-34

	qos show tos-byte-overwrite	53-35
	qos show wfq	53-36
	qos show wred	53-37
	qos wred	53-38
54	radius Commands	54-1
54.1	Command Summary	54-1
	radius accounting command level	54-2
	radius accounting shell	54-3
	radius accounting snmp	54-4
	radius accounting system	54-5
	radius authentication	54-6
	radius enable	54-7
	radius set deadtime	54-8
	radius set key	54-9
	radius set last-resort	54-10
	radius set retries	54-11
	radius set server	54-12
	radius set source	54-14
	radius set timeout	54-15
	radius show	54-16
55	rarpd Commands	55-1
55.1	Command Summary	55-1
	rarpd add	55-2
	rarpd set interface	55-3
	rarpd show	55-4
56	rate-limit Command	56-1
56.1	Command Summary	56-1
	rate-limit aggregate acl	56-2
	rate-limit apply	56-4
	rate-limit disable	56-5
	rate-limit enable	56-6
	rate-limit flow-aggregate	56-7
	rate-limit input acl	56-9
	rate-limit port-level input	56-11
	rate-limit port-level slot	56-13
	rate-limit port-level output	56-14
	rate-limit show	56-15
57	rdisc Commands	57-1
57.1	Command Summary	57-1
	rdisc add address	57-2
	rdisc add interface	57-3
	rdisc set address	57-4
	rdisc set interface	57-5
	rdisc show	57-6
	rdisc start	57-8

	rdisc stop	57-9
58	reboot Command	58-1
	reboot	58-1
59	rip Commands	59-1
59.1	Command Summary	59-1
	rip add interface	59-3
	rip add source-gateways	59-4
	rip add trusted-gateways	59-5
	rip set auto-summary	59-6
	rip set broadcast-state	59-7
	rip set check-zero	59-8
	rip set check-zero-metric	59-9
	rip set default-metric	59-10
	rip set interface	59-11
	rip set max-routes	59-14
	rip set multipath	59-15
	rip set poison-reverse	59-16
	rip set preference	59-17
	rip show	59-18
	rip start	59-19
	rip stop	59-20
	rip trace	59-21
60	rmon Commands	60-1
60.1	Command Summary	60-1
	rmon address-map	60-3
	rmon al-matrix-top-n	60-4
	rmon alarm	60-6
	rmon apply cli-filters	60-9
	rmon capture	60-10
	rmon channel	60-12
	rmon clear cli-filter	60-14
	rmon enable	60-15
	rmon etherstats	60-16
	rmon event	60-17
	rmon filter	60-19
	rmon history	60-21
	rmon hl-host	60-22
	rmon hl-matrix	60-24
	rmon host	60-26
	rmon host-top-n	60-27
	rmon matrix	60-29
	rmon nl-matrix-top-n	60-30
	rmon protocol-distribution	60-32
	rmon set	60-33
	rmon set cli-filter	60-35
	rmon set memory	60-37
	rmon set ports	60-39

	rmon set protocol-directory	60-40
	rmon show address-map	60-42
	rmon show al-host	60-44
	rmon show al-matrix	60-47
	rmon show al-matrix-top-n	60-49
	rmon show alarm	60-51
	rmon show channels	60-52
	rmon show cli-filters	60-53
	rmon show etherstats	60-54
	rmon show events	60-56
	rmon show filters	60-57
	rmon show history	60-58
	rmon show host-top-n	60-60
	rmon show hosts	60-62
	rmon show matrix	60-64
	rmon show nl-host	60-67
	rmon show nl-matrix	60-69
	rmon show nl-matrix-top-n	60-71
	rmon show packet-capture	60-73
	rmon show probe-config	60-74
	rmon show protocol-directory	60-75
	rmon show protocol-distribution	60-77
	rmon show status	60-78
	rmon show user-history	60-80
	rmon user-history-apply	60-81
	rmon user-history-control	60-82
	rmon user-history-objects	60-83
61	route-map Commands	61-1
61.1	Command Summary	61-1
	route-map permit/deny	61-2
	route-map set dampenflap	61-10
	route-map show	61-12
62	rsvp Commands	62-1
62.1	Command Summary	62-1
	rsvp add interface	62-2
	rsvp set global	62-3
	rsvp set interface	62-5
	rsvp set trace-level	62-6
	rsvp set trace-options	62-7
	rsvp show all	62-8
	rsvp show global	62-11
	rsvp show interface	62-13
	rsvp show neighbors	62-16
	rsvp show psb	62-18
	rsvp show rsb	62-19
	rsvp show session	62-20
	rsvp show tcsb	62-22
	rsvp start	62-23

63	save command	63-1
	save	63-1
64	service Commands	64-1
64.1	Command Summary	64-1
	service apply rate-limit acl	64-3
	service apply rate-limit mf-classifier	64-4
	service create rate-limit aggregate	64-7
	service create rate-limit burst-safe	64-9
	service create rate-limit flow-aggregate	64-11
	service create rate-limit per-flow	64-13
	service show rate-limit aggregate	64-14
	service show rate-limit all	64-15
	service show rate-limit burst-safe	64-17
	service show rate-limit flow-aggregate	64-18
	service show rate-limit per-flow	64-19
65	sfs Commands	65-1
65.1	Command Summary	65-1
	sfs enable cdp-hello	65-2
	sfs set cdp-hello transmit-frequency	65-3
	sfs show cdp-hello port-status	65-4
	sfs show cdp-hello transmit-frequency	65-5
66	show Command	66-1
	show	66-1
67	slogin Command	67-1
	slogin	67-1
68	smarttrunk Commands	68-1
68.1	Command Summary	68-1
	smarttrunk add ports	68-2
	smarttrunk clear load-distribution	68-3
	smarttrunk create	68-4
	smarttrunk set load-policy	68-6
	smarttrunk set load-redistribution-params	68-7
	smarttrunk show connections	68-9
	smarttrunk show distribution	68-11
	smarttrunk show load-redistribution-params	68-13
	smarttrunk show protocol-state	68-16
	smarttrunk show trunks	68-18
69	snmp Commands	69-1
69.1	Command Summary	69-1
	snmp disable trap	69-2
	snmp disable port-trap	69-3

	snmp set chassis-id	69-4
	snmp set community	69-5
	snmp set mib	69-6
	snmp set retro-mib-ifspeed	69-8
	snmp set target	69-9
	snmp set trap-source	69-10
	snmp show	69-11
	snmp stop	69-13
	snmp test trap	69-14
70	sonet Commands	70-1
70.1	Command Summary	70-1
	sonet set C2	70-3
	sonet set circuit-id	70-4
	sonet set fcs-16-bit	70-5
	sonet set framing	70-6
	sonet set J0	70-7
	sonet set loopback	70-8
	sonet set path-trace	70-9
	sonet set payload-scramble	70-10
	sonet set protected-by	70-11
	sonet set protection	70-12
	sonet set protection-switch	70-13
	sonet set revertive	70-14
	sonet set S1S0	70-15
	sonet set sd-ber	70-16
	sonet set sf-ber	70-17
	sonet set WTR-timer	70-18
	sonet show alarms	70-19
	sonet show aps	70-21
	sonet show loopback	70-22
	sonet show medium	70-23
	sonet show pathtrace	70-24
71	ssh Commands	71-1
71.1	Command Summary	71-1
	ssh server eliminate_key	71-2
	ssh server generate_key	71-3
	ssh server options	71-4
72	statistics Commands	72-1
72.1	Command Summary	72-1
	statistics clear	72-2
	statistics show arp	72-3
	statistics show framer	72-5
	statistics show icmp	72-6
	statistics show ip	72-7
	statistics show ip-interface	72-10
	statistics show ip-routing	72-12
	statistics show ipx	72-13

	statistics show ipx-interface	72-16
	statistics show ipx-routing	72-18
	statistics show multicast	72-19
	statistics show phy-errors	72-20
	statistics show port-errors	72-22
	statistics show port-packets	72-24
	statistics show port-stats	72-26
	statistics show rarp	72-29
	statistics show summary-stats	72-30
	statistics show tcp	72-31
	statistics show udp	72-33
	statistics show top	72-34
73	stp Commands	73-1
73.1	Command Summary	73-1
	stp enable port	73-2
	stp filter-bpdu	73-3
	stp set bridging	73-4
	stp set port	73-5
	stp set protocol-version	73-6
	stp set vlan-disable	73-7
	stp show bridging-info	73-8
	stp show dampening-info	73-9
	stp show protocol-version	73-10
74	system Commands.	74-1
74.1	Command Summary	74-1
	system disable inputportlevel-rate-limiting	74-4
	system disable nat	74-5
	system disable telnet-server	74-6
	system enable aggregate-rate-limiting	74-7
	system hotswap	74-8
	system image add	74-9
	system image choose	74-11
	system image copy	74-12
	system image delete	74-13
	system image list	74-14
	system kill ssh-session	74-16
	system kill telnet-session	74-17
	system l3-deep-hashing	74-18
	system promimage upgrade	74-19
	system set backup-cm-timeout	74-21
	system set bootprom	74-22
	system set console level	74-23
	system set console limit	74-24
	system set contact	74-25
	system set cpu-traffic-priority	74-26
	system set date	74-27
	system set dns	74-28
	system set dst	74-29
	system set extended-debug	74-32

	system set idle-timeout	74-33
	system set location	74-34
	system set login-banner	74-35
	system set name	74-36
	system set password	74-37
	system set poweron-selftest	74-39
	system set show-config	74-40
	system set syslog	74-41
	system set terminal	74-43
	system set timezone	74-44
	system show active-config	74-46
	system show bootlog	74-47
	system show bootprom	74-49
	system show capacity	74-50
	system show contact	74-54
	system show cpu-utilization	74-55
	system show date	74-56
	system show dns	74-57
	system show environmental-info	74-58
	system show hardware	74-59
	system show idle-timeout	74-61
	system show location	74-62
	system show login-banner	74-63
	system show name	74-64
	system show nat-state	74-65
	system show poweron-selftest-mode	74-66
	system show scratchpad	74-67
	system show serial-number	74-68
	system show ssh-access	74-69
	system show startup-config	74-70
	system show syslog	74-71
	system show syslog buffer	74-72
	system show telnet-access	74-73
	system show terminal	74-74
	system show timezone	74-75
	system show uptime	74-76
	system show users	74-77
	system show version	74-78
75	tacacs Commands	75-1
75.1	Command Summary	75-1
	tacacs enable	75-2
	tacacs set last-resort	75-3
	tacacs set server	75-4
	tacacs set timeout	75-5
	tacacs show	75-6
76	tacacs-plus Commands.	76-1
76.1	Command Summary	76-1
	tacacs-plus accounting command level	76-2
	tacacs-plus accounting shell	76-3

	tacacs-plus accounting snmp	76-4
	tacacs-plus accounting system	76-5
	tacacs-plus authentication	76-6
	tacacs-plus enable	76-7
	tacacs-plus set deadtime	76-8
	tacacs-plus set key	76-9
	tacacs-plus set last-resort	76-10
	tacacs-plus set retries	76-11
	tacacs-plus set server	76-12
	tacacs-plus set single-connect	76-14
	tacacs-plus set source	76-15
	tacacs-plus set timeout	76-16
	tacacs-plus show	76-17
77	telnet Command	77-1
	telnet	77-1
78	traceroute Command	78-1
79	vlan Commands	79-1
79.1	Command Summary	79-1
	vlan add ports	79-2
	vlan create	79-3
	vlan enable l4-bridging	79-6
	vlan enable stackable-vlan	79-7
	vlan forbid ports	79-8
	vlan make access-port	79-9
	vlan make trunk-port	79-10
	vlan show	79-11
80	wan Commands	80-1
80.1	Command Summary	80-1
	wan apply rate-shape-parameters	80-2
	wan clear rate-shape-statistics	80-5
	wan define rate-shape-parameters	80-6
	wan show rate-shape-parameters	80-8
	wan show rate-shape-policies	80-9
	wan show rate-shape-statistics	80-10
81	web-cache Commands	81-1
81.1	Command Summary	81-1
	web-cache apply interface	81-3
	web-cache apply port	81-4
	web-cache create bypass-list	81-5
	web-cache create filter	81-7
	web-cache create server-list	81-8
	web-cache permit deny hosts	81-9
	web-cache selection-policy	81-11
	web-cache set http-port	81-12

web-cache set maximum-connections	81-13
web-cache set redirect-protocol	81-14
web-cache set server-options	81-15
web-cache show all.	81-17
web-cache show cache-name	81-21
web-cache show servers	81-25
web-cache show statistics.	81-27

A	RMON 2 Protocol Directory.	A-1

LIST OF TABLES

Table 1-1	Related Documentation	1-1
Table 1-2	Parameter Types	1-2
Table 1-3	Port Types	1-4
Table 1-4	Pseudo Device Port Types.	1-5
Table 1-5	Port Ranges for Various Port Types	1-5
Table 1-6	Channel Ranges for Channelized T1, E1 and T3 Ports.	1-6
Table 6-1	Display field descriptions for the atm show port-settings command	6-35
Table 6-2	Display field descriptions for the atm show ppp command	6-38
Table 6-3	Display field descriptions for the atm show service command.	6-41
Table 6-4	Display field descriptions for the atm show vcgroup command.	6-44
Table 6-5	Display field descriptions for the atm show vcl command.	6-47
Table 6-6	Display field descriptions for the atm show vpl command.	6-50
Table 9-1	Display Field Descriptions for the cli show history Command	9-5
Table 9-2	Display Field Descriptions for the cli show history Command	9-7
Table 10-1	Forward error correction interleaving.	10-18
Table 10-1	Display Field Descriptions for the cmts show map-stats Command	10-53
Table 16-1	Display field descriptions for the dvmrp show interface command	16-11
Table 16-2	Display field descriptions for the dvmrp show routes command	16-14
Table 26-1	Display field descriptions for the igmp show interface command	26-10
Table 26-2	Display field descriptions for the igmp show timers command	26-12
Table 26-3	Display field descriptions for the igmp show vlans command	26-14
Table 29-1	Display Field Descriptions for the ip-policy show Command	29-14
Table 31-1	Display field descriptions for the ip-router show rib command	31-72
Table 36-1	Display field descriptions for the ldp show all command.	36-25
Table 36-2	Display field descriptions for the ldp show database command.	36-27
Table 36-3	LDP label binding state values	36-28
Table 36-4	Display field descriptions for the ldp show interface command.	36-30
Table 36-5	Display field descriptions for the ldp show interface verbose command	36-31
Table 36-6	Display field descriptions for the ldp show neighbor command.	36-34
Table 36-7	Display field descriptions for the ldp show neighbor verbose command.	36-35
Table 36-8	Display field descriptions for the ldp show session command	36-37
Table 36-9	Display field descriptions for the ldp show session verbose command	36-38
Table 36-10	Display field descriptions for the ldp show statistics command.	36-40
Table 38-1	Display field descriptions for the load-balance show acv-options command.	38-34

Table 38-2	Display field descriptions for the load-balance show hash-stats command	38-36
Table 38-1	Display field descriptions for the load-balance show health-check-clusters command	38-38
Table 38-1	Display field descriptions for the load-balance show session-mirror-info command	38-40
Table 38-2	Display field descriptions for the load-balance show source-mappings command	38-42
Table 38-3	Display field descriptions for the load-balance show statistics command	38-44
Table 38-4	Display field descriptions for the load-balance show virtual-hosts command	38-49
Table 40-1	Display field descriptions for the mpls show admin-groups command	40-32
Table 40-2	Display field descriptions for the mpls show all command	40-34
Table 40-3	Display field descriptions for the mpls show global command	40-35
Table 40-4	Display field descriptions for the mpls show hw-cam-tbl command	40-38
Table 40-5	Display field descriptions for the mpls show hw-ilm-err command	40-40
Table 40-6	Display field descriptions for the mpls show hw-ilm-tbl command	40-42
Table 40-7	Display field descriptions for the mpls show hw-ott-err command	40-44
Table 40-8	Display field descriptions for the mpls show hw-ott-tbl command	40-48
Table 40-9	Display field descriptions for the mpls show ilm-table command	40-51
Table 40-10	Display field descriptions for the mpls show interface command	40-53
Table 40-11	Display field descriptions for the mpls show interface command with label-map option	40-53
Table 40-12	Display field descriptions for the mpls show interface command with verbose option	40-54
Table 40-13	Display field descriptions for the mpls show l2-policy command	40-56
Table 40-14	Display field descriptions for the mpls show l2-policy command with verbose option	40-57
Table 40-15	Display field descriptions for the mpls show label-switched-paths command	40-60
Table 40-16	Display field descriptions for the mpls show label-switched-paths command with verbose option	40-60
Table 40-17	Display field descriptions for the mpls show ott-table command	40-63
Table 40-18	Display field descriptions for the mpls show paths command	40-64
Table 40-19	Display field descriptions for the mpls show policy command	40-66
Table 40-20	Display field descriptions for the mpls show policy command with verbose option	40-66
Table 40-21	Display field descriptions for the mpls show static-paths command	40-68
Table 40-22	Display field descriptions for the mpls show static-paths command with verbose option	40-69
Table 42-1	Display field descriptions for the multicast show interface command	42-3
Table 42-2	Display field descriptions for the multicast show mroutes command	42-5
Table 49-1	Ethernet Port Commands	49-2
Table 49-2	Gigabit Ethernet Port Commands	49-3
Table 49-3	ATM Port Commands	49-4
Table 49-4	Channelized E1 Port Commands	49-4
Table 49-5	Channelized T1 Port Commands	49-5
Table 49-6	Channelized T3 Port Commands	49-6
Table 49-7	Clear Channel E3 Port Commands	49-7
Table 49-8	Clear Channel T3 Port Commands	49-8
Table 49-9	CMTS Port Commands	49-9

Table 49-10	HSSI Port Commands	49-9
Table 49-11	Packet-over-SONET Port Commands.	49-10
Table 49-12	Serial Port Commands.	49-10
Table 49-13	Display Field Description	49-71
Table 49-14	Display Field Descriptions	49-88
Table 56-1	Display Field Descriptions for the rate-limit show all Command	56-16
Table 60-1	Maximum memory allocations for RMON.	60-37
Table 62-1	Display field descriptions for the rsvp show all command.	62-10
Table 62-2	Display field descriptions for the rsvp show global command.	62-11
Table 62-3	Display field descriptions for the rsvp show interface command.	62-14
Table 62-4	Display field descriptions for the rsvp show interface command with verbose option	62-14
Table 62-5	Display field descriptions for the rsvp show interface command with statistics option.	62-15
Table 62-6	Display field descriptions for the rsvp show neighbors command.	62-16
Table 62-7	Display field descriptions for the rsvp show session command	62-21
Table 64-1	Display field descriptions for the service show rate-limit aggregate command.	64-14
Table 64-2	Display field descriptions for the service show rate limit all command.	64-16
Table 64-3	Display field descriptions for the service show rate-limit burst-safe command.	64-17
Table 64-4	Display field descriptions for the service show rate-limit flow-aggregate command.	64-18
Table 64-5	Display field descriptions for the service show rate-limit per-flow command.	64-19
Table 68-1	Display Field Description	68-10
Table 68-2	Display Field Description	68-11
Table 68-3	Display Field Description	68-14
Table 68-4	Display Field Description	68-16
Table 68-5	Display Field Description	68-18
Table 81-1	Display field descriptions for the web-cache show all command.	81-19
Table 81-1	Display field descriptions for the web-cache show cache-name command	81-22
Table 81-1	Display field descriptions for the web-cache show servers command.	81-26
Table 81-1	Display field descriptions for the web-cache show statistics command	81-28
Table A-1	Ethernet applications.	A-1
Table A-2	IP (version 4) applications.	A-2
Table A-3	IPX applications	A-5
Table A-4	TCP applications.	A-6
Table A-5	UDP applications.	A-13

1 PREFACE

This manual provides reference information for the commands in the Riverstone Networks RS Switch Router Command Line Interface (CLI). For product information not available in this manual, see the manuals listed in [Section 1.2, "Related Documentation."](#)

1.1 HOW TO USE THIS MANUAL

The CLI commands and facilities are organized alphabetically in this manual. To locate information about a command, go to the chapter for the command or for the facility that contains the command. For example, to find information about the **interface add** command, go to the *interface Commands* chapter, then locate the description of the **interface add** command within that chapter.

1.2 RELATED DOCUMENTATION

The RS documentation set includes the following items. Refer to these other documents to learn more about your product.

Table 1-1 Related Documentation

For information about...	See the...
Installing and setting up the RS	<i>Riverstone Networks RS Switch Router Getting Started Guide</i>
How to use CLI (Command Line Interface) commands to configure and manage the RS	<i>Riverstone Networks RS Switch Router User Guide</i>
SYSLOG messages and SNMP traps	<i>Riverstone Networks RS Switch Router Message Reference Manual</i>

1.3 CLI PARAMETER TYPES

The following table describes all the parameter types you can use with the CLI.

Table 1-2 Parameter Types

Data Type	Description	Example
conditional	A numerical conditional expression. Special symbols are used to describe a numerical condition: > (greater than), < (less than) and != (not equal to).	<1024 or >2048 or !=4096
hexadecimal	A hexadecimal number	a7 or 0xa7
hostname	Hostname of an IP host	gauguin or john-pc
hostname/IP	Hostname or IP address of a host	nagasaki or 10.43.1.4
keyword	A keyword described in the list of acceptable keywords in the online help	on or off
interface name or IP address	Name of an interface or its IP address	int1 or 10.1.4.33
interface name list	A list of one or more interface names delimited by commas	int1 or int1,int2,int3
IP address	An IP address of the form x.x.x.x. Some commands may explicitly require a unicast or multicast address.	10.1.2.3
IP address/mask	A pair of IP address and mask values. Depending on the command, the mask may be a network mask or filtering mask. The mask can be described using the traditional IP address syntax (255.0.0.0) or a CIDR syntax (/8).	10.1.4.0/255.255.255.0 or 10.1.4.0/24
IP address list	A list of IP addresses separated by spaces but enclosed in quotes.	"10.1.4.4 10.1.5.5 10.1.6.6"
IPX network address	An IPX network address in hexadecimal	
IPX network.node address	An IPX network and node address of the form <netaddr>.<macaddr> where <netaddr> is the network address of a host and <macaddr> is the node or MAC address of the IPX host. For some commands, if the node address is not given, the node address is assumed to be a wildcard.	a1b2c3d4.0820a1:f3:38:11 or aa89f383

Table 1-2 Parameter Types

Data Type	Description	Example
IPX SAP server name	An alphanumeric string representing a valid IPX SAP server name where the following characters are illegal: “*./;<=>?[]\	server1
MAC address	A MAC address specified in one of two forms: xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx	08:00:50:1a:2b:c3 or 080050:1a2bc3
number	An integer number	100
numerical range	A number or a range of numbers	5 or 7-10
port	A single port	et.1.4, gi.2.1, hs.3.1.100, or se.4.2.200
port list	A list of one or more ports. To specify a range of ports within a module, describe the range in parenthesis. You can also specify non-consecutive ports by using commas to separate them. The wildcard character (*) can also be used to specify all modules or all ports within a module	et.1.(3-8) or et.1.(1,3,5), hs.(1-2).1.100, or se.4.(1-3).200, gi.2.*
slot number	A list of one or more occupied slots in the RS	1 or 7
string	A character string. To include spaces in a string, specify the entire string in double quotes (“”).	abc or “abc def”
URL	A Uniform Resource Locator. The type of URL depends on the command where the URL is used. Currently, two URLs are supported: TFTP: <i>tftp://host/pathname</i> RCP: <i>rcp://username@host/pathname</i>	tftp://10.1.4.5/test/abc.txt rcp://dave@rtr/test/abc.txt

1.4 <PORT-LIST> SYNTAX

The *<port-list>* parameter of the port set commands is a comma-separated list of ports to be configured. Wildcard or range sequences may be used as the last field of a port name. For example, when specifying a channel, the channel number may be a wildcard. However, when specifying a virtual circuit, the virtual circuit can be a wildcard or range, but a channel number must be explicitly specified.



Note Where appropriate, the keyword **all-ports** may also be used, if a command is to be applied to all the relevant ports.

The syntax for each *<port-list>* element is:

- For channelized ports:
`<port-type>.<slot>.<port>[:<channel-number>][.<vc>]`
- For other ports, including unchannelized T1/E1:
`<port-type>.<slot>.<port>[.<vc>]`

<port-type>

The type of interface being configured, which can be one of the types shown in [Table 1-3](#).

Table 1-3 Port Types

Port Type	Description
at	An Asynchronous Transfer Mode (ATM) interface.
cm	A Cable Modem Termination System (CMTS) interface.
e1	A G.703 European level-1 interface, with optional G.704/G.706 framing (Channelized E1).
e3	A G.703 European level-3 interface, with optional G.751 framing. (Clear Channel E3).
et	An Ethernet interface.
gi	A Gigabit Ethernet interface.
hs	A HSSI interface.
se	A Serial interface.
so	A Packet Over SONET (POS) interface.
t1	A DS-1 or DSX-1 interface, as specified in ANSI T1.403/T1.408, and so on (Channelized T1).
t3	A DS-3 interface, as specified in ANSI-T1.404 (Channelized T3 or Clear Channel T3).

You can create pseudo devices, with port types shown in [Table 1-4](#).

Table 1-4 Pseudo Device Port Types

Port Type	Description
mp	A Multilink PPP Bundle.
st	A SmartTRUNK.

<slot>

The number of the slot in the router chassis containing the device, or the number of the pseudo device.

<port>

The number of the port to be configured. The range of ports for each port type is shown in [Table 1-5](#).

Table 1-5 Port Ranges for Various Port Types

Port Type	Port Range
ATM	1 to 2
Channelized T1 or Channelized E1	1 to 4
Channelized T3	RS 16000, RS 32000 and RS 38000: 1 to 4 Other systems 1 to 2
Clear Channel T3 or Clear Channel E3	1 or 3
CMTS	1 to 4
Ethernet	1 to 8 or 1 to 16
Gigabit Ethernet	RS 16000, RS 32000 and RS38000: 1 to 4 or 1 to 8 Other systems: 1 to 2
HSSI	1 to 2
POS OC-3c	1 to 4
POS OC-12c	1 to 2
Serial	1 to 4

You can specify a range of ports, for example, t1.3.1-4. Also, you can specify ports as a comma-separated list by entering the list in parentheses. For example, e1.1.(1-4,6).

<channel-number>

Available only for Channelized T1, E1 and T3 interfaces. For Channelized T1 and E1, and fractional T1 and E1 interfaces, a channel is a group of timeslots. For Channelized T3 interfaces, a channel is a T1 line.

The *channel-number* is a logical channel number. For T1 and E1 interfaces, this does not correspond to a physical time-slot on the interface. For T3 interfaces, the logical channel number corresponds to the physical time-slot. The maximum number of logical channels on any one interface is limited by the number of usable time-slots (T1 and E1) or TDM frames (T3). The lowest legal channel number is '1'.

The range of values depends on the interface you are configuring, as shown in [Table 1-6](#).

Table 1-6 Channel Ranges for Channelized T1, E1 and T3 Ports

Port Type	Channel Range
Channelized T1	1 to 24
Channelized E1	1 to 31
Channelized T3	1 to 28

You can specify a single channel number, a comma-separated list of channel numbers, or a range of channel numbers. For a channel range, you must specify a *start-channel* and an *end-channel*; the *end-channel* must be a value greater than that specified for the *start-channel*. See “<port-list> Examples” for examples.

For other port types, including unchannelized T1 and E1 (that is, where port framing is set to **none**), omit <channel-number> and the preceding colon (:). However, the <vc> parameter is still permitted.

<vc>

A virtual channel (VC) number for a Frame Relay interface.

<port-list> Examples

```
at.2.1
cm.1.2
et.1.4
gi.2.1
hs.3.1.100
se.4.2.200
so.3.1
e1.2.1:1
e1.3.3-4:*
e1.2-3.(1,3-4):*
t1.3.2:4-8
t1.3.2:(2,4-8)
t1.3.1:*
t3.4.1:1.100
t3.4.1:2.*
```

1.5 USE OF WAN-ENCAPSULATION

Certain port commands require that you also include **wan-encapsulation frame-relay|ppp|cisco-hdlc** as part of the same command. The port commands where you must include this are:

For HSSI and Serial ports

See “[port set](#)” on page 30 command for non-channelized interfaces:

```
port set <port-list>|all-ports [...] wan-encapsulation frame-relay|ppp|cisco-hdlc
```

For Channelized T1, E1 and T3 ports

See “[port set framing](#)” on page 42 for Channelized T1 and E1:

```
port set <port-list> framing none wan-encapsulation frame-relay|ppp|cisco-hdlc
```

See “[port set timeslots](#)” on page 58 for Channelized T1, E1 and T3:

```
port set <port-list> timeslots <start-slot>[-<end-slot>] wan-encapsulation frame-relay|ppp|cisco-hdlc
```

See “[port set ts16](#)” on page 60 for Channelized E1:

```
port set <port-list> ts16 wan-encapsulation frame-relay|ppp|cisco-hdlc
```

For Clear Channel T3 and E3 ports

For the Clear Channel T3 and E3 commands, **wan-encapsulation** is optional. However, you must specify **wan-encapsulation** with one of the commands (see [Table 49-7](#) and [Table 49-8](#)), for example:

```
port set t3.2.3 framing m23 wan-encapsulation ppp
port set t3.2.3 cablelength 100
port set t3.2.3 scrambling-mode enable
```


2 ACL COMMANDS

The `acl` commands allow you to create ACLs (Access Control Lists) and apply them to IP and IPX interfaces on the RS. An ACL permits or denies switching of packets based on criteria such as the packet's source address and destination address, TCP or UDP port number, and so on. When you apply an ACL to an interface, you can specify whether the ACL affects incoming traffic or outgoing traffic. You also can enable a log of the ACL's use.

2.1 COMMAND SUMMARY

The following table lists the ACL commands. The sections following the table describe the command syntax.

<code>acl <name> apply interface <InterfaceName> input output [logging on off deny-only permit-only][policy local external]</code>
<code>acl <name> apply port <port list> input output [logging [on off] [policy local external]</code>
<code>acl <name> apply service <ServiceName> [logging [on off]]</code>
<code>acl <name> clearCounters aclname all interface service port</code>
<code>acl <name> permit deny icmp <SrcAddr/Mask> <DstAddr/Mask> [log]</code>
<code>acl <name> permit deny igmp <SrcAddr/Mask> <DstIP/mask> [log]</code>
<code>acl <name> permit deny ip <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> [accounting 5-minutes 15-minutes hourly] [log]</code>
<code>acl <name> permit deny ip-protocol <proto-num> <SrcAddr/Mask> <DstAddr/Mask> <tos> <tos-mask> [log]</code>
<code>acl <name> permit deny ipx <SrcAddr> <SrcSocket> <DstAddr> <DstSocket> <SrcNetMask> <DstNetMask></code>
<code>acl <name> permit deny ipxgns <ServerAddr> <ServiceType> <ServiceName></code>
<code>acl <name> permit deny ipxrip <FromNetwork> <ToNetwork></code>
<code>acl <name> permit deny ipxsap <ServerAddr> <ServiceType> <ServiceName></code>
<code>acl <name> permit deny ipxtype20</code>
<code>acl <name> permit deny tcp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask> [accounting 5-minutes 15-minutes hourly] [established] [log]</code>

<code>acl <name> permit deny udp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask> [accounting 5-minutes 15-minutes hourly] [log]</code>
<code>acl-policy enable external policy-routing-external</code>
<code>acl show [aclname <string> all] [interface <string> all-ip] [service] [port<port list> all-ports] [all]</code>

acl apply interface

Mode

Configure

Format

```
acl <name> apply interface <InterfaceName> input|output [logging  
on|off|deny-only|permit-only] [policy local|external]
```

Description

The **acl apply interface** command applies a previously defined ACL to an interface. When you apply an ACL to an interface, you implicitly enable access control on that interface. You can apply an ACL to filter out inbound traffic, outbound traffic, or both inbound and outbound traffic. Inbound traffic is packets coming into the interface while outbound traffic is packets going out of that interface.

When you apply an ACL, you also can enable ACL Logging by using the **logging** keyword. When you enable ACL Logging on an interface, the RS displays ACL Logging messages on the console. The ACL log provides information such as the interface name, the ACL name, whether the packet is forwarded or not, and the internal details of the packet.

You can also specify if the ACL is allowed to be modified or removed from the interface by an external agent (such as a policy manager application) by using the **policy** keyword. If you do not specify the **policy** keyword, an external agent is allowed to modify or remove the applied ACL. Note that the **acl-policy enable external** command must be in the configuration before an external agent can modify or remove an applied ACL.

Parameter	Value	Meaning
acl	<name>	Name of the ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter.
interface	<InterfaceName>	Name of the interface to which you are applying the ACL.
input		Applies the ACL to filter out inbound traffic.
output		Applies the ACL to filter out outbound traffic.
logging		Enables or disables ACL logging for this interface. You can specify one of the following keywords:
	off	Disables all logging.
	on	Enables logging of packets that are dropped or forwarded because of any ACL policy applied on that interface.
	deny-only	Enables logging of dropped packets only.
	permit-only	Enables logging of forwarded packets only.
policy		Allows or prevents an external agent from modifying or removing the applied ACL. You can specify one of the following keywords:

Parameter	Value	Meaning
	local	External agent cannot modify or remove the applied ACL.
	external	External agent can modify or remove the applied ACL. This is the default.

Restrictions

You can apply only one ACL of each type (IP or IPX) to an interface at one time. For example, although you can define two ACLs, “ipacl1” and “ipacl2”, you cannot apply them both to the same interface.

However, you can apply two ACLs to the same interface if one is for inbound traffic and one is for outbound traffic, but not in the same direction. This restriction does not prevent you from specifying many rules in an ACL. You just have to put all of these rules into one ACL and apply it to an interface.

You can apply IP ACLs only to IP interfaces. Likewise, you can apply IPX ACLs only to IPX interfaces.

Examples

To apply ACL “100” to interface *int4* to filter out inbound traffic:

```
rs (config)# acl 100 apply interface int4 input
```

To apply ACL “nonfs” to interface *int16* to filter out outbound traffic and enable logging:

```
rs(config)# acl nonfs apply interface int16 output logging on
```

acl apply port

Mode

Configure

Format

```
acl <name> apply port <port list> input|output [logging on|off] [policy local| external]
```

Description

The **acl apply port** applies a previously defined ACL to one or more ports. This command only applies to ports operating in Layer 4 bridging mode. The ACLs that are applied to a Layer 4 bridging port are only used with bridged traffic. Routed traffic is still subject to the ACLs that are attached to the interface.

Parameter	Value	Meaning
acl	<name>	Name of the ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter.
port	<port list>	Specifies the port(s) in the Layer-4 bridging VLAN to which you are applying the ACL.
input		Applies the ACL to filter out inbound traffic.
output		Applies the ACL to filter out outbound traffic.
logging		Enables or disables ACL logging for this port. You can specify one of the following keywords:
	off	Disables all logging.
	on	Enables logging of packets that are dropped or forwarded because of ACL.
policy		Allows or prevents an external agent from modifying or removing the applied ACL. You can specify one of the following keywords:
	local	External agent cannot modify or remove the applied ACL.
	external	External agent can modify or remove the applied ACL. This is the default.

Restrictions

The line cards that contain the specified ports must support Layer 4 bridging. The RS software checks the line card(s) and displays an error message if new line card(s) are necessary.

Examples

To apply ACL “l4” to slot 1, gigabit port 3 and slot 3, 10/100 port 6 for inbound traffic:

```
rs(config)# acl l4 apply port gi.1.2 et.3.6 input
```

To apply ACL “l4out” to slot 5, all ports for outbound traffic and enable logging:

```
rs(config)# acl l4out apply port et.5.* output logging on
```

acl apply service

Mode

Configure

Format

```
acl <name> apply service <ServiceName> [logging [on|off]]
```

Description

The **acl apply service** command applies a previously defined ACL to a service provided by the RS. A service is typically a server or agent running on the RS, for example, a Telnet server or SNMP agent. By applying an ACL to a service, you can control which host can access individual services on the RS. This type of ACL is known as a Service ACL. It does not control packets going *through* the RS. It only controls packets that are *destined* for the RS, specifically, one of the services provided by the RS. As a result, a Service ACL, by definition, is applied only to check for inbound traffic to the RS. The destination host of a Service ACL is by definition the RS. The destination port is the well-known port of the service.

When you apply an ACL, you also can enable ACL Logging by using the **logging** keyword. When you enable ACL Logging on an interface, the RS displays ACL Logging messages on the console. The ACL log provides information such as the interface name, the ACL name, whether the packet is forwarded or not, and the internal details of the packet.

In addition, you may apply an ACL to a service on a per-interface basis, based on the destination address defined by the ACL.

Parameter	Values	Meaning
acl	<name>	Name of the Service ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter.
service	<ServiceName>	Name of the service on the RS to which you are applying the ACL. Currently, the following services are supported:
	http	HTTP web server
	snmp	SNMP agent
	telnet	Telnet server
[logging]		Enables or disables ACL logging for this interface. You can specify one of the following keywords:
	off	Disables logging.
	on	Enables logging.

Restrictions

You can apply only one ACL of each type (IP or IPX) to a service at one time. For example, although you can define two ACLs, “ipacl1” and “ipacl2”, you cannot apply them both to the same service.

Examples

To permit access to the SNMP agent only from the host 10.4.3.33 (presumably an SNMP management station):

```
rs(config)# acl 100 permit udp 10.4.3.33
rs(config)# acl 100 apply service snmp
```

The following commands permit access to the Telnet server from hosts on the subnet 10.4.7.0/24 with a privileged source port. In addition, with logging enabled, all incoming Telnet accesses are logged to the console.

```
rs(config)# acl 120 permit tcp 10.4.7.0/24 <1024
rs(config)# acl 120 apply service telnet logging on
```

The following commands permit access to the HTTP web server from subnet 10.12.4.0/24. Notice that even though the destination address and port are specified for this ACL (*10.12.7.44* and *any* port), they are ignored. This service ACL will match only packets destined for the RS itself and the well-known port of the service (port 80 for HTTP).

```
rs(config)# acl 140 permit ip 10.12.4.0/24 any 10.12.7.44 any
rs(config)# acl 120 apply service http
```

acl clearCounters

Mode
Configure

Format

acl clearCounters aclname <string> | all | interface | service | port

Description

The **acl clearCounters** commands allows you to clear ACL counters. With ACL logging enabled, the router prints out a message about whether a packet is forwarded or dropped and counters keep track of these statistics. With this command, you can clear these ACL counters.

Parameter	Value	Meaning
aclname	<string>	Clears the counter based on the name of the ACL. Specify all to clear all ACLs.
all		Clears all ACL counters.
interface	<string>	Clears ACL counters attached to specific interfaces. Specify all-ip to clear all counters with IP interfaces.
service		Clears ACL counters that are applied to services.
port	<port list>	Clears ACL counters on specific ports. Specify all-ports to clear counters on all ports.

Restrictions

None

Examples

To clear the ACL counters for ACL ‘engacl’:

```
rs(config)# acl clearCounters aclname engacl
```

acl permit|deny icmp

Mode

Configure

Format

```
acl <name> permit|deny icmp <SrcAddr/Mask> <DstAddr/Mask> <tos> log
```

Description

The **acl permit icmp** and **acl deny icmp** commands define an ACL to allow or block ICMP traffic from entering or leaving the RS. For each of the values describing a flow, you can use the keyword *any* to specify a *wildcard* (“don’t care”) condition. If you do not specify a value for a field, the RS applies a wildcard condition to the field, giving the same effect as if you specify the *any* keyword.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
icmp		Defines an ACL for ICMP.
	<SrcAddr/Mask>	The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).
	<DstAddr/Mask>	The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.
	<tos>	IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.
log		This optional parameter allows you to enable ACL logging for this specific ACL rule. Note that logging must be turned off in the acl apply command for logging to occur only on this specific ACL rule. This is because turning logging on for the acl apply command enables logging for all ACL rules applied on the interface.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To deny ICMP traffic from the subnet 10.24.5.0 (with a 24 bit netmask) to any destination:

```
rs(config)# acl 310 deny icmp 10.24.5.0/24 any
```

To create an ACL to permit ICMP traffic from the host 10.12.28.44 to subnet 10.43.21.0:

```
rs(config)# acl 312 permit icmp 10.12.28.44 10.43.21.0/24
```

acl permit|deny igmp

Mode

Configure

Format

```
acl <name> permit|deny igmp <SrcAddr/Mask> <DstAddr/Mask> <tos> log
```

Description

The **acl permit igmp** and **acl deny igmp** commands define an ACL to allow or block IGMP traffic from entering or leaving the RS. For each of the values describing a flow, you can use the keyword *any* to specify a *wildcard* (“don’t care”) condition. If you do not specify a value for a field, the RS applies a wildcard condition to the field, giving the same effect as if you specify the *any* keyword.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
igmp		Defines an ACL for IGMP.
	<SrcAddr/Mask>	The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).
	<DstAddr/Mask>	The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.
	<tos>	IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.
log		This optional parameter allows you to enable ACL logging for this specific ACL rule. Note that logging must be turned off in the acl apply command for logging to occur only on this specific ACL rule. This is because turning logging on for the acl apply command enables logging for all ACL rules applied on the interface.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create an ACL to deny IGMP traffic from the subnet 10.1.5.0 (with a 24 bit netmask) to any destination:

```
rs(config)# acl 410 deny igmp 10.1.5.0/24 any
```

To create an ACL to permit IGMP traffic from the host 10.33.34.44 to subnet 10.11.21.0:

```
rs(config)# acl 714 permit igmp 10.33.34.44 10.11.21.0/24
```

acl permit|deny ip

Mode

Configure

Format

```
acl <name> permit|deny ip <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
any [accounting 5-minutes|15-minutes|hourly] log
```

Description

The **acl permit ip** and **acl deny ip** commands define an Access Control List to allow or block IP traffic from entering or leaving the router. Unlike the more specific variants of the **acl** commands for TCP and UDP, the IP version of the command includes IP-based protocols such as TCP, UDP, ICMP and IGMP. For each of the values describing a flow, you can use the keyword **any** to specify a *wildcard* (“don’t care”) condition. If you do not specify a value for a field, the RS assumes that the value is a wildcard (as if you had specified the **any** keyword). The two exceptions to this rule are the optional parameters **<tos>** (type of service) and **accounting**. **<tos>** is a value from 0 to 15. The **accounting** keyword is only valid for the **permit** command, can be placed anywhere on the command line, and must be followed by a *checkpoint* time interval. When you specify the **accounting** keyword, LFAP accounting information will be sent to the configured server for flows that match the ACL.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number. The string must be less than 100 characters.
ip		Defines an ACL for IP.
	<SrcAddr/Mask>	The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).
	<DstAddr/Mask>	The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.

Parameter	Value	Meaning
	<SrcPort>	For TCP or UDP, the number of the source TCP or UDP port. This field applies only to TCP or UDP traffic. If the incoming packet is ICMP or another non-TCP or non-UDP packet and you specified a source or destination port, the RS does not check the port value. The RS checks only the source and destination IP addresses in the packet. You can specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024). The port numbers of some popular services are already defined as keywords. For example, for Telnet, you can enter the port number 23 as well as the keyword <code>telnet</code>.
	<DstPort>	For TCP or UDP, the number of the destination TCP or UDP port. This field applies only to incoming TCP or UDP traffic. The same requirements and restrictions for <SrcPort> apply to <DstPort>.
	<tos>	IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.
	<tos-mask>	Mask value used for the TOS byte. You can specify a mask value from 0–255. Default is 30 . Specify any for any TOS value.
accounting		Valid with the permit command only. This optional parameter causes LFAP accounting information to be sent to the configured server for flows that match the ACL. The accounting option must be followed by one of the following <i>checkpoint</i> time periods.
	5-minutes	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every 5 minutes. You must specify the accounting parameter with this.
	15-minutes	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every 15 minutes. You must specify the accounting parameter with this.
	hourly	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every hour. You must specify the accounting parameter with this.
log		This optional parameter allows you to enable ACL logging for this specific ACL rule. Note that logging must be turned off in the acl apply command for logging to occur only on this specific ACL rule. This is because turning logging on for the acl apply command enables logging for all ACL rules applied on the interface.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create an ACL to permit IP traffic from the subnet 10.1.0.0 (with a 16 bit netmask) to any destination:

```
rs(config)# acl 100 permit ip 10.1.0.0/16 any
```

The following command creates an ACL to deny any incoming TCP or UDP traffic coming from a privileged port (less than 1024). If the incoming traffic is not TCP or UDP, then the RS check only the source and destination addresses, not the port number. Therefore, this ACL will deny all non-TCP and non-UDP traffic.

```
rs(config)# acl 120 deny ip any any 1-1024 any
```

To create an ACL to permit Telnet traffic (port 23) from the host 10.23.4.8 to the subnet 10.2.3.0:

```
rs(config)# acl 130 permit ip 10.23.4.8 10.2.3.0/24
```

The following command creates an ACL to permit all IP traffic. Since none of the ACL fields are specified, they are all assumed to be wildcards.

```
rs(config)# acl allip permit ip
```

The above command is equivalent to the following:

```
rs(config)# acl allip permit ip any any any any any
```

acl permit|deny ip-protocol

Mode

Configure

Format

```
acl <name> permit|deny ip-protocol <proto-num> <SrcAddr/Mask> <DstAddr/Mask> <tos> log
```

Description

The **acl permit ip-protocol** and **acl deny ip-protocol** commands define an Access Control List to allow or block IP traffic from entering or leaving the router for any protocol type. Unlike the more specific variants of the acl commands such as **ip**, **tcp** and **udp**, the **ip-protocol** version of the command allows the user to specify any valid IP protocol type. This command allows the user to specify an IP protocol other than the ones available with other **acl permit|deny** commands. For example, to specify an ACL for IP encapsulation in IP, one can use the IPinIP protocol type, 4, in the ACL. For each of the values describing a flow, you can use the keyword **any** to specify a *wildcard* (“don’t care”) condition. If you do not specify a value for a field, the RS assumes that the value is a wildcard (as if you had specified the any keyword).

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
ip-protocol		Defines an ACL for IP-Protocol ‘n’.
	<proto-num>	IP protocol number of this flow.
	<SrcAddr/Mask>	The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).
	<DstAddr/Mask>	The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.
	<tos>	IP TOS (Type of Service) value. You can specify a TOS from 0 – 255.
log		This optional parameter allows you to enable ACL logging for this specific ACL rule. Note that logging must be turned off in the acl apply command for logging to occur only on this specific ACL rule. This is because turning logging on for the acl apply command enables logging for all ACL rules applied on the interface.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create an ACL to permit VRRP traffic (IP protocol type 112) from the subnet 10.14.0.0 (with a 16 bit netmask) to any destination:

```
rs(config)# acl 100 permit ip-protocol 112 10.14.0.0/16 any
```

The following command has the same function as **acl 120 deny igmp** since the protocol type for IGMP is 2.

```
rs(config)# acl 120 deny ip-protocol 2
```


acl permit|deny ipx

Mode

Configure

Format

```
acl <name> permit|deny ipx <SrcAddr> <SrcSocket> <DstAddr> <DstSocket> <SrcNetMask>
<DstNetMask>
```

Description

The **acl permit ipx** and **acl deny ipx** commands define an ACL to allow or block IPX traffic from entering or leaving the RS.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
ipx		Defines an ACL for IPX.
	<SrcAddr>	The source IPX address in <network> . <node> format, where <network> is the network address and <node> is the MAC address. The RS will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword any to specify a wildcard (“don’t care”) condition. To specify any network, enter FFFFFFFF.<node> ; to specify any node, enter <network>. FF:FF:FF:FF:FF:FF .
	<SrcSocket>	Source IPX socket. The RS will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword any to specify a wildcard (“don’t care”) condition.
	<DstAddr>	The destination IPX address in <network> . <node> format. The syntax for the destination address is the same as the syntax for the source address <SrcAddr>. The RS will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword any to specify a wildcard (“don’t care”) condition.
	<DstSocket>	Destination IPX socket. The RS will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword any to specify a wildcard (“don’t care”) condition.

Parameter	Value	Meaning
	<i><SrcNetmask></i>	Source network mask. This field specifies a group of networks for which the ACL applies. This mask field is ANDed with the network portion of <i><SrcAddr></i> and the source network of the incoming packets to determine a hit. The RS will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. This is an optional argument and if you omit the argument, the RS uses the hexadecimal value FFFFFFFF.
	<i><DstNetmask></i>	Destination network mask. This field specifies a group of networks for which the ACL applies. This mask field is ANDed with the network portion of <i><DstAddr></i> and the destination network of the incoming packets to determine a hit. The RS will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. This is an optional argument and if you omit the argument, the RS uses the hexadecimal value FFFFFFFF.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

The following command creates an ACL to permit IPX traffic from the host with IPX address **AAAAAAAA.01:20:0A:F3:24:6D**, any socket, to any other IPX address (network.node), any socket.

```
rs(config)# acl 100 permit ipx AAAAAAAAA.01:20:0A:F3:24:6D any any any
```

The following command creates an ACL to deny IPX traffic from the host with IPX address **F6D5E4.01:20:0A:F3:24:6D**, with socket address 451, to any other IPX address (network.node), any socket.

```
rs(config)# acl 200 deny ipx F6D5E4.01:20:0A:F3:24:6D 451 any any
```

acl permit|deny ipxgn

Mode

Configure

Format

```
acl <name> permit|deny ipxgns <ServerAddr> <ServiceType> <ServiceName>
```

Description

The **acl permit ipxgns** and **acl deny ipxgns** commands define an ACL to allow or block replying to GNS requests.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
ipxgns		Defines an ACL for IPX Get Nearest Server.
	<ServerAddr>	The SAP server's IPX address in <network> . <node> format, where <network> is the network address and <node> is the MAC address. You can use the keyword any to specify a wildcard ("don't care") condition.
	<ServiceType>	The SAP service type. Express the service type in hexadecimal. You do not need to use a "0x" prefix. You can use the keyword any to specify a wildcard ("don't care") condition.
	<ServiceName>	The SAP service name. This is an optional argument and if you omit the argument, the RS applies a wildcard condition to the field.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic. You can only apply the **acl permit ipxgns** and **acl deny ipxgns** commands to output.

Examples

To create a GNS ACL to permit the RS to reply with the server "FILESERVER", whose IPX address is F6D5E4.01:20:0A:F3:24:5D, to get nearest server requests:

```
rs(config)# acl 100 permit ipxgns F6D5E4.01:20:0A:F3:24:5D 0004
FILESERVER
```

To create a GNS ACL to prevent the RS from replying with the server “ARCHIVESERVER”, whose IPX address is F6D5E4.01:20:0A:F3:24:5C, to a get nearest server request:

```
rs(config)# acl 200 deny ipxgns F6D5E4.01:20:0A:F3:24:5C 0009  
ARCHIVESERVER
```

acl permit|deny ipxrip

Mode

Configure

Format

```
acl <name> permit|deny ipxrip <FromNetwork> <ToNetwork>
```

Description

The **acl permit ipxrip** and **acl deny ipxrip** commands define an ACL to allow or block IPX RIP traffic from entering or leaving the RS.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
ipxrip		Defines an ACL for IPX RIP.
	<FromNetwork>	The “from” IPX network address. You can use the any keyword to specify a wildcard condition. If you use any, the RS uses the value 0 for <FromNetwork> and FFFFFFFE for <ToNetwork>.
	<ToNetwork>	The “to” IPX network address. This is an optional parameter. If you omit this parameter, the value that the RS assumes depends on whether you specified any for <FromNetwork>. If you omit the <ToNetwork> value and you used the value any for <FromNetwork>, the RS sets the <ToNetwork> to FFFFFFFE . If you omit the <ToNetwork> value but do not use the value any for <FromNetwork>, the RS sets <ToNetwork> to the same value you specified for <FromNetwork>.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create an ACL to permit IPX RIP traffic from networks AA000001 to AFFFFFFF:

```
rs(config)# acl 100 permit ipxrip AA000001 AFFFFFFF
```

acl permit|deny ipxsap

Mode

Configure

Format

```
acl <name> permit|deny ipxsap <ServerAddr> <ServiceType> <ServiceName>
```

Description

The **acl permit ipxsap** and **acl deny ipxsap** commands define an ACL to allow or block IPX SAP traffic from entering or leaving the RS.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
ipxsap		Defines an ACL for IPX SAP.
	<ServerAddr>	The SAP server’s IPX address in <network> . <node> format, where <network> is the network address and <node> is the MAC address. You can use the keyword any to specify a wildcard (“don’t care”) condition. To specify any network, enter FFFFFFFF .<node>; to specify any node, enter <network>. FF:FF:FF:FF:FF:FF .
	<ServiceType>	The SAP service type. Express the service type in hexadecimal. You do not need to use a “0x” prefix. You can use the keyword any to specify a wildcard (“don’t care”) condition.
	<ServiceName>	The SAP service name. This is an optional argument and if you omit the argument, the RS applies a wildcard condition to the field.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create a SAP ACL to permit SAP information related to the server “FILESERVER” whose IPX address is **F6D5E4.01:20:0A:F3:24:5D**:

```
rs(config)# acl 100 permit ipxsap F6D5E4.01:20:0A:F3:24:5D 0004
FILESERVER
```

To create a SAP ACL to deny SAP information related to the server “ARCHIVESERVER” whose IPX address is **F6D5E4.01:20:0A:F3:24:5C**:

```
rs(config)# acl 200 deny ipxsap F6D5E4.01:20:0A:F3:24:5C 0009  
ARCHIVESERVER
```

acl permit|deny ipxtype20

Mode
Configure

Format

acl <name> permit|deny ipxtype20

Description

The **acl permit ipxtype20** and **acl deny ipxtype20** commands define an ACL to allow or block IPX type 20 packets from entering or leaving the RS.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
ipxtype20		Defines a Type 20 ACL for IPX.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create an ACL to deny IPX type 20 packets:

```
rs(config)# acl 100 deny ipxtype20
```


acl permit|deny tcp

Mode

Configure

Format

```
acl <name> permit|deny tcp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
[accounting 5-minutes|15-minutes|hourly] [established] [log]
```

Description

The **acl permit tcp** and **acl deny tcp** commands define an ACL to allow or block TCP traffic from entering or leaving the RS. For each of the values describing a flow, you can use the keyword **any** to specify a *wildcard* (“don’t care”) condition. If you do not specify a value for a field, the RS applies a wildcard condition to the field, giving the same effect as if you specify the **any** keyword. The two exceptions to this rule are the optional parameters **<tos>** (type of service) and **accounting**. **<tos>** is a value from 0 to 15. The **accounting** keyword is only valid for the **permit** command, can be placed anywhere on the command line, and must be followed by a *checkpoint* time interval. When you specify the **accounting** keyword, LFAP accounting information will be sent to the configured server for flows that match the ACL.

Parameter	Value	Meaning
acl	<name>	Is the name of this ACL. You can use a string of characters or a number.
tcp		Defines an ACL for TCP.
	<SrcAddr/Mask>	Is the source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).
	<DstAddr/Mask>	Is the destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.
	<SrcPort>	For TCP or UDP, is the number of the source TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> You can specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024). The port numbers of some popular services are already defined as keywords. For example, for Telnet, you can enter the port number 23 as well as the keyword <code>telnet</code> .
	<DstPort>	For TCP or UDP, is the number of the destination TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> The same requirements and restrictions for <SrcPort> apply to <DstPort>.

Parameter	Value	Meaning
	<tos>	Is the IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.
	<tos-mask>	Mask value used for the TOS byte. You can specify a mask value from 0–255. Default is 30 . Specify any for any TOS value.
accounting		Is valid with the permit command only. This keyword causes LFAP accounting information to be sent to the configured server for flows that match the ACL. The accounting option must be followed by one of the following <i>checkpoint</i> time periods.
	5-minutes	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every 5 minutes. You must specify the accounting parameter with this.
	15-minutes	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every 15 minutes. You must specify the accounting parameter with this.
	hourly	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every hour. You must specify the accounting parameter with this.
established		Allows TCP responses from external hosts, provided the connection was established internally.
log		This optional parameter allows you to enable ACL logging for this specific ACL rule. Note that logging must be turned off in the acl apply command for logging to occur only on this specific ACL rule. This is because turning logging on for the acl apply command enables logging for all ACL rules applied on the interface.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

To create an ACL to permit TCP traffic from the subnet 10.21.33.0 (with a 24 bit netmask) to any destination:

```
rs(config)# acl 100 permit tcp 10.21.33.0/255.255.255.0 any
```

To create an ACL to deny any incoming HTTP traffic:

```
rs(config)# acl noweb deny tcp any any http any
```

To create an ACL to permit FTP traffic (both command and data ports) from subnet **10.31.34.0** to **10.31.60.0**:

```
rs(config)# acl ftp100 permit tcp 10.31.34.0/24 10.31.60.0/24 20-21 any
```

acl permit|deny udp

Mode

Configure

Format

```
acl <name> permit|deny udp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
[accounting 5-minutes|15-minutes|hourly] [log]
```

Description

The **acl permit udp** and **acl deny udp** commands define an ACL to allow or block UDP traffic from entering or leaving the RS. For each of the values describing a flow, you can use the keyword **any** to specify a *wildcard* (“don’t care”) condition. If you do not specify a value for a field, the RS applies a wildcard condition to the field, giving the same effect as if you specify the **any** keyword. The two exceptions to this rule are the optional parameters **<tos>** (type of service) and **accounting**. **<tos>** is a value from 0 to 15. The **accounting** keyword is only valid for the **permit** command, can be placed anywhere on the command line, and must be followed by a *checkpoint* time interval. When you specify the **accounting** keyword, LFAP accounting information will be sent to the configured server for flows that match the ACL.

Parameter	Value	Meaning
acl	<name>	Name of this ACL. You can use a string of characters or a number.
udp		Defines an ACL for UDP.
	<SrcAddr/Mask>	The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).
	<DstAddr/Mask>	The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.
	<SrcPort>	For TCP or UDP, the number of the source TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> You can specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024). The port numbers of some popular services are already defined as keywords. For example, for Telnet, you can enter the port number 23 as well as the keyword <code>telnet</code> .
	<DstPort>	For TCP or UDP, the number of the destination TCP or UDP port. This field applies only to incoming TCP or UDP traffic. The same requirements and restrictions for <SrcPort> apply to <DstPort>.

Parameter	Value	Meaning
	<tos>	IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.
	<tos-mask>	Mask value used for the TOS byte. You can specify a mask value from 0– 255. Default is 30. Specify any for any TOS value.
accounting		Valid with the permit command only. This keyword causes LFAP accounting information to be sent to the configured server for flows that match the ACL. The accounting option must be followed by one of the following <i>checkpoint</i> time periods.
	5-minutes	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every 5 minutes. You must specify the accounting parameter with this.
	15-minutes	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every 15 minutes. You must specify the accounting parameter with this.
	hourly	Valid with the permit command only. This parameter causes LFAP accounting information to be sent every hour. You must specify the accounting parameter with this.
log		This optional parameter allows you to enable ACL logging for this specific ACL rule. Note that logging must be turned off in the acl apply command for logging to occur only on this specific ACL rule. This is because turning logging on for the acl apply command enables logging for all ACL rules applied on the interface.

Restrictions

When you apply an ACL to an interface, the RS appends an implicit deny rule to that ACL. The implicit deny rule denies all traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must explicitly define a rule to permit all traffic.

Examples

Here are some examples of ACL commands for permitting and denying UDP traffic flows.

```
rs(config)# acl 100 permit udp 10.1.3.0/24 any
```

Creates an ACL to permit UDP traffic from the subnet **10.1.3.0** (with a 24 bit netmask) to any destination.

```
rs(config)# acl notftp deny udp any any tftp any
```

Creates an ACL to deny any incoming TFTP traffic.

```
rs(config)# acl udpnfs permit udp 10.12.0.0/16 10.7.0.0/16 any nfs
```

Creates an ACL to permit UDP based NFS traffic from subnet **10.12.0.0** to subnet **10.7.0.0**.

acl-policy enable external

Mode

Configure

Format

```
acl-policy enable external| policy-routing-external
```

Description

The **acl-policy enable** command allows ACLs to be configured by an external agent, such as the Policy Manager. If this command is in the active configuration, an external server can create, modify, and delete ACLs on the RS. If this command is not in the active configuration, then ACLs can only be created, modified, and deleted using the CLI.

Parameter	Value	Meaning
external		Enables ACLs to be configured by an external agent such as the Policy Manager.
policy-routing-external		Enables policy routing to be configured by an external agent such as the Policy Manager.

Restrictions

The only action allowed by the **acl-policy enable external** command is to allow an external server to create, modify, and delete ACLs. Once entered, this command must be negated in order to prohibit an external server from creating, altering, or deleting ACLs. An external server can only modify ACLs that it created, or ACLs that were created using the CLI with the “external” flag. It cannot modify an ACL that was created using the CLI with the “local” flag.

acl show

Mode
Enable

Format

```
acl show [aclname <string>|all] | [interface <string>|all-ip] | [service] | [port <port list>|all-ports] | [all]
```

Description

The **acl show** command allows you to display the ACLs currently configured. Using the parameters associated with this command allows you to sort and display the ACLs by the name, interface, port, or service type.

Parameter	Value	Meaning
aclname		Use this parameter to display ACLs by name.
	<string>	The name of the ACL.
	all	Specify all to display all ACLs.
interface		
	<string>	The name of the interface.
	all-ip	Specify all to display ACLs attached to all IP interfaces.
service		Use this parameter to display ACLs applied to services.
port		Use this parameter to display ACLs applied to a specified port(s).
	<port list>	The list of port(s) or SmartTRUNK(s)
	all-ports	Specify all to display ACLs applied to all ports.
	all	Use this parameter to display all ACLs.

Restrictions

None.

3 ACL-EDIT COMMANDS

The **acl-edit** command activates the ACL Editor mode. The ACL Editor provides a user-friendly interface for maintaining and manipulating rules in an ACL. Using the editor, you can add, delete or re-order ACL rules. In addition, if the modified ACL is currently applied to an interface, the ACL is automatically “re-applied” to the interface and takes effect immediately. To edit an ACL, you enter the **acl-edit** command in Configure mode. The command must also specify the name of the ACL you want to edit. Only one ACL can be edited at one time.

3.1 COMMAND SUMMARY

The following table lists the commands available with the ACL Editor. The sections following the table describe the command syntax.

<code>acl-edit <aclname></code>
<code>acl <name> permit deny</code>
<code>delete <rule#></code>
<code>exit</code>
<code>move <rule#> after <rule#></code>
<code>save</code>
<code>show</code>

acl-edit

Mode

Configure

Format

acl-edit <aclname>

Description

The **acl-edit** command enters the ACL Editor to edit an ACL specified by the user. Once inside the ACL editor, the user can then add, delete or re-order ACL rules for that ACL. If the ACL happens to be applied to an interface, changes made to that ACL will automatically take effect when the changes are committed to the running system.

Parameter	Value	Meaning
acl-edit	<aclname>	Name of the ACL to edit.

Restrictions

Inside the ACL Editor, you can only add rules for the ACL you specified in the **acl-edit** command. You cannot add rules for other ACLs. Basically, each ACL editing session works only on one ACL at a time. For example, if you start with **acl-edit 110**, you cannot add rules for **ACL 121**.

Example

To edit ACL 111:

```
rs(config)# acl-edit 111
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any

rs(acl-edit)> ?
acl                - Configure L3 Access Control List
delete             - Delete an ACL rule
exit               - Exit current mode
move               - Move an ACL rule
save               - Save changes made to this ACL
show               - Show contents of this ACL
```


acl permit|deny*

Mode

ACL Editor

Format

```
acl <name> permit|deny <address>
```

Description

The **acl permit|deny** commands are equivalent to the same commands in the Configuration mode. You can use these commands to create rules for the ACL that you are editing. Just like the ACL commands in Configuration mode, new rules are appended to the end of the rules. You can use the move command to re-order the rules.

Parameter	Value	Meaning
Refer to Chapter 2, "acl Commands."	Refer to Chapter 2, "acl Commands."	Refer to Chapter 2, "acl Commands."

Restrictions

You can only add rules for the ACL you specified in the acl-edit command. You cannot add rules for other ACLs. For example, if you start with **acl-edit 110**, you cannot add rules for **ACL 121**.

Example

To add a new rule (deny all UDP traffic) to ACL 111:

```
rs(config)# acl-edit 111
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any

rs(acl-edit)> acl 111 deny udp
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 111 deny udp
```

delete

Mode

ACL Editor

Format

```
delete <rule#>
```

Description

The **delete** commands allows the administrator to delete a specific rule from an ACL. When in the ACL Editor, each rule is displayed with its rule number. One can delete a specific rule from an ACL by specifying its rule number with the delete command.

Parameter	Value	Meaning
delete	<rule#>	Number of the ACL rule to delete.

Restrictions

None

Example

To delete ACL rule number 2 from the ACL:

```
rs(config)# acl-edit 111
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 111 deny udp

rs(acl-edit)> delete 2
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 deny udp
```

exit

Mode

ACL Editor

Format

exit

Description

The **exit** command allows the user to exit the ACL Editor. Before exiting, if changes are made to this ACL, the system will prompt the user to see if the changes should be committed to the running system or discarded. If the user commits the changes then changes made to this ACL will take effect immediately. If the ACL is applied to an interface, the ACL is automatically re-applied to the interface. Packets going through this interface will be matched against the new rules in this ACL. If the user chooses not to commit the changes, the changes will be discarded. The next time the user edits this ACL, changes from the previous edit session will be lost.

Parameter	Value	Meaning
exit		Exits the ACL Editor.

Restrictions

None

Example

To create an ACL to deny IGMP traffic from the subnet **10.1.5.0** (with a 24 bit netmask) to any destination:

```
rs(config)# acl-edit 111
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 111 deny udp

rs(acl-edit)> delete 2
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 deny udp

rs(acl-edit)> exit

rs(config)# acl 410 deny igmp 10.1.5.0/24 any
```

move

Mode

ACL Editor

Format

```
move <src-rule#> after <dst-rule#>
```

Mode

ACL Editor

Description

The **move** command provides the user with the ability to re-order rules within an ACL. When new rules are entered in the ACL Editor, they are appended to the end of the rules. One can move these rules to the desired location by using the move command. The move command can also be used on existing ACL rules created in Configuration mode instead of the ACL Editor.

Parameter	Value	Meaning
move	<src-rule#> >	Rule number of the rule you want to move.
after	<dst-rule#> >	Rule number of the rule after which you want the source rule to move to.

Restrictions

None

Examples

To move rule #2 to the end of the list:

```
rs(config)# acl-edit 111
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 111 permit udp 10.1.17.0/24 10.1.22.0/24 2000-2002 any
4*: acl 111 permit udp 10.1.18.0/24 10.1.34.0/24 2003-2005 any

rs(acl-edit)> move 2 after 4
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit udp 10.1.17.0/24 10.1.22.0/24 2000-2002 any
3*: acl 111 permit udp 10.1.18.0/24 10.1.34.0/24 2003-2005 any
4*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
```

save

Mode

ACL Editor

Format

save

Description

The **save** command saves any non-committed changes made by the ACL Editor. If changes are made to this ACL, the changes will be saved and will take effect immediately. If the ACL is applied to an interface, the ACL is automatically re-applied to the interface. Packets going through this interface will be matched against the new rules in this ACL. The **save** command also contains an implicit exit command. Regardless of whether changes were made by the ACL Editor or not, upon completion of the **save** command, the user exits the ACL Editor and returns to Configuration mode. Consequently, one should issue the **save** command after all the changes are made.

Parameter	Value	Meaning
save		Saves any non-committed changes made by the ACL Editor.

Restrictions

None

Examples

To save and commit the changes made by the ACL Editor.

```
rs(config)# acl-edit 111
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 111 deny udp

rs(acl-edit)> delete 2
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 deny udp

rs(acl-edit)> save
```

show

Mode

ACL Editor

Format

show

Description

The **show** command displays the contents of the ACL currently being edited.

Parameter	Value	Meaning
show		Displays ACL currently being edited.

Restrictions

None

Examples

To display the contents of the ACL currently being edited:

```
rs(acl-edit)# show
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
```

4 AGING COMMANDS

The aging commands control aging of learned MAC address entries in the RS's L2 lookup tables or layer3/4 flows. Using the aging commands, you can show L2 or layer 3/4 aging information, set or disable L2 aging on specific ports, set or disable aging of layer 3/4 flows, or set or disable NAT or LSNAT flows.

4.1 COMMAND SUMMARY

The following table lists the L2 and L3 aging commands. The sections following the table describe the command syntax.

<code>aging l2 disable <port-list> all-ports</code>
<code>aging l2 set aging-timeout <seconds> port <port-list> all-ports</code>
<code>aging l2 show status</code>
<code>aging l3 set timeout <seconds> disable</code>
<code>aging l3 set nat-flow-timeout <minutes> disable</code>
<code>aging l3 show status</code>

aging l2 disable

Mode
Configure

Format

aging l2 disable <port-list>|all-ports

Description

By default, the RS ages learned MAC addresses in the L2 lookup tables. Each port has its own L2 lookup table. When a learned entry ages out, the RS removes the aged out entry. You can disable this behavior by disabling aging on all ports or on specific ports.

Parameter	Value	Meaning
disable	<port-list>	The port(s) on which you want to disable aging. You can specify a single port or a comma-separated list of ports. If you use the all-ports keyword, aging is disabled on all ports.
	all-ports	Applied to all ports

Restrictions

Unknown.

Examples

To disable aging on slot 1, port 3:

```
rs(config)# aging l2 disable et.1.3
```

To disable aging on slot 4, port 2, and slots 1 through 3, ports 4, 6, 7, and 8:

```
rs(config)# aging l2 disable et.4.2,et.(1-3).(4,6-8)
```

To disable aging on all ports:

```
rs(config)# aging l2 disable all-ports
```


aging l2 set aging-timeout

Mode

Configure

Format

```
aging l2 set <port-list>|all-ports aging-timeout <seconds>
```

Description

The **aging l2 set aging-timeout** command sets the aging time for learned MAC entries. When the aging time expires for a MAC address, the RS removes the MAC address from the specified port(s). The aging time is specified in seconds.

Parameter	Value	Meaning
set	<port-list>	The port(s) on which you want to set the aging time. You can specify a single port or a comma-separated list of ports. If you use the all-ports keyword, the aging time is set on all ports.
	all-ports	Applied to all ports
aging-timeout	<seconds>	The number of seconds the RS allows a learned MAC address to remain in the L2 lookup table (for the specified port). You can specify from 15 to 1000000 seconds. The default is 300 seconds.

Restrictions

None.

Example

To set the aging time to 15 seconds on all ports:

```
rs(config)# aging l2 set all-ports aging-timeout 15
```

aging l2 show status

Mode
User

Format

aging l2 show status

Description

The **aging l2 show status** command shows whether L2 aging is enabled or disabled on RS ports. For ports on which L2 aging is enabled, this command also shows the aging time.

Parameter	Value	Meaning
status		Shows whether L2 aging is enabled or disabled.

Restrictions

None.

Example

This partial output shows whether L2 aging is enabled and the aging time for each port:

rs# aging l2 show status		
Port	Aging	Timeout (secs)
----	-----	-----
gi.3.1	Disabled	300
gi.3.2	Disabled	300
gi.3.3	Disabled	300
gi.3.4	Disabled	300
gi.3.5	Disabled	300
gi.3.6	Disabled	300
gi.3.7	Disabled	300
gi.3.8	Disabled	300
et.5.1	Disabled	300
et.5.2	Disabled	300
et.5.3	Disabled	300
et.5.4	Disabled	300
et.5.5	Disabled	300
et.5.6	Disabled	300

aging l3 set timeout

Mode

Configure

Format

```
aging l3 set timeout <seconds>|disable
```

Description

The **aging l3 set timeout** command sets the aging time for a layer 3/4 flow. The aging time is specified in seconds.

Parameter	Value	Meaning
timeout	<seconds>	The number of seconds the RS allows for a layer 3/4 flow. You can specify a value from 4 to 3600 seconds. For example, in an ISP environment (where thousands of flows are possible), you could change this value to 180-300 (3-5 minutes) to help in keeping with longer-term flows. The default is 30 seconds.
disable		Disables layer 3/4 aging.

Restrictions

None.

Example

To set the layer 3/4 flow aging time to 300 seconds (5 minutes):

```
rs(config)# aging l3 set timeout 60
```

aging l3 set nat-flow-timeout

Mode
Configure

Format

aging l3 set nat-flow-timeout <minutes>|disable

Description

The **aging l3 set nat-flow-timeout** command sets the aging time for Network Address Translation (NAT) and Load Sharing NAT flows. The aging time is specified in minutes.

Parameter	Value	Menaing
nat-flow-timeout	<minutes>	The number of minutes the RS allows for NAT and LSNAT flows. You can specify from 2 to 120 minutes. The default is 2 minutes.
disable		Disables NAT and LSNAT flow aging.

Restrictions

None.

Example

To set the NAT aging time to 5 minutes:

```
rs(config)# aging l3 set nat-flow-timeout 5
```

aging l3 show status

Mode

User

Format

aging l3 show status

Description

The **aging l3 show status** command shows whether layer 3/4 aging is enabled or disabled on RS ports. For ports on which layer 3/4 aging is enabled, this command also shows the aging time.

Parameter	Value	Meaning
status		Shows whether L3/L4 aging is enabled or disabled.

Restrictions

None.

Example

To show whether layer 3/4 aging is enabled and the aging time for enabled ports:

```
rs# aging l3 show status
L3 Aging: Timeout 30 seconds
```

5 ARP COMMANDS

The **arp** commands enable you to add, display, and clear ARP entries on the RS.

5.1 COMMAND SUMMARY

The following table lists the arp commands. The sections following the table describe the command syntax.

arp add <host> mac-addr <MAC-addr> exit-port <port> keep-time <seconds>
arp clear <host> all [interface <string> all] [port <port>]
arp set drop-unresolved disabled enabled
arp set interface <name> all keep-time <number>
arp set unresolve-threshold <num>
apr set unresolve-timer <num>
arp show <IPaddr> all [undecoded] [unresolved] [interface <string> all] [port <port>]
statistics show arp

arp add

Mode

Enable and
Configure

Format

```
arp add <host> mac-addr <MAC-addr> exit-port <port> keep-time <seconds>
```

Description

The `arp add` command lets you manually add ARP entries to the ARP table. Typically, the RS creates ARP entries dynamically. Using the `arp add` command, you can create an ARP entry to last a specific amount of time or as a permanent ARP entry. This command exists in both Enable and Configure mode with a slight variation. The `keep-time` option is valid only in Enable mode. The `keep-time` option allows you to create an ARP entry to last a specific amount of time. The Configure mode version of the `arp add` command does not use the `keep-time` option. ARP entries created in the Configure mode are permanent ARP entries and they do not have an expiration time. If the exit port is not specified, then packets to the IP address for which the ARP entry is created are transmitted on all ports of the interface. If an ARP request is received from the host for which the ARP entry was created, then the exit port is updated with the port on which the ARP request was received, so that subsequent packets are transmitted on one port only.

Parameter	Value	Meaning
add	<host>	Hostname or IP address of this ARP entry.
mac-addr	<MAC-addr>	MAC address of the host.
exit-port	<port>	The port for which you are adding the entry. Specify the port to which the host is connected.
keep-time	<seconds>	The number of seconds this ARP entry should remain in the ARP table. A value of 0 means this is a permanent ARP entry.



Note This option is valid only for the Enable mode **arp add** command.

Restrictions

If you enter the **arp add** command while in the Configure mode, you can add only permanent ARP entries.

Examples

To create an ARP entry for the IP address **10.8.1.2** at port **et.4.7** for **15** seconds:

```
rs# arp add 10.8.1.2 mac-addr 08:00:20:a2:f3:49 exit-port et.4.7  
keep-time 15
```

To create a permanent ARP entry for the host *nfs2* at port et.3.1:

```
rs(config)# arp add nfs2 mac-addr 080020:13a09f exit-port et.3.1
```


arp clear

Mode

Enable

Format

```
arp clear <host>|all [interface <string>| all] [port <port>]
```

Description

The **arp clear** command lets you manually remove entries from the ARP table. The command can remove both dynamic and permanent entries.

Parameter	Value	Meaning
clear	<host>	Hostname or IP address of the ARP entry to remove.
all		Remove all ARP entries, thus clearing the entire ARP table.
interface		Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific interface.
	<string>	Specifies the interface name.
	all	Specifies all interfaces.
port		Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific exit port.
	<port>	Specifies the exit port.

Examples

To remove the ARP entry for the host **10.8.1.2** from the ARP table:.

```
rs# arp clear 10.8.1.2
```

To clear the entire ARP table.

```
rs# arp clear all
```

If the Startup configuration file contains arp add commands, the Control Module re-adds the ARP entries even if you have cleared them using the arp clear command. To permanently remove an ARP entry, use the **negate** command or no command to remove the entry. Here is an example of the no command:

```
rs# no arp add nfs2 macaddr 080020:13a09f exit-port et.3.1
```

This command removes the ARP entry for “nfs2”.

arp set drop-unresolved

Mode

Configure.

Format

arp set drop-unresolved disabled| enabled

Description

The **arp set drop-unresolved** command lets you specify how to deal with traffic that is unresolved by address resolution protocol. This command specifies that the router will drop all traffic to unresolved IP addresses in hardware until the nexthop MAC address is resolved. Sixth and subsequent packets are dropped.

Paramter	Value	Meaning
drop-unresolved		Specifies router to drop all traffic to unresolved IP addresses.
	disabled	Specifies that all unresolved ARP traffic will be handled by the software. This is the default.
	enabled	Specifies that all unresolved ARP traffic will be dropped into the hardware. The route then tries to resolve the nexthop MAC address by sending ARP requests.

Examples

To enable the drops of unresolved ARP traffic:

```
rs# arp set drop-unresolved enabled
```

arp set interface

Mode

Configure

Format

```
arp set interface <name>|all keep-time <number>
```

Description

The **arp set interface ... keep-time** command lets you specify the lifespan (in seconds) for any or all ARP interface entries.

Parameter	Value	Meaning
interface	<name>	Name of the interface(s) for which you will define the lifespan.
	all	All interfaces
keep-time	<number>	Number of seconds determining lifespan of ARP interfaces. The default value is 1200 seconds (20 minutes).

arp set unresolve-threshold

Mode

Configure.

Format

```
arp set max-unresolved <number>
```

Description

The **arp set max-unresolved** command lets you specify the number of ARP requests to send out to resolve the nexthop MAC address. This command sets the maximum number of ARP entries that the CPU will try to resolve in each attempt when ARP entries have traffic stopped in hardware.

Parameter	Value	Meaning
max-unresolved	<number>	Specifies that maximum number of ARP requests are sent out. Specify any number greater than or equal to 1. The default is 35.

Examples

To configure the CPU to send out 100 ARP requests:

```
rs# arp set unresolve-threshold 100
```

arp set unresolve-timer

Mode

Configure.

Format

```
arp set unresolve-timer <number>
```

Description

The **arp set unresolve-timer** command lets you specify the frequency in which to send out ARP requests to resolve the nexthop MAC address. This command configures the timer which controls the interval after which the CPU sends ARP requests and try to resolve those ARP entries which have traffic stopped in hardware.

Parameter	Value	Meaning
unresolve-timer	<number>	Specifies that interval for which ARP requests are sent out. Specify any number greater than or equal to 20. This parameter is in seconds. The default is 5 seconds.

Examples

To configure the CPU to send out ARP requests every 10 seconds:

```
rs# arp set unresolve-timer 10
```

arp show

Mode
Enable

Format

arp show <IPaddr>|all [undecoded] [unresolved] [interface <string>| all] [port <port>]

Description

The **arp show** command displays the entire ARP table.

Parameter	Value	Meaning
show	<IPaddr>	Shows the ARP entry for the specified IP address.
	all	Shows all entries in the ARP table.
undecoded		Specify this optional parameter to show MAC addresses in hexadecimal format.
unresolved		Specify this optional parameter to show only MAC addresses in the ARP table that have yet to be mapped to an network layer address.
interface	<string>	Specify this optional parameter to show only addresses in the ARP table that is associated with the specific interface.
	all	Specifies all interfaces.
port	<port>	Specify this optional parameter to show only addresses in the ARP table that corresponds to a specific exit port.

6 ATM COMMANDS

6.1 COMMAND SUMMARY

The following table lists the **atm** commands. The sections following this table describe the command syntax for each command.

atm add vcl <ATM-port> to <vc-group> [priority low medium high control] [broadcast-multicast]
atm apply service <string> port <port-list vc-group>
atm clear stats port <port-list>
atm create vcgroup <vc-group> slot <num>
atm create vcl port <port-list> [aal1]
atm define service <string> [srv-catubr cbr abr rt-vbr nrt-vbr] [pcr pcr-kbits] [scr scr-kbits] [mbs] [encaps llc-mux vc-mux] [traffic ppp] [oam on off] [ppp-retry-interval <num>] [ppp-max-failure <num>] [ppp-max-terminate <num>] [ppp-max-configure <num>] [ppp-lcp-magic on off] [ppp-lcp-echo on off] [ppp-auth none pap chap other] [chap-rechallenge-interval <num>]
atm ping port <port> [count <num>] [segment][wait <number>]
atm restart ppp port <port>
atm set cross-connect <ATM-port> to <ATM-port>
atm set peer-addr port <port> ip-address <ipaddr> ipx-address <netaddr>.<macaddr>
atm set port <port-list> all-ports cell-mapping direct plcp
atm set port <port-list> all-ports oam-detect-down
atm set port <port-list> all-ports oam-detect-up
atm set port <port-list> all-ports pdh-cell-scramble on off
atm set port <port-list> all-ports vpi-bits <num>
atm set vcgroup port <vc-group> forced-bridged
atm set vcl port <port> forced-bridged traffic-stats-enable mac-addr-limit <number>

atm set vcl-buffering port <port-list> low <number> medium <number> high <number> control <number>
atm set vcl-priority port <port> [priority <number> low medium high control] [vlan-type all ip ipx l2]
atm set vcl-qos port <port-list> low <number> medium <number> high <number> control <number> relative-latency <number>
atm show vpl port <port list> [summary] vcl port <port-list> [summary] vcgroup port <vc group> ppp port <port list> [summary] service <string> port-settings <port-list> stats port <port-list>
atm show port-settings <port-list> all-ports
atm show ppp port <port-list> all-ports [summary]
atm show service <service-name> all
atm show stats port <port-list>
atm show vcgroup port <vcgroup> all
atm show vcl {port <port-list> all} {summary port <port-list> all}
atm show vpl {port <port-list> all} {summary port <port-list> all}

atm add vcl

Mode

Configure

Format

```
atm add vcl <ATM port> to <vc group> [priority low|medium|high|control]
[broadcast-multicast]
```

Description

The **atm add vcl** command adds a virtual channel to a predefined virtual channel group. A virtual channel group is a grouping of up to four separate virtual channels. This grouping is handled by the RS as one large virtual circuit. Create a VC group using the "atm create vcgroup" command later in this chapter.

Each VC within a virtual channel group is assigned one (or more) of four priority levels: low, medium, high, and control. The priority level prioritize the data on the separate VCs in case of the connection becoming oversubscribed and packets start dropping off. This feature is advantageous when various data traffic passing between two end devices through one virtual channel needs to be prioritized.

One virtual channel within a VC group can be designated as a broadcast or multicast virtual channel.

Parameter	Value	Meaning
vcl	<ATM port>	Is a single ATM port, including the vpl and vcl.
to	<vc group>	Is the virtual channel group designation. Specify a designation in the following format: vg.group_index , where the group_index is any number between 1 and 4095.
priority		Is the priority level assigned to the virtual channel within the VC group.
	low	Assigns low priority level for the virtual channel.
	medium	Assigns medium priority level for the virtual channel.
	high	Assigns high priority level for the virtual channel.
	control	Assigns control priority level for the virtual channel.
broadcast-multicast		Specifies that the virtual channel being added will be designated as the broadcast VC. Note that only one virtual channel may be designated as the broadcast VC. The default is that broadcast-multicast traffic will be transmitted through the lowest priority VC.

Restrictions

This command is valid for ATM OC-12 line card only.

There are some restrictions that should be observed when adding a virtual channel to a VC group.

If a VC group has a service applied to it, the VCs that are added to the VC group must not already have a service applied to it. Either a service can be applied to each individual VC within the VC group, or the VC group can have a service applied to it.

You must remove any service profile first, then add the virtual channel to a VC group. The virtual channel will then take on the service profile applied to the whole group.

The virtual channel cannot already belong to a VLAN. You must remove the virtual channel from any VLAN before adding it to a VC group.

The virtual channel cannot already belong to an interface. You must remove the virtual channel from any interface before adding it to a VC group.

You cannot add a virtual channel with forced-bridged enabled to a VC group.

Example

To add the virtual channel 'at.2.1.0.100' to the VC group 'vg.1', with a high priority:

```
rs(config)# atm add vcl at.2.1.0.100 to vg.1 priority high
```

atm apply service

Mode

Configure

Format

```
atm apply service <service-name> port <port list|vc group>
```

Description

The **atm apply service** command applies a service profile to a virtual channel (VC), VC group, virtual path (VP), and/or atm port. Service profiles define certain values for traffic and PPP parameters. Each service profile has its own unique set of traffic guarantees in handling transmission of ATM cells.

An important concept when applying service profile definitions is the concept of inheritance. Since a service profile definition can be applied to a virtual channel, virtual path, or on a port; the actual connection can inherit the service profile definition from any one of the three. The virtual channel will inherit the service profile definition that is directly applied on it. If no service profile was applied to the virtual channel, the connection will inherit the service profile applied to the virtual path. If no service profile definition was applied to the virtual path, then the connection will inherit the service profile applied to the ATM port. If no service profile was applied to the port, then the default service profile UBR is applied.

The following service classes are supported: CBR (constant bit rate), rt-VBR (real-time variable bit rate), nrt-VBR (non real-time variable bit rate), and UBR (unspecified bit rate). ABR (available bit rate) is currently not supported.

Parameter	Value	Meaning
service	<service-name>	The name of a previously-defined service. You define a service using the "atm define service" command.
port	port list	The port name in the following format: media.slot.port.vpi.vci vg.group_index media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. This parameter is optional. vci Is the Virtual Channel Identifier. This parameter is optional.
	vc-group	For a virtual channel group designation, specify a designation in the following format: vg.group_index , where group_index is any number between 1 and 4095. vg.group_index

Restrictions

You cannot apply a service profile to a VC group if any of the individual virtual channels within the group already has a service profile applied. Either apply a service profile to each VC within a VC group, or apply a service profile to the VC group as a whole. You cannot apply a profile to both.

You must first negate the separate service profiles from each virtual channel before applying a service profile to the whole VC group, and vice versa.

Examples

To apply the pre-defined service profile 'CBR1' to virtual channel at.5.1.1.100:

```
rs(config)# atm apply service CBR1 port at.5.1.1.100
```

To apply the pre-defined service profile 'CBR1' to virtual path at.5.1.1:

```
rs(config)# atm apply service CBR1 port at.5.1.1
```

To apply the pre-defined service profile 'CBR1' to port at.5.1:

```
rs(config)# atm apply service CBR1 port at.5.1
```

atm clear stats

Mode

Enable

Format

atm clear stats port *<port list>*

Description

The **atm clear stats** command clears the statistics for a particular virtual channel.

Parameter	Value	Meaning
port	<i><port list></i>	Specifies the port name and virtual channel in the format: media.slot.port.vpi.vci media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.

Restrictions

This command is valid for the ATM OC-12 line card only.

Example

To clear the statistics for the virtual channel on slot 5, port 1, VPI 1, and VCI 100:

```
rs(config)# atm clear stats port at.5.1.1.100
```

atm create vcgroup

Mode

Configure

Format

```
atm create vcgroup <vc group> slot <num>
```

Description

The **atm create vcgroup** command creates a virtual channel group. A virtual channel group is a grouping of up to four separate virtual channels. This grouping is handled by the RS as one large virtual circuit.

Each VC within a virtual channel group is assigned one (or more) of four priority levels: low, medium, high, and control. The priority level prioritize the data on the separate VCs in case of the connection becoming oversubscribed and packets start dropping off. This feature is advantageous when various data traffic passing between two end devices through one virtual channel needs to be prioritized.

QoS must be enabled on the router in order for traffic to be prioritized in a VC group.

Parameter	Value	Meaning
vcgroup	<vc group>	Is the virtual channel group designation. Specify a designation in the following format: vg.group_index , where group_index is any number between 1 and 4095.
slot	<num>	Is the slot number where the module is installed. Specify a number between 1 and 32

Restrictions

This command is valid for the ATM OC-12 line card only.

Example

To create a virtual channel group 'vg.1' on slot 1:

```
rs(config)# atm create vcgroup vg.1 slot 1
```

atm create vcl

Mode
Configure

Format

```
atm create vcl port <port list> [aal1]
```

Description

The **atm create vcl** command creates a virtual channel on an ATM port. Virtual channels are point to point cell-switched connections used for ATM cell traffic. Virtual channels are defined by specifying a VCI (Virtual Channel Identifier) and VPI (Virtual Path Identifier) pair.

The range of available VCI and VPI for the ATM multi-rate line card is set by the **atm set port vpi-bits** command found later in this chapter. The VPI and VCI bit allocation for the ATM OC-12 line card is fixed: 4 bits allocated for VPI and 12 bits allocated for VCI.



Note Be careful when specifying VCI numbers 0 through 31. Those VPI/VCI pairs are used by some protocols for signaling purposes.

Parameter	Value	Meaning
port	<port list>	The port name in the format: media.slot.port.vpi.vci media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
	aal1	Opens the VC to send and receive AAL1 cells rather than AAL5 packets. VCs opened with this option cannot be added to VLANs or used in an interface create command.

Restrictions

None.

Examples

To create a virtual channel on slot 5, port 1, VPI 1, and VCI 100:

```
rs(config)# atm create vcl port at.5.1.1.100
```

To create VCIs (100, 555-600, 700) on VPIs (1, 3, 4, 5, 7) simultaneously:

```
rs(config)# atm create vcl port at.5.1.(1,3-5,7).(100,555-600,700)
```


atm define service

Mode

Configure

Format

```
atm define service <string> [srv-catubr|cbr|abr|rt-vbr|nrt-vbr] [pcr|pcr-kbits]
[scr|scr-kbits] [mbs] [encaps llc-mux|vc-mux] [traffic ppp] [oam on|off]
[ppp-retry-interval <num>] [ppp-max-failure <num>] [ppp-max-terminate <num>]
[ppp-max-configure <num>] [ppp-lcp-magic on|off] [ppp-lcp-echo on|off] [ppp-auth
none|pap|chap|either] [chap-rechallenge-interval <num>]
```

Description

The **atm define** command defines a set of traffic parameters. You can then apply this set of traffic parameters to a virtual channel or a VC group. Quality of Service (QoS) parameters define the delays, dependability, and peak limits for a virtual channel. Class of Service defines the bandwidth guarantees. When a virtual channel is established, a service profile definition created by this command can then be applied to the connection.

Parameter	Value	Meaning
service	<string>	Is a character string. The maximum length is 32 characters.
srv-cat		Is the service category (UBR is the default):
	ubr	Unspecified Bit Rate. This service category is strictly best effort and runs at the available bandwidth. Users may limit the bandwidth by specifying a PCR value. The SCR and MBS are ignored. This service class is intended for applications that do not require specific traffic guarantees. UBR is the default.
	cbr	Constant Bit Rate. This service category provides a guaranteed constant bandwidth specified by the Peak Cell Rate (PCR). This service requires only the PCR value. The Sustainable Cell Rate (SCR) and Maximum Burst Size (MBS) values are ignored. This service category is intended for applications that require constant cell rate guarantees such as uncompressed voice or video transmission.
	abr	Available Bit Rate. This service category guarantees a minimum cell rate only, intended for best effort applications. This service category is currently unsupported.
	rt-vbr	Real-Time Variable Bit Rate. This service category provides a guaranteed constant bandwidth (specified by the SCR), but also provides for peak bandwidth requirements (specified by the PCR). This service category requires the PCR, SCR, and MBS options and is intended for applications that can accommodate bursty real-time traffic such as compressed voice or video.

Parameter	Value	Meaning
	nrt-vbr	Non Real-Time Variable Bit Rate. This service category provides a guaranteed constant bandwidth (specified by the SCR), but also provides for peak bandwidth requirements (specified by the PCR). This service category requires the PCR, SCR, and MBS options and is intended for applications that can accommodate bursty traffic with no need for real-time guarantees.
pcr	<num>	Is the Peak Cell Rate, and specifies the maximum cell transmission rate, expressed in cells/sec. The default is 353207 cells/sec for the ATM multi-rate line card. The default is 1173584 cells/sec for ATM OC-12. This parameter is valid for CBR, rtVBR, nrtVBR, and UBR service categories.
pcr-kbits	<num>	Is the Peak Cell Rate, and specifies the maximum cell transmission rate, expressed in kbits/sec. The default is 149759 kbits/sec for the ATM multi-rate line card. The default is 497600 kbits/sec for ATM OC-12. This is the same as PCR, but is expressed in kbits/sec, and therefore may be a more convenient form. However, since the natural unit for ATM is cells/sec, there may be a difference in the actual rate because the kbit/sec value may not be an integral number of cells. This parameter is valid for CBR, rtVBR, nrtVBR, and UBR service categories.
scr	<num>	Is the Sustainable Cell Rate, and specifies the average cell rate, expressed in cells/sec. The default is 0 cells/sec. This parameter is valid only for rtVBR and nrtVBR service categories.
scr-kbits	<num>	Is the Sustainable Cell Rate, and specifies the average cell rate, expressed in kbits/sec. The default is 0 kbits/sec. This is the same as SCR, but is expressed in kbits/sec, and therefore may be a more convenient form. However, since the natural unit for ATM is cells/sec, there may be a difference in the actual rate because the kbit/sec value may not be an integral number of cells. This parameter is valid only for rtVBR and nrtVBR service categories.
mbs	<num>	Is the Maximum Burst Size in cells. MBS specifies how many cells can be transmitted at the Peak Cell Rate. Specify any number between 2 and 255. This parameter is valid only for rtVBR and nrtVBR service categories.
encaps		Is the encapsulation scheme to transport multi protocol data over the AAL5 layer.
	llc-mux	Logical link control based multiplexing. This is the default.
	vc-mux	Virtual channel-based multiplexing.
traffic	ppp	Specifies that type of traffic that is being transmitted through the VC is PPP traffic.

Parameter	Value	Meaning
oam		OAM (Operation, Administration, and Management) loop back cells are used to provide loop back capabilities and confirm whether a VC connection is up. Only F5 OAM segments are supported, which provides loop back capabilities on a VC connection level. This parameter turns OAM on or off on the PVC.
	on	OAM on means that the RS generates F5 OAM requests and responses.
	off	OAM off means that the RS only generates F5 OAM responses. This is default.
ppp-retry-interval	<num>	Specifies the amount of time (in seconds) between consecutive Configure-Request and Terminate-Ack packets. Specify any number between 1 and 7200. This parameter is valid only for the ATM OC-12 line card.
ppp-max-failure	<num>	Specifies the number of Configure-Nak packets to send out without receiving any Configure-Ack packets. Configuration is considered not converging if this threshold is met. To facilitate convergence, Configure-Reject packets will be sent in place of Configure-Nak packets. Specify any number equal to or greater than 1. This parameter is valid only for the ATM OC-12 line card.
ppp-max-terminate	<num>	Specifies the number of Terminate-Nak packets to send out without receiving any Terminate-Ack packets before declaring the link down. Specify any number equal to or greater than 1. This parameter is valid only for the ATM OC-12 line card.
ppp-max-configure	<num>	Specifies the number of Configure-Request packets to send out without receiving any Configure-Ack, Configure-Nak, or Configure-Reject packets. Specify any number equal to or greater than 1. This parameter is valid only for the ATM OC-12 line card.
ppp-lcp-magic		Allows you to enable the option to send out magic numbers. A magic number allows you to detect any loops within the connection. If the port sends out a magic number, the other end will reply with a different magic number. If the port receives the same magic number that it sent out, then there is a loop within the connection. This parameter is valid only for the ATM OC-12 line card.
	on	Enables sending out magic numbers. This is default.
	off	Disables sending out magic numbers.
ppp-lcp-echo		Allows you to enable the option to send out echo messages. An echo message allows you to detect whether there is another device present on the other end of the connection. If a port sends out an echo message and there is no device on the other end, the port will not get back an echo message. This parameter is valid only for the ATM OC-12 line card.
	on	Enable sending out echo messages. This is default.

Parameter	Value	Meaning
	off	Disables sending out echo messages.
ppp-auth		Sets the Point-to-Point Protocol authentication scheme to pap , chap , either , or none . This parameter is valid only for the ATM OC-12 line card.
	none	No PPP authentication. This is default.
	pap	Specifies PAP authentication.
	chap	Specifies CHAP authentication.
	either	Specifies either PAP or CHAP authentication, whichever can be negotiated.
chap-rechallenge-interval	<num>	Specifies a time interval upon which another challenge will be sent to the CHAP client. This is to ensure no unauthorized clients have access to the connection. Specify a number between 10 and 7200. Specify a number that is at least 10% of the total number of connections. This parameter is valid only for the ATM OC-12 line card.

Restrictions

scr can not exceed **pcr**. No parameters may exceed the link rate for the type of PHY.

Examples

To define a 10Mbps service:

```
rs(config)# atm define service CBR-example srv-cat cbr pcr_kbits 10000
```

atm ping

Mode

Enable

Format

atm ping port <port> [count <number>][segment][wait <number>]

Description

The **atm ping** command allows you to test the connection between the RS and an ATM device.

Parameter	Value	Meaning
port	<port>	Specifies the ATM port in the format: media.slot.port.vpi.vci. media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
count	<number>	Specifies the number of pings to send.
segment		The adjacent ATM device responds to the OAM request.
wait	<number>	The number of seconds to wait for a response.

Restrictions

None.

Example

Following is an example of the **atm ping** command:

```
rs(config)# atm ping at.5.1.1.100 count 3
```

atm restart ppp

Mode
Enable

Format

atm restart ppp port <port>

Description

The **atm restart ppp** command allows you to restart PPP negotiations. The Link Control Protocol (LCP) establishes a link and negotiates the configuration parameters. The Network Control Protocols (NCP) configures network-layer protocols.

Parameter	Value	Meaning
port	<port>	Specifies the ATM port. media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.

Restrictions

Valid only for the ATM OC-12 line card.

atm set cross-connect

Mode
Configure

Format

atm set cross-connect<ATM-port> to <ATM-port>

Description

The **atm set cross-connect** command allows you to switch packets from a VC on one port to another VC on another port.

Parameter	Value	Meaning
cross-connect	<ATM-port>	Specifies a single port, including virtual channel in the format: media.slot.port.vpi.vci . media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
to	<ATM-port>	Specifies a single port, including virtual channel in the format: media.slot.port.vpi.vci . media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.

Restrictions

This command is valid only for the multi-rate line card.

Example

To configure a cross-connect between at.5.1.0.100 to at.4.1.0.101:

```
rs(config)# atm set cross-connect at.5.1.0.100 to at.4.1.0.101
```

atm set peer-addr

Mode
Configure

Format

atm set peer-addr port <port> ip-address <ipaddr>|ipx-address <netaddr>.<macaddr>

Description

The **atm set peer-addr** command allows you to map a peer address for an ATM port to a specific virtual channel. This allows you to associate a specific virtual channel and its interface to a specific peer address.

Parameter	Value	Meaning
port	<port>	Specifies a single port, including virtual channel, in the format: media.slot.port.vpi.vci . media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
ip-address	<ipaddr>	Specifies an IP address for the peer. Specify a unicast IP address and netmask value in the following format: a.b.c.d/e . This IP address will be mapped to the VC.
ipx-address	<netaddr>.<macaddr>	Specifies an IPX address for the peer. Specify an IPX network and node address in the following format: a1b2c3d4.aa:bb:cc:dd:ee:ff . If an <macaddr> is not specified, then a wildcard address is used. This IPX address will be mapped to the VC.

Restrictions

None.

Example

To map the peer address 10.0.0.100/24 to the virtual channel at.4.1.0.100:

```
rs(config)# atm set peer-addr ports at.4.1.0.100 ip-address 10.0.0.100/24
```


atm set port cell-mapping

Mode

Configure

Format

```
atm set port <port list> |all-ports cell-mapping direct|plcp
```

Description

The **atm set port cell-mapping** command specifies the format for mapping ATM cells into PDH (plesiochronous digital hierarchy) T3 and E3 frames. The ATM cells that each frame carries does not fit exactly into the PDH frame, therefore mapping of the data is necessary in ensure efficient transmission.

Parameter	Value	Meaning
port	<port list>	Specifies the ATM port(s).
	all-ports	Specify all-ports to select all ports.
cell-mapping		Specifies the cell mapping format.
	direct	Specifies ATM direct mapping. Default.
	plcp	Specifies physical layer convergence protocol mapping.

Restrictions

This command is valid only for the ATM multi-rate line card. Cell mapping is valid only for T3 and E3 PHY interfaces.

Example

To set cell-mapping to plcp for ATM port at.9.1:

```
rs(config)# atm set port at.9.1 cell-mapping plcp
```

atm set port oam-detect-down

Mode

Configure

Format

```
atm set port <port list> | all-ports oam-detect-down <number>
```

Description

The **atm set port oam-detect-down** command applies only to VCs to which the OAM service is applied. This command specifies the number of seconds between OAM loopback requests. These requests detect if a VC is down. The default is 15 seconds; but you can lower this value if faster detection is needed. When large numbers of VCs are running OAM on the port, be cautious when lowering this number.

Parameter	Value	Meaning
port	<port list>	Specifies the ATM port(s).
	all-ports	Specify all-ports to select all ports.
oam-detect-down	<number>	The number of seconds between OAM loopback requests.

Restrictions

None.

Example

To set the number of seconds on ATM port at.9.1 for OAM loopback requests to detect if a VC is down:

```
rs(config)# atm set port at.9.1 oam-detect-down 10
```

atm set port oam-detect-up

Mode

Configure

Format

atm set port *<port list>* | all-ports oam-detect-up *<number>*

Description

The **atm set port oam-detect-up** command applies only to VCs to which the OAM service is applied. This command specifies the number of seconds between OAM loopback requests used to detect if a VC is up. The default is 15 seconds; but you can lower this value if faster detection is needed. When large numbers of VCs are running OAM on the port, be cautious when lowering this number.

Parameter	Value	Meaning
port	<i><port list></i>	Specifies the ATM port(s).
	all-ports	Specify all-ports to select all ports.
oam-detect-down	<i><number></i>	The number of seconds between OAM loopback requests.

Restrictions

None.

Example

To set the number of seconds on ATM port at.9.1 for OAM loopback requests to detect if a VC is going up:

```
rs(config)# atm set port at.9.1 oam-detect-up 10
```

atm set port pdh-cell-scramble

Mode

Configure

Format

```
atm set port <port list> |all-ports pdh-cell-scramble on|off
```

Description

The **atm set port pdh-cell-scramble** command allows you to enable payload scrambling for PDH (plesiochronous digital hierarchy) PHY interfaces for the ATM line card, such as T3 and E3. Scrambling a payload is important in optimizing the transmission density of the data stream. Since all transmission use the same source clock for timing, scrambling the payload using a random number generator converts the data stream to a more random sequence. This ensures optimal transmission density of the data stream.

Parameter	Value	Meaning
port	<port list>	Specifies the port in the format: media.slot.port media Specifies the media type. This is at for ATM ports. slot Specifies the slot number where the module is installed. port Specifies the port number.
	all-ports	Specify all-ports to enable payload scrambling on all ports.
pdh-cell-scramble		Specifies whether payload scrambling is enabled or disabled.
	on	Enables cell scrambling.
	off	Disables cell scrambling.

Restrictions

This command is valid only for the ATM multi-rate line card. This command is valid only for PDH PHY interfaces. SONET frames are scrambled using the SONET commands.

Example

To enable cell scrambling for ATM port at.9.1:

```
rs(config)# atm set port at.9.1 pdh-cell-scramble on
```

atm set port vpi-bits

Mode

Configure

Format

```
atm set port <port-list>|all-ports vpi-bits <num>
```

Description

The **atm set port vpi-bits** command allows you to set the number of bits allocated for VPI on an ATM port. There are 12 bits available for each VPI/VCI pair. The number of bits allocated determines the amount of VPI and VCI values available. The following equations define the number of virtual paths and virtual channels:

- # of virtual paths = 2^n ; where n is the number of bits allocated for VPI
- # of virtual channels = 2^{12-n} ; where n is the number of bits allocated for VPI

Since there are only 12 bits available for each VPI/VCI pair, the more bits you allocate for VPI, the less bits remain for VCI. This is a shared number of bits. With the bit allocation command, you set the number of bits allocated for VPI. In turn, the remaining number of bits become the number of bits allocated for VCI.



Note The maximum value for n is 4.

Parameter	Value	Meaning
port	<port list>	This parameter identifies the ATM port in the format: media.slot.port . media Specifies the media type. This is at for ATM ports. slot Specifies the slot number where the module is installed. port Specifies the port number.
	all-ports	Specify all-ports to set bit allocation on all ports.
vpi-bits	<num>	Specifies the number of bits allocated for VPI. Specify any number between 1 and 4. The default is 1.

Restrictions

This command is valid only for the ATM multi-rate line card.

Example

To allocate 3 bits for VPI on port at.9.1:

```
rs(config)# atm set port at.9.1 vpi-bits 3
```

atm set vcgroup

Mode

Configure

Format

```
atm set vcgroup port <vc group> forced-bridged
```

Description

The **atm set vcgroup** command enables forced bridging on a per-VC group basis. Forced-bridging forces the VC group to encapsulate all ingress/egress traffic with a Layer 2 MAC address. This feature allows Layer 3 traffic to travel through an intermediate Layer 2 cloud.

A virtual channel group is a grouping of up to four separate virtual channels. This grouping is handled by the RS as one large virtual circuit.

Parameter	Value	Meaning
port	<vc group>	Is the virtual channel group designation in the following format: vg.group_index . Specify group_index as any number between 1 and 4095.
forced-bridged		Enables encapsulation of all traffic as bridged traffic.

Restrictions

This command is valid only for the ATM OC-12 line card. It cannot be applied to individual VCs. Forced bridging can only be applied to the whole VC group. A VC with forced-bridging enabled cannot be added to a group.

You cannot enable forced-bridging on an individual basis. You can enable forced-bridging for the whole group.

Example

To encapsulate all traffic as bridged traffic on VC group 'vg.1':

```
rs(config)# atm set vcgroup port vg.1 forced-bridged
```

atm set vcl

Mode
Configure

Format

```
atm set vcl port <port> forced-bridged|traffic-stats-enable|mac-addr-limit <number>
```

Description

The **atm set vcl** command enables forced bridging and traffic statistics logging on a per-VC basis. In addition, you can use the `mac-addr-limit` parameter to set the limit on the number of MAC addresses that can be learned on a VC.

Forced-bridging forces the VC to encapsulate all ingress/egress traffic with a Layer 2 MAC address. This feature allows Layer 3 traffic to travel through an intermediate Layer 2 cloud.

Parameters

Parameter	Value	Meaning
port	<port>	Specifies a single port, including the virtual channel in the format: media.slot.port.vpi.vci . media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
forced-bridged		Enables encapsulation of all traffic as bridged traffic.

Parameter	Value	Meaning
traffic-stats-enable		Enables gathering of traffic statistics on a VC. You can display traffic statistics using the atm show stats command. This parameter is valid only for the OC-12 line card.
mac-addr-limit	<number>	Sets the limit on the number of MAC addresses that can be learned on a VC. This is useful for preventing a VC that quickly changes its source MAC address from filling the MAC address table. Specify a number between 0 and 127 inclusive.

Restrictions

None.

Example

To encapsulate all traffic as bridged traffic on at.4.1.0.100:

```
rs(config)# atm set vcl port at.4.1.0.100 forced-bridged
```

atm set vcl-buffering

Mode

Configure

Format

```
atm set vcl-buffering port <port-list> low <number> medium <number> high <number> control <number>
```

Description

By default, the hardware limits the number of internal buffers that each VC can use (21 * 240 bytes) for each queue. You can use the **atm set vcl buffering** command to increase the buffers for a queue in cases in which a bursty application is suffering loss.

Parameter	Value	Meaning
port	<port-list>	This parameter identifies the ATM port in the format: media.slot.port.vpi.vci . media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
low	<number>	Sets the number of bytes dedicated to buffering packets of low priority. Enter a value between 1514 and 50000, inclusive.
medium	<number>	Sets the number of bytes dedicated to buffering packets of medium priority. Enter a value between 1514 and 50000, inclusive.
high	<number>	Sets the number of bytes dedicated to buffering packets of high priority. Enter a value between 1514 and 50000, inclusive.
control	<number>	Sets the number of bytes dedicated to buffering packets of control priority. Enter a value between 1514 and 50000, inclusive.

Restrictions

This command is valid only for the multi-rate line card.

Example

To set the internal buffers on port at.4.1.0.100:

```
rs(config)# atm set vcl-buffering port at.4.1.0.100 ctrl 3000 high 50000  
medium 3000 low 3000
```

atm set vcl-priority

Mode

Configure

Format

```
atm set vcl-priority port <port> [priority <number>|low|medium|high|control] [vlan-type all|ip|ipx|l2]
```

Description

The **atm set vcl priority** command sets the priority of all packets/cells received on the VC from the ATM link.

Parameter	Value	Meaning
port	<port>	This parameter identifies the ATM port(s) in the format: media.slot.port.vpi.vci. media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
priority		The priority can be applied in one of two ways. (1) The frame is assigned a priority within the switch, AND if the exit ports are trunk ports, the frame is assigned an 802.1Q priority. (2) The frame is assigned a priority within the switch. Select low, medium, high or control".
	<number>	Select a number from 0 to 7. The mapping of 802.1Q to internal priorities is the following: 1, 2 = low; 0, 3 = medium; 4, 5 = high; 6, 7 = control.
	low	The frame is assigned a low priority within the switch.
	medium	The frame is assigned a medium priority within the switch.

Parameter	Value	Meaning
	high	The frame is assigned a high priority within the switch.
	control	The frame is assigned control priority within the switch.
vlan-type		Specifies the type of VLAN.
	all	Specifies that the packets/cells received on all VLANs on the VC will be prioritized accordingly.
	ip	Specifies that the packets/cells received on IP VLANs on the VC will be prioritized accordingly.
	ipx	Specifies that the packets/cells received on IPX VLANs on the VC will be prioritized accordingly.
	l2	Specifies that the traffic that is classified as L2 will be prioritized accordingly.

Restrictions

None.

atm set vcl-qos

Mode

Configure

Format

```
atm set vcl-qos port <port-list> low <number> | medium <number> | high <number> | control  
<number> | relative-latency <number>
```

Description

The **atm set vcl qos** command sets parameters for the Weighted Fair Queueing (WFQ) QoS policy. It specifies how the VC's bandwidth is allocated to each traffic queue on the VC. For WFQ, specify percentages for all queues (low, medium, high, and control). For WFQ with Strict Priority, *do not* specify the percentage for the control queue.

Parameter	Value	Meaning
port	<port-list>	Specifies an ATM port or ports, including the virtual channel in the format: media.slot.port.vpi.vci . media Is the media type. This is always at for an ATM port. slot Is the slot number where the module is installed. port Is the number of the port through which data is passing. vpi Is the Virtual Path Identifier. vci Is the Virtual Channel Identifier.
low	<number>	Sets the percentage of the VC's available bandwidth that traffic in the low queue can use. The available bandwidth is what the VC can achieve minus that used by control packets. Enter a value between 10 and 80 inclusive.
medium	<number>	Sets the percentage of the VC's available bandwidth that traffic in the medium queue can use. The available bandwidth is what the VC can achieve minus that used by control packets. Enter a value between 10 and 80 inclusive.

Parameter	Value	Meaning
high	<number>	Sets the percentage of the VC's available bandwidth that traffic in the high queue can use. The available bandwidth is what the VC can achieve minus that used by control packets. Enter a value between 10 and 80 inclusive.
control	<number>	If a percentage is not specified, then the control queue gets all the bandwidth it needs, and the other queues (low, medium, and high) divide the remaining bandwidth according to their percentages. Enter a value between 10 and 80 inclusive.
relative-latency	<number>	By default, the QoS algorithm attempts to minimize latency at the expense of accuracy of the bandwidth allocation. By increasing this value, the bandwidth allocation becomes more accurate but the worst case latency increases. Setting a low value decreases worst case latency and bandwidth allocation accuracy. Enter a number between 1 and 100 inclusive. Note that the maximum value is dependent upon the values of the percentages specified for each queue. Though the CLI limits the maximum value to 100, this may actually be much less due to other limitations.

Restrictions

This command can be used only with the ATM multi-rate line card.

atm show port-settings

Mode

Enable

Format

atm show port-settings <*port list*>|all-ports

Description

The `atm show port-settings` command displays the characteristics of an ATM port.

Parameter	Value	Meaning
port-settings	< <i>port list</i> >	Specify the port using the following format: at.slot.port . Example: at.3.1 .
	all-ports	Specify all-ports to show characteristics of all ATM ports.

Restrictions

None.

Examples

The following example displays the settings for a port on an ATM multi-rate line card:

```
rs# atm-show port-settings at.9.1
Port information for Slot 9, Port 1:
  Port Type:          T3 ATM coaxial cable
  Xmt Clock Source:   Local
  Scramble Mode:      Payload
  Line Coding:        B3ZS
  Cell Mapping:       Direct
  Framing:            Cbit-Parity
  VC Mode:            1 bit of VPI, 11 bits of VCI
  Service Definition: user-default-OC3
    Service Class:     UBR
    Peak Bit Rate:     Best Effort
    Sustained Bit Rate: 0 Kbits/sec (0 cps)
    Maximum Burst Size: 0 cells
    Encapsulation Type: VC-MUX
    F5-OAM:            Requests & Responses
```

Table 6-1 Display field descriptions for the `atm show port-settings` command

Field	Description
Port Type	Shows the type of PHY interface for the port.
Xmt Clock Source	Shows the timing source for the port. Local indicates the on board clock oscillator as the timing source. Loop indicates the receiver input as the timing source.
Scramble Mode	Shows the scramble/descramble mode for the port. None indicates no scrambling. Payload indicates scrambling of the payload only. Frame indicates scrambling of the stream only. Both indicates scrambling of payload and stream.
Line Coding	Shows the particular DS3/T3 coding convention.
Cell Mapping	Shows the format used to map ATM cells. Direct indicates direct cell mapping. Plcp indicates physical layer convergence protocol mapping.

Table 6-1 Display field descriptions for the atm show port-settings command (Continued)

Field	Description
Framing	Shows the type of framing scheme. cbit-parity is used for T3 framing. m23 is used for T3 framing. esf indicates extended super frame and is used for T1 framing. g832 is used for E3 framing. g751 is used for E3 framing.
VC Mode	Shows the bit allocation for VPI and VCI.
Service Definition	Shows the name of the defined service on the port and its traffic parameters.

atm show ppp

Mode

Enable

Format

```
atm show ppp {port <port list> |all} {summary port <port list> |all}
```

Description

The **atm show ppp** command displays either detailed or summarized Point-to-Point (PPP) statistics on a port.

Parameter	Value	Meaning
port	<port list>	Specify at.slot.port to display all PPP statistics on the port. Specify at.slot.port.vpl to display all PPP statistics for a specified VPL. Specify at.slot.port.vpl.vcl to display PPP statistics only for the specified VCL on the port.
	all	Specify all to display verbose PPP statistics on all ports.

Restrictions

None.

Examples

To display PPP statistics:

```
rs# atm show ppp port all
-----
at.5.1:
Total LCP          (Enabled/Up): 0/0
Total IP           (Enabled/Up): 0/0
Total IPX          (Enabled/Up): 0/0
Total Bridging     (Enabled/Up): 0/0
Total Authentication (Enabled/Up): 0/0

Virtual Path Identifier:      1
Virtual Channel Identifier:   100
LCP Status:                  Disabled/Down
IP Status:                   Disabled/Down
IPX Status:                  Disabled/Down
Bridging Status:             Disabled/Down
Authentication Status:       Disabled/Down
Authentication Type:         None/None
-----
```

Table 6-2 Display field descriptions for the atm show ppp command

FIELD	DESCRIPTION
Total LCP	Indicates whether LCP is activated on the ATM port.
Total IP	Indicates whether IP is activated on the ATM port.
Total IPX	Indicates whether IPX is activated on the ATM port.
Total Bridging	Indicates whether bridging is activated on the ATM port.
Total Authentication	Indicates whether a PPP authentication scheme is activated.
Virtual Path Identifier	Identifies the VP for which PPP traffic statistics is displayed.
Virtual Channel Identifier	Identifies the VC for which PPP traffic statistics is displayed.
LCP Status	Indicates whether LCP is activated.
IP Status	Indicates whether IP is activated.
IPX Status	Indicates whether IPX is activated.

Table 6-2 Display field descriptions for the atm show ppp command (Continued)

FIELD		DESCRIPTION
Bridging	Status	Indicates whether bridging is activated.
Authentication	Status	Indicates whether a PPP authentication scheme is activated.
Authentication	Type	If PPP authentication was activated, this field displays the PPP authentication scheme: PAP or CHAP.

atm show service

Mode
Enable

Format

atm show service <service-name>|all

Description

The **atm show service** command displays the service profiles that were configured.

Parameter	Value	Meaning
service	<string>	Shows the profile for a specified service.
	all	Shows all ATM service profiles.

Restrictions

None.

Examples

To display information about all the defined service profiles for UBR:

```
rs# atm show service all

user-default-OC3
  Service Class:      UBR
  Peak Bit Rate:      Best Effort
  Sustained Bit Rate: 0 Kbits/sec (0 cps)
  Maximum Burst Size: 0 cells
  Encapsulation Type: VC-MUX
  F5-OAM:             Responses Only
```

Table 6-3 Display field descriptions for the atm show service command

Field	Descriptions
Service Class	Shows the type of service class. UBR indicates Unspecified Bit Rate CBR indicates Constant Bit Rate RT - VBR indicates Real-time Variable Bit Rate NRT - VBR indicates Non Real-time Variable Bit Rate
Peak Bit Rate	Shows the maximum bit transmission rate.
Sustained Bit Rate	Shows the average bit transmission rate (in Kilobits per second).
Maximum Burst Size	Shows how many cells can be transmitted at the Peak Bit Rate.
Encapsulation Type	Shows the encapsulation scheme to transport multi protocol data over the AAL5 layer. LLC - MUX indicates logical link control encapsulation (default). VC - MUX indicates VC-based multiplexing encapsulation.
F5 - OAM	Shows how OAM (Operation, Administration, and Management) loop back cells provide loop back capabilities and confirm whether a VC connection is up. Only F5 OAM segments are supported, which provides loop back capabilities on a VC connection level. Responses Only indicates that the port will respond but doesn't generate OAM cells. Requests & Responses indicates that the port will respond and generate OAM cells.

atm show stats

Mode
Enable

Format

atm show stats port *<port list>*

Description

The atm show stats command displays the traffic statistics of a virtual channel. Traffic statistics must first be enabled using the **atm set vcl traffic-stats-enable** command.

Parameter	Value	Meaning
port	<i><port list></i>	Specify at.slot.port.vpl to display traffic statistics for all VCL within a specified VPL. Specify at.slot.port.vpl.vcl to display traffic statistics only for the specified VCL.

Restrictions

None.

Examples

The following example displays the statistics for a port on an OC-12 line card. The output displays the statistics for each type of packet.

RS-8000# atm show stats port at.5.1.0.100		
PORT = 1, VPI = 0, VCI = 100		
	Received	Transmitted
	-----	-----
SAR statistics:		
Packets discarded	0	0
Packets Reassembled/Segmented	119	119
Received cells	119	119
AMAC statistics:		
Unicast	0	0
Multicast	0	0
Broadcast	0	0
Discarded	0	0 (includes sent to ACPU)
<64 bytes	0	0
63< <256	0	0
255< <1519	0	0
>1518	0	0
	Enabled	Up/Down
	-----	-----
OAM status	No	N/A
Statistics Cleared * Never Cleared *		

atm show vcgroup

Mode
Enable

Format

atm show vcgroup port <vc-group>|all

Description

The **atm show vcgroup** command displays virtual channel group statistics.

Parameter	Value	Meaning
port	<vc-group>	Specify a VC group in the following format: vg.group_index . For example, vg.100 .
	all	Specify all to display statistics for all VC groups.

Restrictions

None.

Examples

Following is an example of the output displayed by the **atm show vcgroup** command.

RS-8000# atm show vcgroup port vg.100										
Port		Control		High		Medium		Low		Bcast
		Vpi	Vci	Vpi	Vci	Vpi	Vci	Vpi	Vci	
vg.100	Conf	0	0	0	0	1	100	2	100	
vg.100	Actv	0	0	0	0	0	0	0	0	

Table 6-4 Display field descriptions for the atm show vcgroup command

FIELD	DESCRIPTION
Port	The VC group for which statistics are displayed.
Control	The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) of the VC in the control queue.
High	The VPI and VCI of the VC in the high queue.
Medium	The VPI and VCI of the VC in the medium queue.

Table 6-4 Display field descriptions for the atm show vcgroup command

FIELD	DESCRIPTION
Low	The VPI and VCI of the VC in the low queue.
Bcast	The VPI and VCI of the broadcast VC .

atm show vcl

Mode

Enable

Format

```
atm show vcl {port <port list>|all} {summary port <port list>|all}
```

Description

The **atm show vcl** command displays either detailed or summarized VCL configuration information on a port.

Parameter	Value	Meaning
port	<port list>	Specify at.slot.port to display all VCLs configurations on the port.
		Specify at.slot.port.vpl to display all VCL configurations for a specified VPL.
		Specify at.slot.port.vpl.vcl to display only the specified VCL configuration on the port.
	all	Specify all to display VCL configurations on all ports.

Restrictions

None.

Examples

To display VCL configuration information for port at.7.1.1.100:

```
RS-8000# atm show vcl port at.7.1.1.100
at.7.1:
  Virtual Path Identifier:    1
  Virtual Channel Identifier: 100
  MAC Address Limit:         No Limit
  QoS Settings:              C: Strict H: 55% M: 25% L: 20%, Rel.
  Latency: 3
  QoS Burst Settings:        C: 4800 H: 4800 M: 4800 L: 4800
  Priority Settings:          L2: 6 IP: 6 IPX: 6
  Cross Connect:             None
  Force Bridge Format:        Disabled
  AAL:                       AAL 5
  Administrative Status:      Up
  Operational Status:         Down
  Last State Change:          158651
  Service Definition:         default-OC3
    Service Class:            UBR
    Peak Bit Rate:            Best Effort
    Encapsulation Type:       LLC Multiplexing
    Traffic Type:             RFC-1483, multi-protocol
    F5-OAM:                   Responses Only
```

Table 6-5 Display field descriptions for the atm show vcl command

FIELD	DESCRIPTION
Virtual Path Identifier	The virtual path identifier that, together with the VCI (Virtual Channel Identifier), defines the virtual channel.
Virtual Channel Identifier	The virtual channel identifier that, together with the Virtual Path Identifier (VPI), defines the virtual channel.
MAC Address Limit	The maximum number of MAC addresses the VC can learn. This is configured through the atm set vcl mac-addr-limit command.
QoS Settings	The QoS policy, the latency value, and the percentages configured for each queue. This is configured through the atm set vcl-qos command.
Priority Settings	The VC priority settings as configured through the atm set vcl-priority command.
Cross Connect	If cross-connects were configured, the port on the other end of the cross-connect.

Table 6-5 Display field descriptions for the atm show vcl command

FIELD	DESCRIPTION
Force Bridge Format	Displays whether forced-bridge mode was enabled.
AAL	Displays whether the VC sends and receives AAL1 cells or AAL5 packets.
Administrative Status	Shows whether the VC is a viable network element. • Up indicates a viable network element • Down indicates a non-viable network element
Operational Status	Shows whether the VC is passing traffic. • Up indicates traffic • Down indicates no traffic
Last State Change	Shows the last time the VC went up or down. Time is in seconds relative to system bootup.
Service Definition	The service profile that was defined through the atm define service command.
Service Class	The service class that was defined through the atm define service command.
Peak Bit Rate	The maximum cell transmission rate expressed in kbits/second.
Encapsulation Type	The encapsulation used as defined through the atm define service command.
Traffic Type	The format of the traffic the VC carried. This is configured through the atm define service command.
F5-OAM	Identifies whether OAM is off or on. This is set through the atm define service command.

atm show vpl

Mode

Enable

Format

```
atm show vpl {port <port list>|all} {summary port <port list>|all}
```

Description

The **atm show vpl** command displays either detailed or summary VPL configuration information for a specified port.

Parameter	Value	Meaning
port	<port list>	Specify at.slot.port to display all VPL configurations on the port.
		Specify at.slot.port.vpl to display only the specified VPL configuration on the port.
		Specify summary to display summarized VPL configuration in tabular form.
	all	Specify all to display VPL configurations on all ports.

Restrictions

None.

Examples

To display information about the VPL configurations on ATM port at.9.1:

```
rs# atm show vpl port at.9.1

VPL Table Contents for Slot 9, Port 1:
  Virtual Path Identifier: 1
  Administrative Status:   Up
  Operational Status:     Up
  Last State Change:      1581
  Service Definition:      user-default-OC3
    Service Class:         UBR
    Peak Bit Rate:         Best Effort
    Sustained Bit Rate:    0 Kbits/sec (0 cps)
    Maximum Burst Size:    0 cells
    Encapsulation Type:    VC-MUX
    F5-OAM:                Requests & Responses
```

Table 6-6 Display field descriptions for the atm show vpl command

Field	Description
Virtual Path Identifier	Identifies a particular VP.
Administrative Status	Shows whether the VP is a viable network element. Up indicates a viable network element. Down indicates a non-viable network element.
Operational Status	Shows whether the VP is passing traffic. Up indicates traffic. Down indicates no traffic.
Last State Change	Shows the last time the VP went up or down. Time is in seconds relative to system bootup.
Service Definition	Shows the name of the defined service and its traffic parameters

7 BGP COMMANDS

The BGP commands let you display and set parameters for the Border Gateway Protocol (BGP).

7.1 COMMAND SUMMARY

The following table lists the BGP commands. The sections following the table describe the command syntax

<code>bgp add peer-host <ipaddr> group <number-or-string></code>
<code>bgp clear flap-statistics <ipaddr-mask> all longer-prefixes</code>
<code>bgp clear peer-host <ipaddr> all soft-inbound</code>
<code>bgp create peer-group <number-or-string></code>
<code>bgp set DampenFlap <option></code>
<code>bgp set default-localpref <num></code>
<code>bgp set default-metric <num></code>
<code>bgp set cluster-id <ipaddr></code>
<code>bgp set multipath off</code>
<code>bgp set peer-group <number-or-string> <option></code>
<code>bgp set peer-host <ipaddr> <option></code>
<code>bgp set preference <num></code>
<code>bgp show aspath-regular-expression <regex> all</code>
<code>bgp show aspaths all</code>
<code>bgp show cidr-only <ip-addr-mask> default all</code>
<code>bgp show community community-id <number> autonomous-system <number> well-known-community [no-export no-advertise no-export-subconfed] reserved-community <number>]</code>
<code>bgp show community-list <name> all</code>
<code>bgp show flap-statistics [<ip-addr-mask> all damped history] longer-prefixes</code>
<code>bgp show neighbor <ip-addr-mask> all</code>
<code>bgp show peer-as <number></code>

bgp show peer-group-type external internal igp routing
bgp show peer-host <ipaddr> received-routes all-received-routes advertised-routes
bgp show regexp
bgp show routes <ip-addr-mask> default all longer-prefixes
bgp show summary
bgp show sync-tree
bgp start stop
bgp trace <option>

bgp add peer-host

Mode
Configure

Format

bgp add peer-host <ipaddr> group <number-or-string>

Description

The **bgp add peer-host** command adds a peer-host to a BGP group.

Parameter	Value	Meaning
peer-host	<ipaddr>	Specifies the peer host's IP address.
group	<number-or-string>	Specifies the group ID of the group to which the peer host belongs.

Restrictions

None.

bgp clear flap-statistics

Mode

Configure

Format

```
bgp clear flap-statistics <ip-addr-mask>|all longer-prefixes
```

Description

The **bgp clear peer-host** command clears flapping and suppressed route information for the specified route(s).

Parameter	Value	Meaning
flap-statistics	<ip-addr-mask>	Specifies the IP address and subnet of the route.
	all	Clears all route dampening history
	longer-prefixes	Clears route dampening history for the route specified by the entered IP address and subnet mask, as well as all other routes with longer subnet masks.

Restrictions

None

bgp clear peer-host

Mode

Configure

Format

```
bgp clear peer-host <ipaddr>|all soft-inbound
```

Description

The **bgp clear peer-host** command is used to refresh the routing database of the RS with respect to the specified peer-host. If this command is used without the **soft-inbound** option, routing information from the specified peer-host is obtained by breaking the connection to the peer-host. When the connection is reestablished, the peer-host sends its routing information to the RS. If the **soft-inbound** option is used, the connection to the peer-host remains intact. Instead, **soft-inbound** signals the specified peer-host to re-send its routing information.

**Note**

Without using the **soft-inbound** option, routing will not resume until the connection(s) is reestablished and all route database information is updated.

Parameter	Value	Meaning
peer-host	<ipaddr>	Specifies the peer-host's IP address.
	all	Specifies all peer-hosts connected to the RS.
	soft-inbound	Requests the specified peer-host(s) to re-send their routing information without breaking the connection with the peer-host(s).

Restrictions

In order to use the **soft-inbound** option, the **bgp set peer-host/peer-group route refresh** command must be entered and in the active configuration.

Some earlier versions of BGP do not support the functionality of **soft-inbound**. In this case, the connection to the peer-host must be broken in order for routing information exchange to occur.

bgp create peer-group

Mode

Configure

Format

```
bgp create peer-group <number-or-string> type external|routing [autonomous-system <number>]  
[proto any|rip|ospf|static] [interface <interface-name-or-ipaddr> |all]
```

Description

The **bgp create peer-group** command creates a BGP group based on type or the autonomous system of the peers. You can create any number of groups, but each group must have a unique combination of type and peer autonomous system.

Parameter	Value	Meaning
peer-group	<number-or-string>	Is a group ID, which can be a number or a character string.
type		Specifies the type of BGP group you are adding
	external	In the classic external BGP group, full policy checking is applied to all incoming and outgoing advertisements. The external neighbors must be directly reachable through one of the machine's local interfaces.
	routing	An internal group which uses the routes of an interior protocol to resolve forwarding addresses. Type routing groups will determine the immediate next hops for routes by using the next hop received with a route from a peer as a forwarding address, and using this to look up an immediate next hop in an IGP's routes. Such groups support distant peers, but need to be informed of the IGP whose routes they are using to determine immediate next hops. This implementation comes closest to the IBGP implementation of other router vendors.
autonomous-system	<number>	Specifies the autonomous system of the peer group. Specify a number from 1 to 65535.
proto		Specifies the interior protocol to be used to resolve BGP next hops.
	any	Use any igp to resolve BGP next hops.
	rip	Use RIP to resolve BGP next hops.
	ospf	Use OSPF to resolve BGP next hops.
	ospf-ase	Use OSPF ASE to resolve BGP next hops.
	static	Use static to resolve BGP next hops.

Parameter	Value	Meaning
interface	<name-or-IPaddr>	Interfaces whose routes are carried via the IGP for which third-party next hops may be used instead. Use only for type ROUTING group.
	all	Specifies all interfaces.

Restrictions

None.

bgp set cluster-id

Mode

Configure

Format

```
bgp set cluster-id <ipaddr>
```

Description

The **bgp set cluster-id** command specifies the route reflection cluster ID for BGP. The cluster ID defaults to the same as the router-id. If a router is to be a route reflector, then a single cluster ID should be selected and configured on all route reflectors in the cluster. If there is only one route reflector in the cluster, the cluster ID setting may be omitted, as the default will suffice.

Parameter	Value	Meaning
cluster-id	<ipaddr>	Is the cluster ID.

Restrictions

The only constraints on the choice of cluster ID are (a) IDs of clusters within an AS must be unique within that AS, and (b) the cluster ID must not be 0.0.0.0. Choosing the cluster ID to be the router ID of one router in the cluster will always fulfill these criteria.

bgp set compare-MED

Mode

Configure

Format

bgp set compare-MED always|confed

Description

By default, the MED attribute from different autonomous systems is *not* compared. The **bgp set compare-MED** command allows you to specify whether the MED attribute should *always* be compared or only compared when two routes are from the same BGP confederation.

Parameter	Value	Meaning
compare-MED	always	MED attribute is always compared.
	confed	MED attribute is compared only if two routes are from the same BGP confederation.

Restrictions

None.

bgp set dampenflap

Mode

Configure

Format

```
bgp set dampenflap [state enable|disable][route-map <num>|<string>][suppress-above
<num>][reuse-below <num>][max-flap <num>][unreach-decay <num>][reach-decay
<num>][keep-history <num>]
```

Description

The **bgp set dampenflap** command configures the state of Weighted Route Dampening.

Parameter	Value	Meaning
state		Causes the Route Instability History to be maintained (enable option) or not (disable option).
	enable	Causes the Route Instability History to be maintained.
	disable	Causes the Route Instability History to not be maintained.
route-map	<num> <string>	Name of route-map to carry specified dampening parameters. If no route-map is specified, the global dampening values are changed.
suppress-above	<num>	Is the value of the instability metric at which route suppression will take place. A route will not be installed in the FIB or announced even if it is reachable during the period that it is suppressed. The default is 3.0.
reuse-below	<num>	Is the value of the instability metric at which a suppressed route will become unsuppressed, if it is reachable but currently suppressed. The value must be less than that for the suppress-above option. The default is 2.0.
max-flap	<num>	Is the upper limit of the instability metric. This value must be greater than the larger of 1 and that for suppress-above. The default is 16.0.
unreach-decay	<num>	Specifies the time in seconds for the instability metric value to reach one-half of its current value when the route is <i>unreachable</i> . This half-life value determines the rate at which the metric value is decayed. The default is 900.

Parameter	Value	Meaning
reach-decay	<num>	Specifies the time in seconds for the instability metric value to reach one half of its current value when the route is <i>reachable</i> . This half-life value determines the rate at which the metric value is decayed. A smaller half-life value will make a suppressed route reusable sooner than a larger value. The default is 300.
keep-history	<num>	Specifies the period in seconds over which the route flapping history is to maintained for a given route. The size of the configuration arrays is directly affected by this value. The default is 1800.

Restrictions

None.

bgp set default-localpref

Mode

Configure

Format

```
bgp set default-localpref <num>
```

Description

The **bgp set default-localpref** command sets the default local preference value for EBGp routes. Note that EBGp routes do not normally have a preference value. However, if necessary for route computations that include EBGp routes, a value can be assigned.

Parameter	Value	Meaning
default-localpref	<number>	Sets a local preference number for EBGp routes. Value can be any number between 0 and 65535, the default is 100.

Restrictions

None.

bgp set default-metric

Mode

Configure

Format

bgp set default-metric *<num>*

Description

The **bgp set default-metric** command lets you set the default metric BGP uses when it advertises routes. If this command is not specified, no metric is propagated. This metric may be overridden by a metric specified on the neighbor or group statements or in an export policy.

Parameter	Value	Meaning
default-metric	<i><num></i>	Specifies the default cost. Specify a number from 0 - 65535.

Restrictions

None.

bgp set multipath

Mode

Configure

Format

```
bgp set multipath off
```

Description

The **bgp set multipath** command disables multipath route calculation for BGP routes. No multipath forwarding occurs as a result of this command. Multipath route calculation is enabled by default.

Parameter	Value	Meaning
multipath	off	Disables multipath route calculation for BGP routes.

Restrictions

None.

bgp set peer-group

Mode

Configure

Format

```
bgp set peer-group <number-or-string> [no-med|reflector-client|no-client-reflect|
[confederation][metric-out <num>]][set-pref <num>] [local-pref <num>] [local-as
<num>][ignore-first-as-hop][generate-default enabled|disabled]][gateway|multihop]
|next-hop-self|[preference <num>][preference2 <num>][local-address <ipaddr>]|
[hold-time <num>]][route-map-in <route-map-id> [in-sequence <seq-num>]]|route-map-out
<route-map-id> [out-sequence <seq-num>]]|[version 4]|passive|[send-buffer
<num>]][recv-buffer <num>]][in-delay <num>]][out-delay <num>]][keep all|none]|
show-warnings|no-aggregator-id|keep-alives-always|v3-asloop-okay| no-v4-asloop|
[as-count <num>]][log-up-down][ttl <num>]][password <password>]] [delete-policy-rejects]
[optional-attributes-list <number-or-string>]][no-route-refresh]
```

Description

The **bgp set peer-group** command sets parameters for the specified BGP group.

Parameter	Value	Meaning
peer-group	<number-or-string>	Specifies the group.
no-med		Forces MED not to be used for route selection process. By default, any metric (Multi_Exit_Disc, or MED) received on a BGP connection is used in route selection. If it is desired not to use MEDs in route selections, the no-med option must be specified in this (create peer-group) command. By default, MEDs are sent on external connections. To send MEDs, use the metric option of the create bgp-export-destination statement or the metric-out option of the set peer-group or set peer-host commands.
reflector-client		The reflector-client option specifies that ROSRD will act as a route reflector for this group. All routes received from any group member will be sent to all other internal neighbors, and all routes received from any other internal neighbors will be sent to the reflector clients. Since the route reflector forwards routes in this way, the reflector-client group need not be fully meshed. Use only for INTERNAL and ROUTING groups.

Parameter	Value	Meaning
no-client-reflect		If the no-client-reflect option is specified, routes received from reflector clients will only be sent to internal neighbors which are not in the same group as the sending reflector client. In this case the reflector-client group should be fully meshed. In all cases, routes received from normal internal peers will be sent to all reflector clients.
 Note It is necessary to export routes from the local AS into the local AS when acting as a route reflector. The reflector-client option specifies that ROSRD will act as a route reflector for this group. All routes received from any group member will be sent to all other internal neighbors, and all routes received from any other internal neighbors will be sent to the reflector clients. Since the route reflector forwards routes in this way, the reflector-client group need not be fully meshed.		
confederation		Set this parameter for all groups in the same confederation.
metric-out	<num>	Specifies the primary metric used on all routes sent to the specified peer group. Specify a number from 0 - 65535.
set-pref	<num>	Routes propagated by IBGP must include a Local_Pref attribute. By default, BGP sends the Local_Pref path attribute as 100, and ignores it on receipt. ROSRD BGP does not use Local_Pref as a route-preference decision maker unless the setpref option has been set. For Routing- or Internal-type groups, the setpref option allows ROSRD's global protocol preference to be exported into Local_Pref and allows Local_Pref to be used for ROSRD's route selection preference. Note that the setpref option is the only way for ROSRD to send a route with a given local_pref. The local_pref is never set directly, but rather as a function of the ROSRD preference and setpref metrics. Allows BGP's LOCAL_PREF attribute to be used to set the ROSRD preference on reception, and allows the ROSRD preference to set the LOCAL_PREF on transmission. The set-pref metric works as a lower limit, below which the imported LOCAL_PREF may not set the ROSRD preference. Use only for INTERNAL and ROUTING groups. Specify a number from 0-255.
local-pref	<num>	Sets the BGP LOCAL_PREF attribute. Use for only INTERNAL and ROUTING groups. Specify a number from 1 - 65535.

Parameter	Value	Meaning
local-as	<num>	Identifies the autonomous system which the router is representing to this group of peers. The default is the one configured by the ip-router global set autonomous_system command. Specify a number from 1 to 65535.
ignore-first-as-hop		Some routers, known as Route Servers, are capable of propagating routes without appending their own AS to the AS path. By default, ROSRD will drop such routes. Specifying ignore-first-as-hop here or on either the create peer-group or set peer-host CLI commands disables this feature. This option should only be used if it is positively known that the peer is a route server and not a normal router.
generate-default		Specifies whether the router should generate a default route when BGP receives a valid update from its peer. If this option is not specified, then the generation of default route is enabled.
	enabled	Enables the generation of default routes.
	disabled	Disables the generation of default routes.
gateway multihop		If a network is not shared with a peer, this option specifies a router on an attached network to be used as the next hop router for routes received from this neighbor. This field is used for EBGp Multihop.
 Note The gateway option is supported for compatibility with earlier software releases; this option will be phased out at a later release.		
next-hop-self		This option causes the next hop in route advertisements set to this peer or group of peers to be set to our own router's address even if it would normally be possible to send a third-party next hop. Use of this option may cause efficient routes to be followed, but it may be needed in some cases to deal with broken bridged interconnect media (in cases where the routers on the shared medium do not really have full connectivity to each other) or broken political situations.
preference	<num>	Specifies the preference used for routes learned from these peers. Specify a number from 0 - 255.
preference2	<num>	In case of a preference tie, this option (the second preference), may be used to break the tie. The default value is 0. Specify a number from 0 - 255.

Parameter	Value	Meaning
local-address	<ipaddr>	Specifies the address to be used on the local end of the TCP connection with the peer or with the peer's gateway when the gateway option is used. A session with an external peer will only be opened when an interface with the appropriate local address (through which the peer or gateway address is directly reachable). In either case incoming connections will only be recognized as matching a configured peer if they are addressed to the configured local address. Use only for INTERNAL and ROUTING groups. <i>It should be one of the interface addresses.</i>
hold-time	<num>	Specifies the hold time value to use when negotiating the connection with this peer, in seconds. If BGP does not receive a keepalive, update, or notification message from a peer within the period specified in the Hold Time field of the BGP Open message, then the BGP connection will be closed. The value must be either 0 (no keepalives will be sent) or at least 6.
route-map-in	<route-map-id>	Identifier of the route-map to be applied while importing routes from this peer group. This can be overridden using the bgp set peer-host route-map-in command.
in-sequence	<seq-num>	The sequence in which route-map-in is applied.
route-map-out	<route-map-id>	Identifier of the route-map to be applied while exporting routes to this peer group. This can be overridden using the bgp set peer-host route-map-out command.
out-sequence	<seq-num>	The sequence in which route-map-out is applied.
version	4	Specifies version 4 of the BGP protocol to use with this peer.
passive		Specifies that active OPENs to this peer should not be attempted. BGP would wait for the peer to issue an OPEN. By default, all explicitly configured peers are active, they periodically send OPEN messages until the peer responds. Note that if it is applied to both sides of a peering session, it will prevent the session from ever being established.
send-buffer	<num>	Controls the amount of send buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 – 65535.

Parameter	Value	Meaning
recv-buffer	<num>	Controls the amount of receive buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 – 65535.
in-delay	<num>	Used to dampen route fluctuations. In delay specifies the amount of time in secs a route learned from a BGP peer must be stable before it is accepted into the routing database. Specify a number equal to or greater than 0. The default value is 0, meaning that this feature is disabled.
out-delay	<num>	Used to dampen route fluctuations. Out delay is the amount of time in secs a route must be present in the routing table before it is exported to BGP. Specify a number equal to or greater than 0. The default value is 0, meaning that this feature is disabled.
keep		Used to retain routes learned from a peer even if the routes' AS paths contain one of our exported AS numbers.
	all	Retain all learned routes from a peer.
	none	Do not retain learned routes from a peer.
show-warnings		This option causes ROSRD to issue warning messages when receiving questionable BGP updates such as duplicate routes and/or deletions of non-existing routes. Normally these events are silently ignored.
no-aggregator-id		This option causes ROSRD to specify the router ID in the aggregator attribute as zero (instead of its router ID) in order to prevent different routers in an AS from creating aggregate routes with different AS paths.
keep-alives-always		This option causes ROSRD to always send keepalives, even when an update could have correctly substituted for one. This allows interoperability with routers that do not completely obey the protocol specifications on this point.
v3-as-loop-okay		By default ROSRD will not advertise routes whose AS path is looped (i.e. with an AS appearing more than once in the path) to version 3 external peers. Setting this flag removes this constraint. Ignored when set on internal groups or peers.
no-v4-as-loop		Prevents routes with looped AS paths from being advertised to version 4 external peers. This can be useful to avoid advertising such routes to peer which would incorrectly forward the routes on to version 3 neighbors.

Parameter	Value	Meaning
as-count	<num>	This option determines how many times the RS will insert its own AS number when sending the AS path to an external neighbor. Specify a number between 1 and 25. The default is 1. Higher values typically are used to bias upstream neighbors' route selection. (All else being equal, most routers will prefer to use routes with shorter AS Paths. Using as-count , the AS Path the RS sends can be artificially lengthened.)
 Note as-count supersedes the no-v4-asloop option—regardless of whether no-v4-asloop is set, we will still send multiple copies of our own AS if the as-count option is set to something greater than one. Also, note that if the value of as-count is changed and ROSRD is reconfigured, routes will not be sent to reflect the new setting. If this is desired, it will be necessary to restart the peer session.		
log-up-down		This option causes a message to be logged whenever a BGP peer enters or leaves the ESTABLISHED state.
ttl	<num>	By default, BGP sets the IP TTL for local peers to ONE and the TTL for non-local peers to 255. This option is provided when attempting to communicate with improperly functioning routers that ignore packets sent with a TTL of ONE. Specify a number between 1 and 255.
password	<password>	Specifies the password for MD5 access to a peer group. Password is case-sensitive and can be 80 characters or less.
delete-policy-rejects		Deletes routes learned from a peer but rejected by a policy.
optional-attributes-list	<number-or-string>	Specifies the ID of the optional-attributes-list to be associated with this peer-group.
no-route-refresh		Allows turning off the route-refresh function for purposes of compatibility with older versions of BGP. By default, BGP advertises to the peer-group the ability to accept route database refreshes without breaking and reestablishing the connection with the peer-group. This option must be active to use the soft-inbound option with the bgp clear peer-host command.

Restrictions

None.

bgp set peer-host

Mode

Configure

Format

```
bgp set peer-host <ipaddr> [group <number-or-string>|[metric-out <num>]] [set-pref
<num>][local-as <num>]|ignore-first-as-hop| [generate-default enabled|disabled]]
[gateway | multihop]|next-hop-self| [preference <num>][preference2 <num>][local-address
<ipaddr>]] [hold-time <num>]][route-map-in <route-map-id> [in-sequence <seq-num>]]|
[route-map-out <route-map-id> [out-sequence <seq-num>]]|[version 4]|passive|
[send-buffer <num>]] [recv-buffer <num>]][in-delay <num>]][out-delay <num>]][keep
all|none]| show-warnings|no-aggregator-id|keep-alives-always|v3-asloop-okay|
no-v4-asloop|[as-count <num>]][log-up-down]][ttl <num>]] [password <password>] |
[max-prefixes] [max-prefixes-reset-session] [max-prefixes-threshold]
[max-prefixes-warn-only] [delete-policy-rejects][optional-attributes-list
<number-or-string>] [shutdown] [max-prefix-len <length>]] [no-route-refresh]
```

Description

The **bgp set peer-host** command lets you set various parameters for the specified BGP peer hosts.

Parameter	Value	Meaning
peer - host	<ipaddr>	Specifies the peer host.
group	<number-or-string>	Specifies the group ID.
metric-out	<num>	Specifies the primary metric used on all routes sent to the specified peer group. The metric hierarchy is as follows, starting from the most preferred: 1) The metric specified by export policy. 2) Peer-level metricout. 3) Group-level metricout 4) Default metric. For INTERNAL and ROUTING hosts use the group command to set the metric-out. Specify a number from 0 - 65535.
set-pref	<num>	Allows BGP's LOCAL_PREF attribute to be used to set the ROSRD preference on reception, and allows the ROSRD preference to set the LOCAL_PREF on transmission. The set-pref metric works as a lower limit, below which the imported LOCAL_PREF may not set the ROSRD preference. For ROUTING hosts, use the group command to set the metric-out. Specify a number from 0 - 255. This parameter applies only to ROUTING hosts only.

Parameter	Value	Meaning
local-as	<num>	Identifies the autonomous system which the router is representing to this group of peers. The default is the one configured using the <code>ip-router global set autonomous_system</code> command. Specify a number from 1 to 65535.
ignore-first-as-hop		Some routers, known as Route Servers, are capable of propagating routes without appending their own AS to the AS path. By default, ROSRD will drop such routes. Specifying <code>ignore-first-as-hop</code> here or on either the <code>create peer-group</code> or set peer-host CLI commands disables this feature. This option should only be used if it is positively known that the peer is a route server and not a normal router.
generate-default		Specifies whether the router should generate a default route when BGP receives a valid update from its peer. If this option is not specified, then the generation of default route is enabled.
	enabled	Generates a default route when BGP receives a valid update.
	disabled	Does not generate a default route when BGP receives a valid update.
gateway multihop		If a network is not shared with a peer, this option specifies a router on an attached network to be used as the next hop router for routes received from this neighbor. This is used for EBGp multihop.
 Note The gateway option is supported for compatibility with earlier software releases; this option will be phased out at a later release.		
next-hop-self		This option causes the next hop in route advertisements set to this peer or group of peers to be set to our own router's address, even if it would normally be possible to send a third-party next hop. Use of this option may cause inefficient routes to be followed, but it may be needed in some cases to deal with broken bridged interconnect media (in cases where the routers in the shared medium do not really have full connectivity to each other) or broken political situations. <i>Use only for external peer hosts.</i>

Parameter	Value	Meaning
preference	<num>	Specifies the preference used for routes learned from these peers. This can differ from the default BGP preference set in the <code>bgp set preference</code> statement, so that ROSRD can prefer routes from one peer, or group of peer, over others. This preference may be explicitly overridden by import policy. Specify a number from 0 - 255.
preference2	<num>	In case of preference tie, this option (the second preference), may be used to break the tie. The default value is 0. Specify a number from 0 - 255.
local-address	<ipaddr>	Specifies the address to be used on the local end of the TCP connection with the peer or with the peer's gateway when the gateway option is used. A session with an external peer will only be opened when an interface with the appropriate local address (through which the peer or gateway address is directly reachable). In either case incoming connections will only be recognized as matching a configured peer if they are addressed to the configured local address. For ROUTING hosts use the group command to set the local-address. <i>It should be one of the interface addresses.</i>
hold-time	<num>	Specifies the hold time value to use when negotiating the connection with this peer, in seconds. If BGP does not receive a keepalive, update, or notification message from a peer within the period specified in the Hold Time field of the BGP Open message, then the BGP connection will be closed. The value must be either 0 (no keepalives will be sent) or at least 6.
route-map-in	<route-map-id>	Identifier of the route-map to be applied while importing routes from this peer host.
in-sequence	<seq-num>	The sequence in which route-map-in is applied.
route-map-out	<route-map-id>	Identifier of the route-map to be applied while exporting routes to this peer host.
 Note You can set parameters using route-map on export to EBGp peers but not to IBGP peers. If you need to control the export of routes to specific peers, create a peer-group for each of the peers (with one peer-group per peer), and define a group-specific policy.		
out-sequence	<seq-num>	The sequence in which route-map-out is applied.
version	4	Specifies version 4 of the BGP protocol to use with this peer.

Parameter	Value	Meaning
passive		Specifies that active OPENs to this peer should not be attempted. BGP would wait for the peer to issue an OPEN. By default, all explicitly configured peers are active, they periodically send OPEN messages until the peer responds. Note that if it is applied to both sides of a peering session, it will prevent the session from ever being established.
send-buffer	<num>	Controls the amount of send buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 - 65535.
recv-buffer	<num>	Controls the amount of receive buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 – 65535.
in-delay	<num>	Used to dampen route fluctuations. In delay specifies the amount of time in secs a route learned from a BGP peer must be stable before it is accepted into the routing database. The default value is 0, meaning that this feature is disabled. Specify a number equal to or greater than 0.
out-delay	<num>	Used to dampen route fluctuations. Out delay is the amount of time in secs a route must be present in the routing table before it is exported to BGP. The default value is 0, meaning that this feature is disabled. Specify a number equal to or greater than 0. For INTERNAL and ROUTING hosts, use the group command to set out-delay .
keep		Used to retain routes learned from a peer even if the routes' AS paths contain one of our exported AS numbers.
	all	Retain all routes learned from a peer.
	none	Doesn't retain routes learned from a peer.
show-warnings		This option causes ROSRD to issue warning messages when receiving questionable BGP updates such as duplicate routes and/or deletions of non-existing routes. Normally these events are silently ignored.
no-aggregator-id		This option causes ROSRD to specify the router ID in the aggregator attribute as zero (instead of its router ID) in order to prevent different routers in an AS from creating aggregate routes with different AS paths.

Parameter	Value	Meaning
keep-alives-always		This option causes ROSRD to always send keepalives, even when an update could have correctly substituted for one. This allows interoperability with routers that do not completely obey the protocol specifications on this point.
v3-as loop-okay		By default ROSRD will not advertise routes whose AS path is looped (i.e. with an AS appearing more than once in the path) to version 3 external peers. Setting this flag removes this constraint. Ignored when set on internal groups or peers.
no-v4-as loop		Prevents routes with looped AS paths from being advertised to version 4 external peers. This can be useful to avoid advertising such routes to peer which would incorrectly forward the routes on to version 3 neighbors.
as-count	<num>	This option determines how many times we will insert our own AS number when we send the AS path to an external neighbor. Specify a number equal to or greater than 0. The default is 1. Higher values are typically used to bias upstream neighbors' route selection. (All things being equal most routers will prefer to use routes with shorter AS Paths. Using ascount, the AS Path the RS sends can be artificially lengthened.)
 Note Ascount supersedes the no-v4-as loop option--regardless of whether no-v4-as loop is set, the RS will still send multiple copies its own AS if the as-count option is set to something greater than one.		
 Note Also, note that if the value of ascount is changed and ROSRD is reconfigured, routes will not be sent to reflect the new setting. If this is desired, it will be necessary to restart the peer session. Use only for external peer_hosts. Specify a number from 1-25.		
log-up-down		Causes a message to be logged via the SYSLOG mechanism whenever a BGP peer enters or leaves the ESTABLISHED state.
ttl	<num>	By default, BGP sets the IP TTL for local peers to ONE and the TTL for non-local peers to 255. This option is provided when attempting to communicate with improperly functioning routers that ignore packets sent with a TTL of ONE. Specify a number from 1-255.

Parameter	Value	Meaning
password	<password>	Specifies the password for MD5 access to a peer host. Password is case sensitive and can be 80 characters or less.
max-prefixes	<number>	Specifies the maximum number of routes to accept from an external BGP peer. Specify a number from 0-150000.
max-prefixes-reset-session		This option resets the session to the peer when max-prefixes is exceeded. The default action is to drop the routes.
max-prefixes-threshold	<number>	Used with the max-prefixes-warn-only keyword. This parameter specifies a percentage of the max-prefixes value which, if reached, causes a warning to appear. Specify a number from 1-100. For example, if max-prefixes is 10000 and max-prefixes-threshold is 80, and max-prefixes-warn-only is set, then a warning will appear when 8000 routes are accepted from an external BGP peer.
max-prefixes-warn-only		Causes a warning message to appear when the max-prefixes-threshold number is exceeded. The default action is to drop the routes.
delete-policy-rejects		Deletes routes learned from a peer but rejected by a policy.
optional-attributes-list	<number-or-string>	Specifies the ID of the optional-attributes-list to be associated with this peer-group.
shutdown		Specifies that this peer should not be brought up.
max-prefix-len	<length>	Specifies the maximum length of the prefix that will be accepted from this peer. If the prefix length exceeds this value, prefixes received from the peer will not be added to the routing table. Specify a number from 1-32.
no-route-refresh		Allows turning off the route-refresh function for purposes of compatibility with older versions of BGP. By default, BGP advertises to the peer-host the ability to accept route database refreshes without breaking and reestablishing the connection with the peer-host. This option must be active to use the soft-inbound option with the bgp clear peer-host command.

Restrictions

None.

bgp set preference

Mode

Configure

Format

bgp set preference <num>

Description

The **bgp set preference** command lets you set the BGP preference for the RS.

Parameter	Value	Meaning
preference	<num>	Specifies the preference of routes learned from BGP. Specify a number from 0 -255. The default preference is 170.

Restrictions

None.

bgp show aspath-regular-expression

Mode
Enable

Format

bgp show aspath-regular-expression <regex>|all

Description

The **bgp show aspath-regular-expression** command displays configuration information for a specified AS path regular expression or all AS path regular expressions.

Parameter	Value	Meaning
aspath-regular-expression	<regex>	Displays configuration information for the specified AS path regular expression.
	all	Displays configuration information about all AS path regular expressions.

Restrictions

None.

Example

To display all configured AS path regular expressions:

```
rs# bgp show aspath-regular-expression all
Name          Regular Expression
====          =====
aa
              (1 2)
              (1 .*)
bb
              ((1 2)|(3 4))
              (5 6)
```

Name is the identifier of the AS path regular expression list.

Regular Expression is the list of AS path regular expressions.

To display configured AS path regular expressions for the list 'bb':

```
rs# bgp show aspath-regular-expression bb
Name          Regular Expression
====          =====
bb
              ((1 2)|(3 4))
              (5 6)
```

bgp show aspaths

Mode
Enable

Format

bgp show aspaths all

Description

The **bgp show aspaths** command displays information about all AS paths. The AS path is listed along with the number of routes that use it.

Parameter	Value	Meaning
aspaths	all	Displays information about all AS paths.

Restrictions

None.

Example

To display information about all AS paths:

rs# bgp show aspaths all		
Hash	Ref	Path
0	5	IGP (Id 1)
2	1	(64900) 64901 64902 IGP (Id 3)
7	4	(64900) 64901 IGP (Id 2)

bgp show cidr-only

Mode

Enable

Format

```
bgp show cidr-only <ip-addr-mask> |all
```

Description

The **bgp show cidr-only** command displays the same type of route information as the **bgp show routes** command. The difference is that the **bgp show cidr-only** command limits the display to CIDR routes only.

Parameter	Value	Meaning
cidr-only	<ip-addr-mask>	Displays information about the specified CIDR route.
	all	Displays information about all CIDR routes.

Restrictions

None.

Example

To display information all CIDR routes in the RS's BGP route table:

rs# bgp show cidr-only all				
Proto	Route/Mask	NextHop	ASPath	
BGP	12.2.19/25	207.135.89.65	(64800)	64753 64752 64751 6379
3561 11277	IGP (Id 13805)			
BGP	12.5.172/22	207.135.89.65	(64800)	64753 64752 64751 6379
3561 1	IGP (Id 173)			
BGP	12.5.252/23	207.135.89.65	(64800)	64753 64752 64751 6379
5646 1 7018	6301 IGP (Id 926)			
BGP	12.6.42/23	207.135.89.65	(64800)	64753 64752 64751 6379
5646 1 7018	11090 IGP (Id 979)			
BGP	12.6.134/23	207.135.89.65	(64800)	64753 64752 64751 6379
5646 1 701	7314 10562 IGP (Id 388)			
BGP	12.7.214/23	207.135.89.65	(64800)	64753 64752 64751 6379
5646 7018 4129	IGP (Id 31004)			

bgp show community

Mode

Enable

Format

```
bgp show community community-id <number> autonomous-system <number> | well-known-community  
[no-export|no-advertise|no-export-subconfed] | reserved-community <number>]
```

Description

The **bgp show community** command displays routes that belong to a specified community in a specified autonomous system.

Parameter	Value	Meaning
community-id	<number>	Is the community identifier portion of a community split. This is combined with the autonomous-system value entered to create a value for the community attribute.
autonomous-system	<number>	Is an autonomous system number. Can be any value from 1 to 65535.
well-known-community		Is one of the well-known communities. Specify one of the following:
	no-export	Is a special community that indicates the routes associated with this attribute must not be advertised outside a BGP confederation boundary.
	no-advertise	Is a special community indicating that the routes associated with this attribute must not be advertised to other BGP peers.
	no-export-subconfed	Is a special community indicating the routes associated with this attribute must not be advertised to external BGP peers. (This includes peers in other members' autonomous systems inside a BGP confederation.)
reserved-community	<number>	This option specifies one of the reserved communities that is not well-known. A reserved community is one that is in one of the following ranges (0x00000000 - 0x0000FFFF) or (0xFFFF0000 - 0xFFFFFFFF).

Restrictions

None.

Example

To display routes that belong to community 160 in AS 64900:

```
rs# bgp show community community-id 160 autonomous-system 64900
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Path
*> 192.68.20/24      172.16.20.2              64901 i
*> 192.68.222/24     172.16.20.2             64901 64902 i
```

bgp show community-list

Mode

Enable

Format

```
bgp show community-list <name> |all
```

Description

The **bgp show community-list** command displays a specific community list or all community lists configured on the RS.

Parameter	Value	Meaning
community-list	<name>	The name of the community list.
	all	Show all configured community lists.

Restrictions

None.

Examples

To display all community lists configured on the RS:

```
rs# bgp show community-list all
Name                Count Community List
=====
cde                  4 5:67 7:89 5:67 7:89
abc                  4 5:67 7:89 5:67 7:89
cm1                   3 COMMUNITY_NO_EXPORT_SUB COMMUNITY_NO_EXPORT
COMMUNITY_NO_ADVERTISE
comm                  4 4:56 COMMUNITY_NO_EXPORT 6:78 COMMUNITY_NO_ADVERTISE
```

Name is the identifier for the list of communities created with the **ip-router policy create community-list** command.

Count is the number of communities in the list.

Community List is the communities in the list. For 'cm1' in the above example, the community list includes the well-known communities no-export-subconfed, no-export, and no-advertise.

To display a specific community list configured on the RS:

```
rs# bgp show community-list comm
Name                Count Community List
=====
comm                  4 4:56 COMMUNITY_NO_EXPORT 6:78 COMMUNITY_NO_ADVERTISE
```

bgp show flap-statistics

Mode

Enable

Format

bgp show flap-statistics [*<ip-addr-mask>* |all|damped|history] longer-prefixes

Description

The **bgp show flap-statistics** command displays all routes that are flapping, suppressed, or withdrawn.

Parameter	Value	Meaning
flap-statistics	<i><ip-addr-mask></i>	IP address and subnet mask of a particular route.
all	all	Shows all routes that are flapping, suppressed, or withdrawn.
damped		Shows all routes that are suppressed because of damping.
history		Shows all routes that are unreachable and have a history of flapping.
longer-prefixes		Show statistics for the route specified by the entered IP address and subnet mask, as well as all other routes with longer subnet masks.

Restrictions

None.

bgp show neighbor

Mode

Enable

Format

bgp show neighbor <ipaddr-mask> |all

Description

The **bgp show neighbor** command displays a specific peer or all peers configured on the RS.

Parameter	Value	Meaning
neighbor	<ipaddr>	The IP address, in the form a.b.c.d, of the peer.
	all	Show all peers.

Restrictions

None.

Examples

To display all peers configured on the RS:

```
rs# bgp show neighbor all
Peer: 5.5.5.5+179      Local: 5.5.5.1+1024      Type: External      remote AS
  State: Established      Flags: <GenDefault>
  Last State: OpenConfirm Last Event: RecvKeepAlive      Last Error: None
  Options: <>
  Configured parame :
  Used parameters :
  Peer Version: 4 Peer ID: 5.5.5.5      Local ID: 43.1.1.1      Active Holdtime: 180
  Uptime 0d0h2m34s
  Last traffic (seconds): Received 34      Sent 34 Checked 34
  Input messages: Total 4 Updates 1      Octets 102
  Output messages:      Total 5 Updates 0      Octets 105
      count of sent routes 0
```

To display a specific peer configured on the RS

:

```
rs# bgp show neighbor 5.5.5.5
Peer: 5.5.5.5+179      Local: 5.5.5.1+1024      Type: External      remote AS
      State: Established      Flags: <GenDefault>
      Last State: OpenConfirm Last Event: RecvKeepAlive      Last Error: None
      Options: <>
      Configured parame :
      Used parameters :
      Peer Version: 4 Peer ID: 5.5.5.5      Local      ID:      43.1.1.1      Active Holdtime:
180
      Uptime 0d0h3m30s
      Last traffic (seconds): Received 30      Sent 30 Checked 30
      Input messages: Total 5 Updates 1      Octets 121
      Output messages:      Total 6 Updates 0      Octets 124
      count of sent routes 0
```

bgp show peer-as

Mode

Enable

Format

bgp show peer-as <number>

Description

The **bgp show peer-as** command displays information about routers in a specified autonomous system that are peered with the RS.

Parameter	Value	Meaning
peer-as	<number>	Is the AS number of a peer autonomous system.

Restrictions

None.

Example

To display information about TCP and BGP connections to autonomous system 64901:

```
rs# bgp show peer-as 64901
group type External AS 64901 local 64900 flags <>
peer 172.16.20.2 version 4 lcladdr (null) gateway (null)
  flags 0x20
  state 0x6 <Established>
  options 0x0 <>
  metric_out -1 preference 170 preference2 0
  recv buffer size 0 send buffer size 0
  messages in 10039 (updates 5, not updates 10034) 190863 octets
  messages out 10037 (updates 1, not updates 10036) 190743 octets
```

bgp show peer-group-type

Mode

Enable

Format

bgp show peer-group-type external|internal|igp|routing

Description

The **bgp show peer-group-type** command displays status information about BGP peers according to their group.

Parameter	Value	Meaning
peer-group-type		The peer group type to be displayed.
	external	Displays status information about external peers.
	internal	Displays status information about internal peers.
	igp	Displays status information about igp peers.
	routing	Displays status information about routing peers.

Restrictions

None.

Example

To display status information about external peers:

```
rs# bgp show peer-group-type external
Group   Neighbor      V   AS MsgRcvd MsgSent State
external 172.16.20.2    4 64901  10045  10044 Established
BGP summary, 1 peers in group type "external"
```

bgp show peer-host

Mode

Enable

Format

bgp show peer-host <ipaddr> received-routes|all-received-routes|advertised-routes

Description

The **bgp show peer-host** command displays information related to a specified BGP peer host. Three types of information can be displayed: routes received and accepted from a BGP peer host, all BGP routes (both accepted and rejected) from a peer host, and all routes the RS has advertised to a peer host.

Parameter	Value	Meaning
peer-host	<ipaddr>	Is the IP address of a BGP peer host
received-routes		Displays all valid BGP routes received and accepted from the specified peer host.
all-received-routes		Displays all BGP routes (both accepted and rejected) from the specified peer host.
advertised-routes		Displays all routes the RS has advertised to the specified peer host.

Restrictions

None.

Examples

To display all valid BGP routes received and accepted from peer host 172.16.20.2:

```
rs# bgp show peer-host 172.16.20.2 received-routes
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Path
*> 172.16.70/24      172.16.20.2              64901 i
*> 172.16.220/24     172.16.20.2              64901 i
*> 192.68.20/24      172.16.20.2              64901 i
*> 192.68.222/24     172.16.20.2              64901 64902 i
```


To display all BGP routes (both accepted and rejected) from peer host 172.16.20.2:

```
rs# bgp show peer-host 172.16.20.2 all-received-routes
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Path
   172.16.20/24      172.16.20.2              64901 i
*> 172.16.70/24      172.16.20.2              64901 i
*> 172.16.220/24     172.16.20.2              64901 i
*> 192.68.20/24      172.16.20.2              64901 i
*> 192.68.222/24     172.16.20.2             64901 64902 i
```

Displays all routes the RS has advertised to peer host 172.16.20.2:

```
rs# bgp show peer-host 172.16.20.2 advertised-routes
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Path
*> 172.16.20/24      172.16.20.1              i
*> 192.68.11/24      192.68.11.1              i
```

bgp show regexp

Mode
Enable

Format

bgp show regexp <string>

Description

The **bgp show regexp** command searches through all BGP routes that contain specified keywords belonging to an AS path. These specified keywords are the AS path regular expression upon which the search is executed. The character string can be a combination of AS numbers or names.

Some BGP character string shorthand conventions:

- . Matches any AS number
- * Zero or more repetitions
- + One or more repetitions
- ? Zero or one repetition
- | Alternation
- () Parentheses group subexpressions

Parameter	Value	Meaning
regexp	<string>	A character string that specifies the regular expression. Specify an AS.

Restrictions

None.

Example

To display the BGP routes starting with “64751”:

rs# bgp show regexp "64751 .*"					
Network	Next Hop	Metric	LocPrf	Path	
*> 193.226.64/22	134.141.178.33		64751	6379 1 1239 11331 8338 i	

bgp show routes

Mode

Enable

Format

bgp show routes <ip-addr>|<ip-addr-mask>|all longer-prefixes

Description

The **bgp show routes** command displays the IP address/netmask, next hop, and AS path for each BGP route.

Parameter	Value	Meaning
routes	<ip-addr>	Display information about the specified route without specifying the subnet mask.
	<ip-addr-mask>	Displays information about the specified route.
	all	Displays information about all routes.
	longer-prefixes	Displays all routes with subnet mask of that specified in <ip-addr-mask> and longer.

Restrictions

None.

Example

To display the BGP routing table

```
rs# bgp show routes all
BGP table : Local router ID is 134.141.178.48
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop          MED    LocPrf Path
   -----                -
*> 3/8                    207.135.89.21    50      (64901) 64751 6379 1 701 80
i
  4/8                    207.135.89.21      (64901) 64751 6379 1 i
  6/8                    207.135.89.21      (64901) 64751 6379 1 7170 1455 i
  9.2/16                 207.135.89.21      (64901) 64751 6379 1 701 i
  9.20/17                207.135.89.21      (64901) 64751 6379 1 2685 2686 i
  9.184.112/20           207.135.89.21      (64901) 64751 6379 1 6461 3786 i
  9.186.144/20           207.135.89.21      (64901) 64751 6379 1 6461 3786 i
  12/8                   207.135.89.21      (64901) 64751 6379 1 7018 i
  12.0.48/20             207.135.89.21      (64901) 64751 6379 1 13646 1742 i
  12.6.208/20            207.135.89.21      (64901) 64751 6379 1 13646 1742 i
  12.13.224/19           207.135.89.21      (64901) 64751 6379 1 7018 196 i
  12.43.128/20           207.135.89.21      (64901) 64751 6379 1 7018 16711 i
  12.43.144/20           207.135.89.21      (64901) 64751 6379 1 7018 16711 i
  12.44.224/20           207.135.89.21      (64901) 64751 6379 1 16499 i
  12.64.128/19           207.135.89.21      (64901) 64751 6379 1 7018 4264 i
  12.64.160/20           207.135.89.21      (64901) 64751 6379 1 7018 4264 i
  12.96.240/20           207.135.89.21      (64901) 64751 6379 1 3561 19384 i
-- More: m,<space> - Quit: q - One line: <return> - Search: s,/ --
```

Notice that the display shows the route to each network, the next hop, the MED number (if any), the local preference, and the path. Additionally, the display indicates the status of the route and its origin: i = IGP, e = EGP, and ? = incomplete.

bgp show summary

Mode
Enable

Format

bgp show summary

Description

The **bgp show summary** command displays the status of all BGP peers of the RS.

Parameter	Value	Meaning
summary		Displays BGP connection information.

Restrictions

None.

Example

To display the status of all BGP connections:

rs# bgp show summary							
Neighbor	V	AS	MsgRcvd	MsgSent	Up/Down	State	Prefixes
-----	-	--	-----	-----	-----	-----	-----
172.16.20.2	4	64901	10033	10031	6d23h8m1s	Established	1
BGP summary, 1 groups, 1 peers							

bgp show sync-tree

Mode

Enable

Format

bgp show sync-tree

Description

The **bgp show sync-tree** command displays the BGP synchronization tree. The synchronization tree is used by IBGP peers to resolve the next hop (forwarding address). It gives information about routes that are orphaned because the next hop could not be resolved.

Restrictions

None.

Examples

The following example shows the next hops for some of the routes that are not resolved (by showing orphaned routes):

```
rs# bgp show sync tree
Task BGP_Sync_64805:
    IGP Protocol: Any          BGP Group: group type Routing AS 64805

    Sync Tree (* == active, + == active with alternate, - ==
inactive with alternate:
    Orphaned routes
        Forwarding address 172.23.1.18
            3/255 peer 172.23.1.26 preference 170
            128.36/255.255 peer 172.23.1.26 preference 170
            128.152/255.255 peer 172.23.1.26 preference 170
            129.200/255.255 peer 172.23.1.26 preference 170
            129.253/255.255 peer 172.23.1.26 preference 170
            130.44/255.255 peer 172.23.1.26 preference 170
            130.50/255.255 peer 172.23.1.26 preference 170
            130.132/255.255 peer 172.23.1.26 preference 170
            134.54/255.255 peer 172.23.1.26 preference 170
            134.120/255.255 peer 172.23.1.26 preference 170
            134.173/255.255 peer 172.23.1.26 preference 170
            134.217/255.255 peer 172.23.1.26 preference 170
            134.244/255.255 peer 172.23.1.26 preference 170
            136.1/255.255 peer 172.23.1.26 preference 170
            137.49/255.255 peer 172.23.1.26 preference 170
            137.159/255.255 peer 172.23.1.26 preference 170
            138.239/255.255 peer 172.23.1.26 preference 170
```

The following example shows the next hop for all the routes that are resolved.:

```
rs# bgp show sync-tree
Task BGP_Sync_64805:
      IGP Protocol: Any      BGP Group: group type Routing AS 64805

      Sync Tree (* == active, + == active with alternate, - ==
inactive with alternate:
      Node 3/8388608 route 3/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 4/8388608 route 4/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 6/8388608 route 6/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 9.2/32768 route 9.2/255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 9.20/16384 route 9.20/255.255.128 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 10.12.1/2 route 10.12.1/255.255.255.252 metric 0 interface
      Node 10.12.1.4/2 route 10.12.1.4/255.255.255.252 metric 2 next hop 172.23.1.22
      Node 10.200.12/128 route 10.200.12/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 10.203.12/128 route 10.203.12/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 10.204.12/128 route 10.204.12/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12/8388608 route 12/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.2.19/64 route 12.2.19/255.255.255.128 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.2.97/128 route 12.2.97/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.3.123/128 route 12.3.123/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.4.5/128 route 12.4.5/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.4.164/128 route 12.4.164/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.5.164/128 route 12.5.164/255.255.255 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.5.172/512 route 12.5.172/255.255.252 metric -1 next hops 172.23.1.6
172.23.1.22
      Node 12.5.252/256 route 12.5.252/255.255.254 metric -1 next hops 172.23.1.6
172.23.1.22
```

bgp start | stop

Mode

Configure

Format

bgp start|stop

Description

The **bgp start** command starts BGP on the RS. The **bgp stop** command stops BGP on the RS.

Parameter	Value	Meaning
start		Starts BGP.
stop		Stops BGP.

Restrictions

None.

bgp trace

Mode

Configure

Format

```
bgp trace [packets|open|update|keep-alive [detail|send|receive|[group <number>
[peer-host <ipaddr>]]] [aspath] [local-options
all|general|state|normal|policy|task|timer|route]
```

Description

The **bgp trace** command lets you set BGP trace options for the RS.

Parameter	Value	Meaning
packets		Trace all BGP packets.
open		Traces BGP OPEN packets, which are used to establish a peer relationship.
update		Traces BGP update packets, which are used to pass network reachability information.
keep-alive		Traces BGP KEEPALIVE packets, which are used to verify reachability.
detail		Shows detailed information about the specified packets.
send		Shows the specified packets sent by the router.
receive		Shows the specified packets received by the router.
group	<number>	Is the group ID of the group for which tracing needs to be enabled.
peer-host	<ipaddr>	Peer-host IP address for which tracing needs to be enabled. The peer-host has to be qualified by the group to which it belongs
aspath		Traces aspath related events.
local-options		Sets trace options for this protocol only.
	all	Traces all additions, changes, and deletions to the ROSRD routing table.
	general	Activates normal and route tracing.
	state	Traces state machine transitions in the protocol
	normal	Traces normal protocol occurrences. (Abnormal protocol occurrences are always traced.)

Parameter	Value	Meaning
	policy	Traces the application of protocol and user-specified policies to routes being imported and exported
	task	Traces system interface and processing associated with this protocol or peer
	timer	Traces timer usage by this with this protocol or peer
	route	Traces routing table changes for routes installed by this protocol or peer

**Note**

If neither the group nor peer-host is specified then tracing is enabled for all groups and peers. If the group is specified and the peer-host is not specified then the tracing is enabled for that group. If both the peer-host and group are specified then the tracing is enabled for that peer-host in the specified group.

Restrictions

None.

8 CISCO-HDLC COMMANDS

The **cisco-hdlc** commands allow you to:

- Define Cisco HDLC service profiles, so you can configure your RS to more efficiently utilize available bandwidth for Cisco HDLC communications.
- Monitor Cisco HDLC ports.

You must also define the type and location of your Cisco HDLCWAN port(s) using the **port set wan-encapsulation cisco-hdlc** command (see [Chapter 49, "port Commands."](#) for details).

8.1 COMMAND SUMMARY

The following table lists the **cisco-hdlc** commands. The sections following the table describe the command syntax for each command.

cisco-hdlc apply service <service-name> ports <port-list>
cisco-hdlc clear stats-counter [frame-drop-qdepth-counter] [max-frame-enqueued-counter] [frame-drop-red-counter] [rmon] port <port-list>
cisco-hdlc define service <service-name> keepalive <number> rmon on off high-priority-queue-depth <number> low-priority-queue-depth <number> med-priority-queue-depth <number> red on off red-maxTh-high-prio-traffic <number> red-maxTh-med-prio-traffic <number> red-maxTh-low-prio-traffic <number> red-minTh-high-prio-traffic <number> red-minTh-med-prio-traffic <number> red-minTh-low-prio-traffic <number>
cisco-hdlc restart slarp ports <port-list>
cisco-hdlc set cisco-hdlc-encaps-bgd ports <port-list>
cisco-hdlc show [service <service-name> all] [stats ports <port-list> all-ports [summary]]

cisco-hdlc apply service

Mode

Configure

Format

cisco-hdlc apply service *<service-name>* **ports** *<port-list>*

Description

The **cisco-hdlc apply service** command allows you to apply a previously defined service profile to one or more ports. The service profile must have been defined previously with the **cisco-hdlc define service** command.

Parameter	Value	Meaning
service	<i><service-name></i>	Name of a service defined with the cisco-hdlc define service command.
ports	<i><port-list></i>	The port(s) to which you wish to apply the pre-defined service profile. You can specify a single port or a comma-separated list of ports.

Restrictions

Restricted to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Example

To apply the service “s1” to slot 2, serial ports 1 and 2:

```
rs(config)# cisco-hdlc apply service s1 ports se.2.1,se.2.2
```

cisco-hdlc clear stats-counter

Mode

Enable

Format

cisco-hdlc clear stats-counter [**frame-drop-qdepth-counter**] [**max-frame-enqueued-counter**] [**frame-drop-red-counter**] [**rmon**] **port** <port-list>

Description

The **cisco-hdlc clear stats-counter** command allows you to specify a particular statistic counter and have the statistics reset to zero. There are statistic counters on each Cisco HDLC port, and you can use the **cisco-hdlc clear stats-counter** command to clear the counter for an individual port or for a group of ports.

Parameter	Value	Meaning
frame-drop-qdepth-counter		Specify this optional parameter to reset the frame drop counter to zero.
max-frame-enqueued-counter		Specify this optional parameter to reset the max enqueuedframes counter to zero.
frame-drop-red-counter		Specify this optional parameter to reset the packet drop counter to zero.
rmon		Specify this optional parameter to reset the RMON counter to zero.
port	<port-list>	The port(s) on which you wish to clear the counter.

Restrictions

Restricted to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Example

To clear the frame drop counter to zero on port se.3.1:

```
rs# cisco-hdlc clear frame-drop-qdepth-counter port se.3.1
```

cisco-hdlc define service

Mode
Configure

Format

```
cisco-hdlc define service <service-name> keepalive <interval> rmon on|off
high-priority-queue-depth <number> low-priority-queue-depth <number>
med-priority-queue-depth <number> red on|off red-maxTh-high-prio-traffic <number>
red-maxTh-med-prio-traffic <number> red-maxTh-low-prio-traffic <number>
red-minTh-high-prio-traffic <number> red-minTh-med-prio-traffic <number>
red-minTh-low-prio-traffic <number>
```

Description

The **cisco-hdlc define service** command allows you to specify the following attributes for a newly created service profile:

- The keepalive interval (default is 10 seconds).
- Enable/disable RMON. Before you can view RMON statistics such as Ethernet statistics and history for Cisco HDLC ports, RMON has to be activated.
- Activate or deactivate Random Early Discard (RED) for Cisco HDLC ports.
- The maximum and minimum threshold values for RED high-, low-, and medium-priority traffic. In general, Riverstone recommends that the maximum threshold values be less than or equal to the respective high-, low-, or medium-priority queue depth. The minimum threshold values should be one-third of the respective maximum threshold.

You must specify at least one parameter.



Note When you apply cisco-hdlc encapsulation to a WAN port, a default service profile is applied. You need only use the **cisco-hdlc define service** command if you want to change a parameter from the default value.

Parameter	Value	Meaning
service	<service-name>	The name you wish to assign to the newly created service profile.
keepalive	<interval>	The number of seconds that a response to a keepalive message should be received before an error event is recorded.
rmon	on off	Specifying the on keyword enables RMON for Cisco HDLC ports. Specifying the off keyword disables RMON for Cisco HDLC ports.

Parameter	Value	Meaning
high-priority-queue-depth	<i><number></i>	The number of items allowed in the Cisco HDLC queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 - 100 item range. The default value is 20.
med-priority-queue-depth	<i><number></i>	The number of items allowed in the Cisco HDLC queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 - 100 item range. The default value is 20.
low-priority-queue-depth	<i><number></i>	The number of items allowed in the Cisco HDLC queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 - 100 item range. The default value is 20.
red	on off	Specifying the on keyword enables RED for Cisco HDLC ports. Specifying the off keyword disables RED for Cisco HDLC ports.
red-maxTh-high-prio-traffic	<i><number></i>	The maximum allowable threshold for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-maxTh-low-prio-traffic	<i><number></i>	The maximum allowable threshold for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-maxTh-med-prio-traffic	<i><number></i>	The maximum allowable threshold for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-minTh-high-prio-traffic	<i><number></i>	The minimum allowable threshold for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
red-minTh-low-prio-traffic	<i><number></i>	The minimum allowable threshold for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
red-minTh-med-prio-traffic	<i><number></i>	The minimum allowable threshold for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.

Restrictions

Restricted to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Example

To create a service profile named “s1” with the following attributes:

- Keepalive set to 15 seconds
- RED disabled
- RMON enabled

then you would enter the following command line in Configure mode:

```
rs(config)# cisco-hdlc define service s1 keepalive 15 red off rmon on
```


cisco-hdlc restart slarp

Mode

Enable

Format

cisco-hdlc restart slarp ports *<port-list>*

Description

The **cisco-hdlc restart slarp** command allows you to reset and restart the SLARP negotiation process for Cisco HDLC ports.

Parameter	Value	Meaning
ports	<i><port-list></i>	The ports for which you want to re-establish SLARP negotiation.

Restrictions

Restricted to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Example

To restart SLARP negotiation on serial ports 1 and 2 of slot 4:

```
rs# cisco-hdlc restart slarp ports se.4.1,se.4.2
```

cisco-hdlc set cisco-hdlc-encaps-bgd

Mode

Configure

Format

cisco-hdlc set cisco-hdlc-encaps-bgd ports *<port-list>*

Description

The **cisco-hdlc set cisco-hdlc-encaps-bgd** command allows you to use bridged format encapsulation on one or more Cisco HDLC ports.

Parameter	Value	Meaning
ports	<i><port list></i>	The port(s) to which you wish to use bridged encapsulation. You can specify a single port or a comma-separated list of ports.

Restrictions

Restricted to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Example

To force bridged encapsulation to slot 2, serial ports 1 and 2:

```
rs(config)# cisco-hdlc set cisco-hdlc-encaps-bgd ports se.2.1,se.2.2
```

cisco-hdlc show

Mode

Enable

Format

```
cisco-hdlc show [service <service-name>|all] [stats ports <port-list>|all-ports [summary ]]
```

Description

The `cisco-hdlc show` command lets you view one or all Cisco HDLC service profiles or the statistics of Cisco HDLC ports.

Parameter	Value	Meaning
service	<service-name> all	Displays the parameters for the specified service profile or for all service profiles.
stats ports	<port-list> all-ports	Displays the statistics of the specified Cisco HDLC port or for all Cisco HDLC ports.
summary		The keyword summary displays a summary of the statistics for the ports.

Restrictions

Restricted to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Example

To display a summary of statistics for all Cisco HDLC ports:

rs# cisco-hdlc show stats port all-ports summary		
	Link	Keepalive
	Adm/Opr	sec
Port	States	
----	--/--	-----
se.2.1	Up/Up	15
se.2.3	Up/Up	15

To display detailed statistics for all Cisco HDLC ports:

```

rs# cisco-hdlc show stats ports all-ports
SLARP Keepalive          15
  SLARP Local Seq        34
  SLARP Remote Seq       33
  SLARP Seq Retries      1

Service Features Status
-----
RMON:                    Disabled
RED:                     Enabled

Current Random Early Drop Counters
-----
  RED max threshold high priority traffic  12
  RED min threshold high priority traffic   4
  RED max threshold med  priority traffic  12
  RED min threshold med  priority traffic   4
  RED max threshold low  priority traffic  12
  RED min threshold low  priority traffic   4
  High priority packets dropped due to RED  0
  Med priority packets dropped due to RED   0
  Low priority packets dropped due to RED   0
  Ctl priority packets dropped due to RED   0

Current Output Queue States
-----
  High priority queue depth                100
  Med  priority queue depth                 50
  Low  priority queue depth                 35
  Ctrl priority queue depth                 20
  Max number frames enqueued in high priority queue  0
  Max number frames enqueued in med priority queue   0
  Max number frames enqueued in low priority queue   0
  Max number frames enqueued in ctrl priority queue   2
  Current number of frames in high priority queue    0
  Current number of frames in med  priority queue    0
  Current number of frames in low  priority queue    0
  Current number of frames in ctrl priority queue    0
  Frames dropped due to ctrl queue depth exceeded    0
  Frames dropped due to high queue depth exceeded    0
  Frames dropped due to med queue depth exceeded     0
  Frames dropped due to low queue depth exceeded     0

```

continued...

MIB II Stats

```

-----
Transmitted octets          0
Transmitted unicast frames  0
Transmitted broadcast frames 0
Transmitted multicast frames 0
Discarded transmit frames   9
Error transmit frames       0
Received octets             0
Received unicast frames     0
Received broadcast frames   0
Received multicast frames   0
Discarded receive frames    0
Error receive frames        0

```

To display Cisco HDLC service profiles:

```
rs# cisco-hdlc show service all
```

Service Features Status

Service hdlc(Cisco HDLC):

```

High priority queue depth      100
Medium priority queue depth    50
Low priority queue depth       35
RMON                           Disabled
DE-MARK:                       Disabled
RED:                           Enabled
  RED max threshold high priority traffic 12
  RED min threshold high priority traffic 4
  RED max threshold med priority traffic 12
  RED min threshold med priority traffic 4
  RED max threshold low priority traffic 12
  RED min threshold low priority traffic 4
Keepalive Timeout              15
Ports                          se.2.(1,3)

```


9 CLI COMMANDS

Use the **cli** commands to set CLI parameters.

9.1 COMMAND SUMMARY

The following table lists the **cli** commands. The sections following the table describe the command syntax.

<code>cli set command completion on off</code>
<code>cli set history size <num> default maxsize</code>
<code>cli set terminal rows <num> columns <num></code>
<code>cli show history</code>
<code>cli show terminal</code>
<code>cli terminal monitor on off</code>

cli set command completion

Mode

User and
Configure

Format

cli set command completion on | off

Description

Use the **cli set command completion** command to enable or disable command completion support. Command completion allows a user to type in a partial command, such as **cli se**, and then press the Space Bar to complete the command. This feature is helpful when long commands are required.

This command works in the user mode and the configure mode, and on both the primary and backup CMs. When executed in the configure mode, the command enables or disables command completion support for the entire system. When executed in the user mode, the command affects only the current login session.

Parameter	Value	Meaning
completion		Specifies command completion support. By default, command completion is enabled. It can be disabled either in the configuration mode or in the enable mode. A disable (or enable) in the enable mode applies only to the console (or telnet session) it is run in. A disable in the config mode applies to all new consoles (or telnet sessions) launched after it is added.
	on	Specify to enable command completion.
	off	Specify to disable command completion.

Restrictions

None.

Examples

To enable command completion in the user mode:

```
rs> cli set command completion on
```


cli set history

Mode

User and
Configure

Format

cli set history size <num> | default | maxsize

Description

Use the **cli set history** command to set the size of the command history buffer. Each command stored in this buffer can be recalled without the user typing in the complete command again. Setting the size of the history buffer determines how many of the most recently executed commands are stored. When the buffer is full, the oldest commands are dropped, to make room for the newest command.

The **cli set history** command works in both the user mode and the configure mode. When executed in the configure mode, the command sets the history size of the entire system. When executed in the user mode, the command affects only the current login session.

Parameter	Value	Meaning
size	<num>	A number that specifies how many of the most recently executed commands should be kept. By default, size is 25. The range of <i>num</i> is 0 to 2147483648. To disable history support, specify a size of 0.
	default	Sets the history buffer size to the system default.
	maxsize	Sets the history buffer size to the system maximum.

Restrictions

None.

Examples

To set the history buffer size to 100 enter this command:

```
rs> cli set history size 100
```

cli set terminal

Mode

User

Format

```
cli set terminal [columns <num>] [rows <num>]
```

Description

Use the **cli set terminal** command to modify the terminal screen size of the current session. Specifying the number of rows causes the RS to automatically pause when the screen output fills the screen to *num*.

Parameter	Value	Meaning
columns	<num>	This is the number of columns for the terminal. The default column size is 80. The range of <i>num</i> is 0 to 2147483648.
rows	<num>	This is the number of rows for your terminal. The default row size is 24. The range of <i>num</i> is 0 to 2147483648. To prevent output from pausing after filling the screen, set the value to 0.

Restrictions

None.

Examples

To set the number of rows to 50 lines:

```
rs# cli set terminal rows 50
```

cli show history

Mode
User

Format

cli show history

Description

The **cli show history** command displays the commands issued during the current CLI session. A number is associated with each command. This number is useful for re-entering, modifying, or negating the command. Configure the number of commands by setting the command history buffer size using the **cli set history** command.



Note A command history recall can be performed by entering **!*** at the command prompt.

Restrictions

None.

Examples

To display a history of your most-recently-issued commands:

```
rs# cli show history
1 en
2 aging l2 show status
3 aging l3 show status
4 aging l2 show status
5 cli show history
```

Table 9-1 Display Field Descriptions for the cli show history Command

Field	Description
1 en	The first command issued.
2 aging l2 show status	The second command issued.
5 cli show history	The last command issued. 3 aging l3 show status and 4 aging l2 show status are the third and fourth commands issued.

cli show terminal

Mode

User

Format

cli show terminal

Description

The **cli show terminal** command displays information about terminal settings. Terminal settings determine the display characteristics of a CLI session.

Restrictions

None.

Examples

To display terminal settings:

```
rs# cli show terminal
History:
  Active           : Yes
  Current buffer size : 25 entries
  Maximum buffer size : 25 entries
Terminal:
  Number of rows    : 24
  Number of columns : 80
Other:
  Command completion : On
Special Characters
(not changeable):
  Command completion : ' ' and <tab>
  Help               : '?'
  History expansion  : '!'
```

Table 9-2 Display Field Descriptions for the cli show history Command

Field	Description
History	By default, the history feature is active. The buffer size is the number of commands the RS stores in history. By default, the RS stores the 25 most recently issued commands. Use the cli set history command to deactivate the history feature, or to resize the buffer.
Terminal	This is the terminal screen size of the current session.
Command completion	Command completion is enabled by default. This means that the RS will automatically complete a partially entered command when the Space Bar is pressed
Help	Enter ? for help.
History expansion	Recall history commands by entering ! followed by the command's number in the cli show history command.

For more information on the command completion and history features, refer to the *Riverstone Networks RS Switch Router User Guide*.

cli terminal monitor

Mode

Enable

Format

`cli terminal monitor on | off`

Description

Some system messages are normally sent only to the management console. The **cli terminal monitor** command sets up the current CLI session to also receive those system messages. This command is only useful in a current Telnet CLI session where the debugging output normally sent to the management console is also displayed on the Telnet screen.

Parameter	Value	Meaning
monitor		Allows the CLI session screen to display system messages.
	on	Specify to enable receipt of console output.
	off	Specify to disable receipt of console output.

Restrictions

None.

Examples

To enable displaying console output on a Telnet screen enter:

```
rs> cli terminal monitor on
```

10 CMTS COMMANDS

The **cmts** commands are used to configure cable modem interfaces for DOCSIS and EuroDOCSIS compatible cable modem headend terminations.

10.1 COMMAND SUMMARY

The following table lists the **cmts** commands. The sections following the table describe the command syntax.

<code>cmts clear error-stats <port-list all-ports> {[all] [downstream <range> all] [upstream <range> all]}</code>
<code>cmts clear flap-list</code>
<code>cmts clear map-stats <port-list all-ports> [upstream <range> all]</code>
<code>cmts clear misc-stats <port-list> all-ports</code>
<code>cmts clear packet-stats <port-list all-ports> [all] [downstream <range> all] [upstream <range> all]</code>
<code>cmts reset ak <port-list> type <reset_type> macaddr <value></code>
<code>cmts reset modem <port-list> macaddr <value></code>
<code>cmts reset tek <port-list> sid <sid></code>
<code>cmts set ak <port-list> macaddr <value> ak-lifetime <value> ak-gracetime <value></code>
<code>cmts set cpe <port-list> macaddr <macaddr> modem-macaddr <macaddr> vlan <string> ip <ipaddr></code>
<code>cmts set dschannel <port-list> downstream <num-list all> {frequency <range> width <6Mhz 8Mhz> modulation <qam256 qam64> interleave <8 12 16 32 64 128> power <value> ip-broadcast <on off> ip-multicast <on off> state <on off> modulation-state <on off> policing <on off>}</code>
<code>cmts set flapthresh <port-list> {aging <value> insertion-time <value> power-adjust <value> miss <value>}</code>

cmts set headend <port-list> {mic-check <skip do-not-skip> mac-check <skip do-not-skip> tftp-check <skip do-not-skip> auth-str <string> state <on off> default-vlan <string> tftp-ip-check <skip do-not-skip> client-mac-move <allow disallow allow-inform disallow-inform> upstream-extended-freq <on off> hcs-err <fwd drop> fcs-err <fwd drop> anti-ip-spoofing <enable disable> anti-dhcp-spoofing <enable disable> modem-debug <enable disable> dhcp-ipaddr-snoop <enable disable> dhcp-strict <enable disable> relay-agent-circuit-id <add do-not-add> relay-agent-remote-id <add do-not-add>}
cmts set ipc-local <port> <fast slow>
cmts set ipc-main <fast slow>
cmts llc-ping <value> xid test
cmts set mac <port-list> {sync-interval <value> ucd-interval <value> inv-range-attempts <value> map-length <value> map-lead-time <value> init-maint-length <value> insert-interval <value> vendor-specific non-ip-filter <on off> bpdu-filter <on off> ucc-retry-interval <number> ucc-retries <number>}
cmts set modem <port-list> macaddr <value> [vlan <string>] new-upstream-id <value> [cpe-vlan <string>]
cmts set modulation <profile_number all-values> int-usage-code <keyword> {type <qpsk qam16> preamble-len <value> diff-encoding <on off> fec-error-correct <value> fec-codeword-length <value> scrambler-seed <value> max-burst-size <value> last-codeword-short <on off> scrambler-enable <on off>}
cmts set multicast-ip <port-list> ipaddr <address> prefix-length <value> sid <value>
cmts set multicast-sid <port-list> macaddr <value> sid <id>
cmts set privacy <port-list> {[ak-lifetime <value>] [tek-lifetime <value>]}
cmts set relay-agent interface <name> giaddr <address>
cmts set tek <port-list> sid <value> {[tek-lifetime <value>] [tek-gracetime <value>]}
cmts set uschannel <port-list> upstream <range all> {frequency <num> width <value> power <value> modulation-profile <value> * slot-size <value> range-back-off-start <value> range-backoff-end <value> tx-backoff-start <value> tx-backoff-end <value> power-adj <value> state <on off> policing <on off> policing-alarm <on off> qos-confirm <on off> qos-max-bps <number>}
cmts show ak <port-list all-ports> [macaddr <value> all-macs]
cmts show dschannel <port-list all-ports> [downstream <channel_range> all]
cmts show error-stats <port-list all-ports> [all] [downstream <range> all] [upstream <range> all]

cmts show flap-list
cmts show flap-thresh <port-list all-ports>
cmts show headend <port-list all-ports>
cmts show mac <port-list all-ports>
cmts show map-stats <port-list all-ports> [upstream <range> all]
cmts show misc-stats <port-list> all
cmts show modem <port-list all-ports> macaddr <value all-macs> [detailed]
cmts show modulation <index all-values> interval-usage-code <code-type> [verbose]
cmts show multicast-ip <port-list all-ports> ipaddr <value all-ips> prefix-length <value all-length>
cmts show multicast-sid <port-list all-ports> macaddr <value all-macs> sid <id all-sids>
cmts show packet-stats <port-list all-ports> {[all] [downstream <range> all] [upstream <range> all]}
cmts show privacy <port-list all-ports>
cmts show qosprofile <list-ports all-ports> <id all>
cmts show qosproppermissions
cmts show signalquality <port-list all-ports> upstream <range all>
cmts show service <port-list all-ports> id <range all-values>
cmts show status <port-list all-ports>
cmts show tek <port-list all-ports> sid <value> all-sids
cmts show uschannel <port-list all-ports> [upstream <range> all]
cmts-diag set 3033 <port-list> reg_offset <num> value <num>

cmts clear error-stats

Mode

Enable

Format

```
cmts clear error-stats <port-list | all-ports> {[all] | [downstream <range> | all] | [upstream <range> | all]}
```

Description

The **cmts clear error-stats** facility clears port error statistics.

Parameter	Value	Meaning
error-stats	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to clear all ports.
all		Specify all to clear all ports, both upstream and downstream.
downstream	<range>	Specify downstream to clear downstream or transmit ports. The variable <i>range</i> takes a range of port numbers. This is the range of downstream ports that you want to clear. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to clear all ports.
upstream	<range>	Specify upstream to clear upstream or receive ports. The variable <i>range</i> takes a range of port numbers. This is the range of upstream ports that you want to clear. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to clear all ports.



Note You must specify one parameter, either **all**, **downstream**, or **upstream**.

Restrictions

None.

cmts clear flap-list

Mode

Enable

Format

```
cmts clear flap-list
```

Description

This command clears system parameters in the flap list table.

A cable flap list is a table maintained by the CMTS for every cable modem (active or not active) that is having difficulties communicating with the headend. Flapping refers to the rapid disconnecting and reconnecting of a cable modem. The flap list contains cable modem MAC addresses and logs of the time of the most recent activity.

Restrictions

None.

cmts clear map-stats

Mode
Enable

Format

cmts clear map-stats <port-list | all-ports> | [upstream <range> | all]

Description

The **cmts clear map-stats** facility clears port map statistics.

Parameter	Value	Meaning
map-stats	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to clear all ports upstream.
upstream	<range>	Specify upstream to clear upstream or recieve ports. The variable <i>range</i> takes a range of port numbers. This is the range of upstream ports that you want to clear. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to clear all ports.



Note You must specify one parameter, **all** or **upstream**.

Restrictions

None.

cmts clear misc-stats

Mode

Enable

Format

```
cmts clear misc-stats <port-list> | all-ports
```

Description

The **cmts clear map-stats** facility clears port miscellaneous statistics.

Parameter	Value	Meaning
	<i><port-list></i>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to clear all ports. This keyword must be specified in the command.

Restrictions

None.

cmts clear packet-stats

Mode

Enable

Format

```
cmts clear packet-stats <port-list | all-ports> [all] | [downstream <range> | all] |
[upstream <range> | all]
```

Description

The **cmts clear packet-stats** facility erases the port's list of port packet statistics.

Parameter	Value	Meaning
packet-stats	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to clear all ports. This keyword must be specified in this command.
all		Specify all to clear all ports, both downstream and upstream.
downstream	<range>	Specify downstream to clear downstream or transmit port. The variable <i>range</i> takes a range of port numbers. This is the range of downstream ports that you want to clear. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to clear all ports.
upstream	<range>	Specify upstream to clear upstream or receive ports. The variable <i>range</i> takes a range of port numbers. This is the range of upstream ports that you want to clear. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to clear all ports.



Note You must specify one parameter, either **all**, **downstream**, or **upstream**..

Restrictions

None.

cmts reset ak

Mode

Enable

Format

```
cmts reset ak <port-list> type <reset_type> macaddr <value>
```

Description

Resets the authorization key. This command can be used to have the cable modem re-authenticate itself. Or the authorization key might be used to tell the cable modem that it has been provisioned to receive new multicast traffic. The static multicast configuration is passed to the cable modem through an Authentication Reply.

Parameter	Value	Meaning
ak	<port-list>	<port-list> is a list of physical ports. For the CMTS module, only one port can be specified. For example, when a CMTS module is located in slot 7, specify the CMTS port-list as cm . 7 . 1 .
type		Specifies the type of reset. <i>reset_type</i> must be one of the following:
	invalid	Setting type to invalid causes the CMTS to invalidate the current CM authorization key, but not to transmit an Authorization Invalid message nor to invalidate unicast TEKs.
	Send-invalid	This option causes the CMTS to invalidate the current CM authorization key, and to transmit an Authorization Invalid message to the CM, but not to invalidate unicast TEKs.
	Tek-invalid	Setting type to Tek-invalid causes the CMTS to invalidate the current CM authorization key, to transmit an Authorization Invalid message to the CM, and to invalidate all unicast TEKs associated with this CM authorization.
macaddr	<value>	Specifies a cable modem MAC, to reset it's authorization key. <value> can be in the form xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.

Restrictions

None.

cmts reset modem

Mode

Enable

Format

cmts reset modem *<port-list>* macaddr *<value>*

Description

Resets the cable modem.

Parameter	Value	Meaning
modem	<i><port-list></i>	The variable <i>port-list</i> is a list of physical ports. For the CMTS module, only one port can be specified. For example, when a CMTS module is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
macaddr	<i><value></i>	Specifies a cable modem MAC for which to reset the modem in the form xx:xx:xx:xx:xx:xx or xxxxxxx:xxxxxx.

Restrictions

None.

cmts reset tek

Mode

Enable

Format

cmts reset tek *<port-list>* sid *<sid>*

Description

Resets the traffic keys. The command is used to make sure the traffic flow to the cable modem is properly encrypted.

Parameter	Value	Meaning
tek	<i><port-list></i>	This is a list of physical ports. Only one port per line is specified. For example, when a CMTS module is located in slot 7, specify the CMTS port-list as cm . 7 . 1 .
sid	<i><sid></i>	Reset the traffic key <i>lifetime</i> for a specific SID.

Restrictions

None.

cmts set ak

Mode

Configure

Format

cmts set ak *<port-list>* macaddr *<value>* ak-lifetime *<value>* ak-gracetime *<value>*

Description

Sets the authorization key.

Parameter	Value	Meaning
ak	<i><port-list></i>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
macaddr	<i><value></i>	Specifies a cable modem MAC, to set it's authorization key. <i><value></i> can be in the form xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.
ak-lifetime	<i><value></i>	Specify the authorization key lifetime. Valid values are 1 to 60480000.
ak-gracetime	<i><value></i>	Specify the authorization key gracetime. Valid values are 1 to 1800.

Restrictions

None.

cmts set cpe

Mode

Configure

Format

```
cmts set cpe <port-list> macaddr <macaddr> modem-macaddr <macaddr> vlan <string> ip <ipaddr>
```

Description

This command allows you to configure CPE parameters.

Parameter	Value	Meaning
cpe	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
macaddr	<macaddr>	This is the MAC address of the CPE that the modem is connected to.
modem-macaddr	<macaddr>	This is MAC address of the modem.
vlan	<string>	This is the name of the VLAN that the CPE will be added to.
ip	<ipaddr>	This is the IP address of the CPE.

Restrictions

None.

cmts set dschannel

Mode

Configure

Format

```
cmts set dschannel <port-list> downstream <num-list | all> {frequency <range> | width <6Mhz | 8Mhz> |
modulation <qam256 | qam64> | interleave <8 | 12 | 16 | 32 | 64 | 128> | power <value> | ip-broadcast <on
| off> | ip-multicast <on | off> | state <on | off> | modulation-state <on | off> | policing <on | off>}
```

Description

This command modifies the downstream channel settings.

Parameter	Value	Meaning
dschannel	<port-list>	Is a list of physical port. For the CMTS module, only one port can be specified. For example, when a CMTS module is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
downstream		Selects information about downstream ports.
	num-list	Specify a port number or a range of port numbers.
	all	Specify all for all ports.
frequency	<range>	The CMTS provides IF output. This setting is informational only. It has no impact on operation.
width	<	This parameter sets the downstream channel width.
	6Mhz	Specify 6MHz for the U.S.
	8Mhz	Specify 8MHz for Europe.
modulation		The modulation type associated with this downstream channel.
	qam256	qam64 = 6 bits per symbol.
	qam64	qam256 = 8 bits per symbol.
interleave <8 12 16 32 64 128>		The interleave depth for a downstream port on a cable modem card. The valid values are 8, 16, 32 (default), 64 and 128. These values are for DOCSIS. The default value and only value for EuroDOCSIS is 12. A higher interleave depth provides more protection from bursts of noise on the HFC network. However, it will increase downstream latency which slows data transfer rates.
	8	Interleave depth value of 8.
	16	Interleave depth value of 16.

Parameter	Value	Meaning
	32	Interleave depth value of 32. This is the default.
	64	Interleave depth value of 64.
	128	Interleave depth value of 128.
power	<value>	Specify the CMTS operational transmit power.
ip-broadcast		Is the operational state of IP broadcasting.
	on	Enables IP broadcasting.
	off	Disables IP broadcasting.
ip-multicast		Is the operational state of IP multicasting.
	on	Enables IP multicasting.
	off	Disables IP multicasting.
state		Specifies the state of the downstream channel.
	on	The downstream channel is enabled.
	off	The downstream channel is disabled.
modulation-state		Specifies the state of modulation of the downstream channel.
	on	Modulation of the downstream channel is enabled.
	off	Modulation of the downstream channel is disabled.
policing		Sets downstream traffic policing.
	on	Enables downstream policing.
	off	Disables downstream policing.



Note Although options for frequency and power are supplied, setting these values has no effect since the upconverter (external) changes the power and frequency in the downstream direction.

Table 10-1 lists the Forward Error Correction (FEC) interleaving used for the downstream channel.

Table 10-1 Forward error correction interleaving

Interleave Depth Value	Burst Protection		Latency	
	64 QAM	256 QAM	64 QAM	256QAM
8	5.9 usec	4.1 usec	.22 msec	.15 msec
16	12 usec	8.2 usec	.48 msec	.33 msec
32	24 usec	16 usec	.98 msec	.68 msec
64	47 usec	33 usec	2 msec	1.4 msec
128	95 usec	66 usec	4 msec	2.8 msec

Restrictions

Although options for frequency and power are supplied, setting these values has no effect since the upconverter (external) changes the power and frequency in the downstream direction.

Example

To enable downstream channel 1, enter:

```
cmts set dschannel cm.7.1 downstream 1 state on
```


cmts set flapthresh

Mode

Configure

Format

```
cmts set flapthresh <port-list> {aging <value> | insertion-time <value> | power-adjust <value> | miss <value>}
```

Description

A cable flap list is a table maintained by the CMTS for every cable model (active or not active) that is having difficulties communicating with the headend. *Flapping* refers to the rapid disconnecting and reconnecting of a cable modem.

The flap list contains cable modem MAC addresses and logs of the times of modem activity. This list can not be accessed by a user. It is generated automatically. When a modem *flaps*, it is entered in the list.

Parameter	Value	Meaning
flapthresh	<port-list>	<port-list> is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify <i>port-list</i> as cm. 7 . 1 .
aging	<value>	Specify the number of days after which data is aged out. Valid values are 1 to 60.
insertion-time	<value>	Specify the insertion request threshold. Valid values are 60 to 86400. Link insertion is where a modem performs an initial maintenance procedure to establish a link with the CMTS. A cable modem is placed in the flap list if it makes insertion requests more frequently than the period of time defined by this command.
power-adjust	<value>	Specify the power -adjust threshold. Valid values are 1 to 10. Power-adjust represents the number of times the CMTS tells a cable interface to adjust the transmit power. A modem is placed in the flap list when it's power adjustment exceeds the configured threshold value. Constant power adjustments are an indication of upstream plant problems like amplifier degradation, poor connections, or attenuation problems.
miss	<value>	Specify the miss threshold. Valid values are 1 or *. Miss specifies the number of MAC-layer keepalive misses. If the CMTS does not receive a response from the cable modem, the event is counted as a miss. A large number of misses is an indication of potential problems on the upstream side.

Restrictions

None.

Example

To set up a flap list for cm.7.1 enter the following:

```
cmts set flapthresh cm.7.1 aging 30 insertion-time 60 miss *
```

cmts set headend

Mode

Configure

Format

```
cmts set headend <port-list> {mic-check <skip | do-not-skip> | mac-check <skip | do-not-skip> |
tftp-check <skip | do-not-skip> | auth-str <string> | state <on | off> | default-vlan <string> |
tftp-ip-check <skip | do-not-skip> | client-mac-move <allow | disallow | allow-inform |
disallow-inform> | upstream-extended-freq <on | off> | hcs-err <fwd | drop> | fcs-err <fwd | drop>
| anti-ip-spoofing <enable | disable> | anti-dhcp-spoofing <enable | disable> | modem-debug
<enable | disable> | dhcp-ipaddr-snoop <enable | disable> | dhcp-strict <enable | disable> |
relay-agent-circuit-id <add | do-not-add> | relay-agent-remote-id <add | do-not-add>
```

Description

The **cmts set headend** command sets parameters for the headend manager.

Parameter	Value	Meaning
headend	<port-list>	This is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
mic-check		Specifies whether or not to perform the MIC check at startup.
	skip	Specify to skip the MIC check.
	do-not-skip	Specify to perform the MIC check.
mac-check		Specifies whether or not to perform the MAC check at startup.
	skip	Specify to skip the MAC check.
	do-not-skip	Specify to perform the MAC check.
tftp-check		Specifies whether or not to perform the TFTP check at startup.
	skip	Specify to skip the TFTP check.
	do-not-skip	Specify to perform the TFTP check.
auth-str	<string>	Specifies an authorization string in text or hexadecimal format. To use this option a string must be specified.
state		Specifies the state of the headend.
	on	Specifies that the headend is enabled.
	off	Specifies that the headend is disabled.
default-vlan	<string>	Specifies the name of the default VLAN to which modems are added.

Parameter	Value	Meaning
tftp-ip-check		Specifies checking IP TFTP.
	skip	Specify to not check IP TFTP.
	do-not-skip	Specify to check IP TFTP.
client-mac-move		Specifies to allow the client MAC to move between modems and whether or not a warning message is displayed when such a move occurs.
	allow	Specify to allow the client MAC to move between modems.
	disallow	Specify to disallow the client MAC to move between modems.
	allow-inform	Specify to display a warning message when the client MAC is moved.
	disallow-inform	Specify to not display a warning message when the client MAC is moved.
upstream-extended-freq		Use this parameter to enable (on) or disable (off) the upstream extended frequency range. The extended frequency range is 42 to 65 Mhz.
	on	Specify to enable upstream extended frequency.
	off	Specify to disable upstream extended frequency.
hcs-err		Specify to forward or drop packets with header checksum errors.
	fwd	Specify to forward packets.
	drop	Specify to drop packets.
fcs-err		Specify to forward or drop packets with frame checksum errors.
	fwd	Specify to forward packets.
	drop	Specify to drop packets.
anti-ip-spoofing		Enables anti-IP spoofing checks.
	enable	Specify enable to do the check.
	disable	Specify disable not to do the check.
anti-dhcp-spoofing		Enables anti-DHCP spoofing checks.
	enable	Specify enable to do the check.
	disable	Specify disable not to do the check.
modem-debug		Use this parameter to snoop packets for modem debug information.
	enable	Specify enable to snoop packets.

Parameter	Value	Meaning
	disable	Specify disable to not snoop packets.
dhcp-ipaddr-snoop		Use this parameter to snoop DHCP packets for client IP information.
	enable	Specify enable to snoop packets.
	disable	Specify disable to not snoop packets.
dhcp-strict		Use this parameter to enable or disable DHCP strict enforcement.
	enable	Specify enable to ensure that all modems and clients use DHCP.
	disable	Specify disable to ensure that all modems and clients do not use DHCP.
relay-agent-circuit-id		Specify to enable or disable adding the relay agent circuit ID.
	add	Specify add to add the relay agent circuit ID.
	do-not-add	Specify do-not-add to add the relay agent circuit ID.
relay-agent-remote-id		Specify to enable or disable adding the relay agent remote ID.
	add	Specify add to add the relay agent remote ID.
	do-not-add	Specify do-not-add to add the relay agent remote ID.

**Note**

Client MAC address movement may occur when a technician is setting up or repairing more than one modem which communicates with a particular headend.

Restrictions

When an authentication string is entered, it is encrypted and saved in the configuration file. When you look at the configuration file it will appear as the following:

```
cmts set headend <port> hashed-auth-string <encrypted string>
```

rather than:

```
cmts set headend <port> auth-string <string>
```

cmts set ipc-local

Mode

Enable

Format

```
cmts set ipc-local <port> <fast | slow>
```

Description

Sets the speed of the local IPC.

Parameter	Value	Meaning
ipc-local	<port>	The variable <i>port</i> is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
fast		Specifies the speed of the interface as fast.
slow		Specifies the speed of the interface as slow.

Restrictions

None.

cmts set ipc-main

Mode

Enable

Format

cmts set ipc-main <fast | slow>

Description

Sets the speed of the main IPC interface.

Parameter	Value	Meaning
fast		Specifies the speed of the interface as fast.
slow		Specifies the speed of the interface as slow.

Restrictions

None.

cmts llc-ping

Mode

Enable

Format

```
cmts llc-ping <value> xid test
```

Description

This command forwards a ping request to a destination MAC address.

Parameter	Value	Meaning
llc-ping	<value>	Specifies a destination MAC address to ping, in the form XX:XX:XX:XX:XX:XX or XXXXXX:XXXXXX.
xid		Specify this parameter to send out an XID frame.
test		Specify this parameter to send out a TEST frame.

Restrictions

None.

cmts set mac

Mode

Enable

Format

```
cmts set mac <port-list> {sync-interval <value> | ucd-interval <value> |
inv-range-attempts <value> | map-length <value> | map-lead-time <value> |
init-maint-length <value> | insert-interval <value> | vendor-specific} |
non-ip-filter <on | off> | bpdu-filter <on | off> | ucc-retry-interval <number> |
ucc-retries <number>}
```

Description

Sets or modifies the RFI CMTS MAC interface attribute settings.

Parameter	Value	Meaning
mac	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
sync-interval	<value>	Specifies the SYNC message interval. Valid values are 1 to 200.
ucd-interval	<value>	Specifies the upstream channel descriptor message interval. Valid values are 1 to 2000.
inv-range-attempts	<value>	Specifies the maximum number of ranging request invitations. Valid values are 1 to 1024.
map-length	<value>	Specifies the map length in microseconds. Valid values are 1 to 2000,000. The default value is automatically computed.
map-lead-time	<value>	Specifies the map lead time in microseconds. Valid values are 1 to 2000. The default value is automatically computed.
init-maint-length	<value>	Specifies the initial maintenance interval in microseconds. Valid values are 1 to 2000,000. The default value is 2000 microseconds.
insert-interval	<value>	Specifies the insertion interval in milliseconds. The valid range is 1 to 2000.
	vendor-specific	Specify vendor-specific for non-fixed time vendor specific algorithms.
non-ip-filter		Specifies the use of non-ip filtering.
	on	Specifies using non-ip filtering.
	off	Specifies not using non-ip filtering.

Parameter	Value	Meaning
bpdu-filter		Specifies the use of BPDU filtering.
	on	Specifies using BPDU filtering.
	off	Specifies not using BPDU filtering.
ucc-retry-interval	<number>	Specifies the UCC retry interval.
ucc-retries	<number>	Specifies the number of UCC retries.

Restrictions

None.

cmts set modem

Mode

Configure and
Enable

Format

cmts set modem *<port-list>* macaddr *<value>* [vlan *<string>*] new-upstream-id *<value>*

Description

This command is used to set modem parameters.

Parameter	Value	Meaning
modem	<i><port-list></i>	This is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm . 7 . 1 .
macaddr	<i><value></i>	The MAC address of the modem in the form XX:XX:XX:XX:XX:XX or XXXXXX:XXXXXX.
vlan	<i><string></i>	<i><string></i> is the name of the VLAN to which the modem is to be added. This command is valid in the Configure mode only.
new-upstream-id	<i><value></i>	The string specifies the new DOCSIS upstream channel ID. This command is valid in the Enable mode only.

Restrictions

None.

cmts set modulation

Mode

Configure

Format

```
cmts set modulation <profile_number | all-values> int-usage-code <keyword> {type <qpsk | qam16> |
preamble-len <value> | diff-encoding <on | off> | fec-error-correct <value> | fec-codeword-length
<value> | scrambler-seed <value> | max-burst-size <value> | last-codeword-short <on | off> |
scrambler-enable <on | off> | guard-time-size <value>}
```

Description

This command modifies RFI upstream channel modulation profile settings. When configuring an upstream cable interface using the **cmts set uschannel** command, you can specify a profile that supplies values for upstream channel configuration settings. Up to eight profiles can be configured.

Parameter	Value	Meaning
modulation	<profile_number>	Modifications to profile configuration settings can be made in a single profile or to all the profiles. Up to eight profiles can be configured and used when configuring upstream interfaces. <profile_number> is a number from 1 to 8.
	all-values	Specifying all-values modifies all profiles.
int-usage-code	<keyword>	Is the interval usage code to be modified with this command.
	request	Modify for request type int-usage-code.
	request-data	Modify for request-data type int-usage-code.
	initial-ranging	Modify for initial ranging type int-usage-code.
	periodic-ranging	Modify for periodic ranging type int-usage-code.
	short-data	Modify for short data type int-usage-code.
	long-data	Modify for long data type int-usage-code.
	all-values	Modify for all values of int-usage-code.
type		The modulation type used on a channel.
	qpsk	Equal to 2 bits per second.
	qam16	Equal to 4 bits per second.
preamble-len	<value>	The preamble length for this modulation profile in bits. Valid values are from 2 to 320 bits.
diff-encoding		Specifies whether or not differential encoding is used on a channel.

Parameter	Value	Meaning
	on	Specify to use differential encoding on the channel. This is the default.
	off	Specify to not use differential encoding on the channel.
fec-error-correct	<value>	The number of correctable incorrect bytes used in the FEC code. The valid range is 1 to 10 bytes. The value of 0 indicates no correction is used.
fec-codeword-length	<value>	The number of data bytes in the FEC code word. The valid range is 8 to 254 bits This value is ignored if FEC error correction is zero.
scrambler-seed	<value>	The 15 bit <i>seed value</i> for the scrambler polynomial. The scrambler seed is in hexadecimal format. The valid range is 0x0000 to 0x7FFF.
max-burst-size	<value>	The maximum burst length in bytes. Valid values are 0 to 255. 0 means no limit on the burst length.
last-codeword-short		Indicates the handling FEC for the last code word.
	on	Fixed codeword length.
	off	Truncated last code word.
scrambler-enable		Indicates if the scrambler is used.
	on	Scrambler is used. This is the default.
	off	Scrambler is not used.
guard-time-size	<value>	Number of symbols of guard time following the burst. Valid values are 0 to 255.

Restrictions

None.

cmts set multicast-ip

Mode

Configure

Format

```
cmts set multicast-ip <port-list> ipaddr <address> prefix-length <value> sid <value>
```

Description

Create a multicast map entry. This command matches a multicast traffic flow with a multicast SID.

Parameter	Value	Meaning
multicast-ip	<port-list>	The variable <i>port-list</i> is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
ipaddr	<address>	Specify a multicast IP address.
prefix-length	<value>	Specify a multicast IP address prefix length. Valid values are 1 to 32.
sid	<value>	Specify a multicast map SID. Valid values are 8192 to 16368.

Restrictions

None.

Example

The following example shows mapping from a multicast IP address to a multicast SID.

```
cmts set multicast-ip cm.5.1 ipaddr 224.1.1.1 prefix-length 32 sid 9000
```

cmts set multicast-sid

Mode

Configure

Format

```
cmts set multicast-sid <port-list> macaddr <value> sid <id>
```

Description

This command creates a mapping between a multicast SID and a specific cable modem.

Parameter	Value	Meaning
multicast-sid	<port-list>	The variable <i>port-list</i> is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1.
macaddr	<address>	Specify a multicast privacy MAC address in the form XX:XX:XX:XX:XX:XX or XXXXXX:XXXXXX.
sid	<value>	Specify a multicast map SID. Valid values are 8192 to 16368.

Restrictions

None.

Example

The following command allows the flow on the multicast SID 9000 to be delivered to the cable modem with a MAC address of 008043:64ABAC.

.

```
cmts set multicast-sid cm.5.1 sid 9000 macaddr 008043:64ABAC
```

cmts set privacy

Mode

Configure

Format

```
cmts set privacy <port-list> {[ak-lifetime <value>]} [tek-lifetime <value>]}
```

Description

Sets or modifies baseline privacy attributes.

Parameter	Value	Meaning
privacy	<port-list>	This is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
ak-lifetime	<value>	Specifies the <i>lifetime</i> a CMTS assigns to a new authorization key. Valid values are 1 to 604800.
tek-lifetime	<value>	Specifies the <i>lifetime</i> the CMTS assigns to a new traffic key. Valid values are 1 to 604800.

Restrictions

None.

Example

The following command specifies an authorization key lifetime of 600 and a new traffic 180.

```
cmts set privacy cm.5.1 ak-lifetime 600 tek-time 180
```


cmts set relay-agent

Mode

Configure

Format

```
cmts set relay-agent interface <name> giaddr <address>
```

Description

This command sets the GI address of the relay agent.

Parameter	Value	Meaning
interface	<name>	Specifies the name of the interface being set.
giaddr	<address>	Specifies the IP address of the relay agent.

Example

The following command set the GI address of the CMTS interface.

```
cmts set relay agent interface cmts giaddr 10.20.1.1
```

cmts set tek

Mode

Enable

Format

cmts set tek <port-list> sid <value> {[tek-lifetime <value>]} [tek-gracetime <value>]}

Description

This command modifies the attributes of the CM Traffic Encryption Key (TEK).

Parameter	Value	Meaning
tek	<port-list>	Specifies the name of the interface being set.
sid	<value>	This is the traffic key service identifier.
tek-lifetime	<value>	Lifetime, in seconds, the CMTS assigns to keys for this TEK association. Valid values are 1 to 604800.
tek-gracetime	<value>	Gracetime in seconds. Valid values are 1 to 1800.

Restrictions

None.

cmts set uschannel

Mode

Enable

Format

```
cmts set uschannel <port-list> upstream <range | all> {frequency <num> | width <value> | power <value> |
modulation-profile <value | *> | slot-size <value> | range-back-off-start <value> |
range-backoff-end <value> | tx-backoff-start <value> | tx-backoff-end <value> | power-adj <value> |
state <on | off> | policing <on | off> | policing-alarm <on | off> | qos-confirm <on | off> |
qos-max-bps <number>}
```

Description

Set or modify attributes for upstream channels.

Parameter	Value	Meaning
uschannel	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
upstream	<range>	Specifies a specific upstream channel or a range of channels.
	all	Specify all to modify information for all the upstream channels.
frequency	<num>	Specify the center of the frequency band for this upstream channel. Valid values are 5000000 to 42000000.
width	<value>	Specify the bandwidth in kHz for this upstream channel. Valid values are 200, 400, 800, 1600, and 3200.
power	<value>	Specify the input power level for this channel. Valid values are -16dB to 26dB.
modulation-profile	<value>	Specify the profile. Valid values are 1 and above.
	*	Specify a value depending on the index shown in the cmts show modulation command.
slot-size	<value>	Specify the slot size in the number of 6.25 microsecond ticks in each upstream channel. Valid values are 1 to 128.
range-back-off-start	<value>	Specify the start of the random backoff window for retrying ranging.
range-backoff-end	<value>	Specify the end of the random backoff window for retrying ranging.
tx-backoff-start	<value>	Specify the start of the random backoff window for retrying transmission.

Parameter	Value	Meaning
tx-backoff-end	<value>	Specify the end of the random backoff window for retrying transmission.
power-adj	<value>	Specify the maximum power adjustment in 1/4 dB units. The valid range is 0 to 255.
state		Enables or disables the upstream channel.
	on	Specify on to enable the upstream channel.
	off	Specify off to disable the upstream channel.
policing		Specifies policing on the upstream channel.
	on	Specify on to enable policing on the upstream channel.
	off	Specify off to disable policing on the upstream channel.
policing-alarm		Specifies the policing alarm on the upstream channel.
	on	Specify on to enable the policing alarm on the upstream channel.
	off	Specify off to disable the policing alarm on the upstream channel.
qos-confirm		Specifies QOS confirmation on the upstream channel.
	on	Specify on to enable QOS confirmation on the upstream channel.
	off	Specify off to disable QOS confirmation on the upstream channel.
qos-max-bps	<number>	Specifies the number of QOS bits per-second on the upstream channel.

Restrictions

None.

Example

To enable all the upstream channels, enter:

```
cmts set all-ports upstream all state on
```

cmts show ak

Mode

Enable

Format

cmts show ak <port-list | all-ports> [macaddr <value | all-macs>]

Description

Displays the authorization key attributes.

Parameter	Value	Meaning
ak	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
	all-ports	Specify all-ports to view or modify all ports.
macaddr	<value>	Specify to show the authorization key values for a particular MAC in the form xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.
	all-macs	Specify to show the authorization key values for all MACs.

Restrictions

None.

Example

To display authorization key values, enter:

```
cmts show ak cm.5.1 macaddr 001095:02D08B
```

Here is what displays after the **cmts show ak** command is entered:

```
CMTS Authorization Key Parameters
Port: cm.5.1          MAC: 001095:02D08B
CM Public Key       : 00 BC 65 0C D7 0D 68 97 CB 23 B3 F0 AC FB 56 7E 0D
21 81 A9 95 6A 9B FA 9F B4 AC 34 CA 3B 3D 32 74 39 D5 05 A9 62 91 17 77
44 19 9B F1 F5 E2 EC 55 48 52 48 4C 49 62 D0 73 0C ED 5A A9 8A 4A 6A 91
B6 1F ED C4 5D 66 DD 2E 0D 99 3A A7 2A 29 51 58 3B C2 BE 5D 56 EA CD 12
F0 8A 8D C7 01 B2 51 15
AK Sequence         : 7
AK Expiration        : 447
AK Lifetime          : 600
AK Gracetime         : 60
AK Reset             : No Reset Requested
AK Requests          : 8
AK Replys            : 8
AK Rejects           : 0
AK Invalids          : 0
AK Reject Error      : None
AK Invalid Error     : None
```

cmts show dschannel

Mode

Enable

Format

cmts show dschannel <port-list | all-ports> [downstream <channel_range | all>]

Description

Lists attributes for downstream channels.

Parameter	Value	Meaning
dschannel	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
	all-ports	Specify all-ports to view all ports.
downstream	<channel_range>	Specify a channel, range of channels, or all channels to show CMTS downstream port information.
	all	Specify to show the downstream port information for all downstream ports.

Restrictions

None.

Example

To display the downstream channel parameter values enter:

```
cmts show dschannel all-ports downstream all
```

Here is what displays after the **cmts show dschannel** command is entered:

```
Downstream Channel Parameters
Port: cm.5.1   CATV Downstream Channel: 1
  DS Channel ID       : 91
  DS Channel Frequency : 345000000
  DS Channel Bandwidth : 6000000
  DS Channel Modulation Type : QAM64
  DS Channel FEC Interleaving : 128
  DS Channel Power Level : 0
  IP Broadcast        : On
  IP Multicast        : On
  Downstream State    : On
  Annex Mode         : B
Port: cm.6.1   CATV Downstream Channel: 1
  DS Channel ID       : 97
  DS Channel Frequency : 345000000
  DS Channel Bandwidth : 6000000
  DS Channel Modulation Type : QAM64
  DS Channel FEC Interleaving : 128
  DS Channel Power Level : 0
  IP Broadcast        : On
  IP Multicast        : On
  Downstream State    : On
  Annex Mode         : B
```


cmts show error-stats

Mode

Enable

Format

cmts show error-stats <port-list | all-ports> {[all] | [downstream <range> | all] | [upstream <range> | all]}

Description

Displays error statistics.

Parameter	Value	Meaning
error-stats		Display error statistics.
	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to show all ports.
all		Specify all to show all ports, both upstream and downstream.
downstream		Specify downstream to show downstream or transmit ports.
	<range>	The variable <i>range</i> takes a range of port numbers. This is the range of downstream ports that you want to display. For multiple port specification, you can use commas, ranges, or the * character.
	all	Specify all to display all downstream ports.
upstream		Specify upstream to show upstream or receive ports.
	<range>	The variable <i>range</i> takes a range of port numbers. This is the range of upstream ports that you want to display. For multiple port specification, you can use commas, ranges, or the * character.
	all	Specify all to display all upstream ports.

Restrictions

None.

Example

To display error statistics enter:

```
cmts show error-stats cm.5.1
```

Here is what displays after the **cmts show error-stats** command is entered:

```
Error Statistics
Port: cm.5.1   CATV Downstream Channel: 1
  Errored Packets: 0
  Packets Discarded: 0
  Unknown Protocol Packets: 0
```

Note When Packets Discarded displays a 0, the headend, modem, or SID is disabled.

cmts show flap-list

Mode

Enable

Format

cmts show flap-list

Description

Displays a list of modems that are flapping.

Restrictions

None.

Example

To display a list of modems that are flapping, enter:

```
cmts show flap-list
```

Here is what displays after the **cmts show flap-list** command is entered:

Flap List Statistics							
MAC Address	Port	US	Ins	Miss	P-Adj	Flap	Date & Time
001095:02be60	cm.6.1	3	1	1	0	2	2000-05-02 14:59:49
009083:32E1A8	cm.5.1	2	1	2	1	4	2000-04-30 18:36:23

cmts show flap-thresh

Mode

Enable

Format

cmts show flap-thresh <port-list | all-ports>

Description

Display the flap list threshold settings.

Parameter	Value	Meaning
flap-thresh	<port-list>	This is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
	all-ports	Specify all-ports to view information for all ports.

Restrictions

None.

Example

To display the flap list thresholds enter:

```
cmts show flap-thresh all-ports
```

Here is what displays after the **cmts show flap-thresh** command is entered:

```
Flap List Threshold Settings
Port: cm.5.1
Flaplist State           : Enabled
Table Aging              : 20 days
Table Size               : 80 modems
Insertion Request Threshold : 60 seconds
Miss Threshold           : 10 misses
Power Adjust Threshold   : 10 dBmV

Port: cm.6.1
Flaplist State           : Enabled
Table Aging              : 10 days
Table Size               : 20 modems
Insertion Request Threshold : 40 seconds
Miss Threshold           : 15 misses
Power Adjust Threshold   : 10 dBmV
```

cmts show headend

Mode

Configure

Format

cmts show headend *<port-list | all-ports>*

Description

The **cmts show headend** command displays a list of the current of the CMTS headend setting.

Parameter	Value	Meaning
headend	<i><port-list></i>	<i><port-list></i> is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
	all-ports	Specify all-ports to view headend information for all ports.

Restrictions

None.

Examples

To display headend settings enter:

```
cmts show headend all-ports
```

The following displays:

```
Headend : cm.5.1
  State           : On
MIC Check         : Do not Skip
MAC Check         : Do not Skip
TFTP Check        : Do not Skip
Client MAC Move   : Disallow
Client MAC Move Msgs : Silent
Headend : cm.6.1
  State           : On
MIC Check         : Do not Skip
MAC Check         : Do not Skip
TFTP Check        : Do not Skip
Client MAC Move   : Disallow
Client MAC Move Msgs : Silent
```

cmts show mac

Mode
Enable

Format

cmts show mac <port-list | all-ports>

Description

Displays the MAC interface settings.

Parameter	Value	Meaning
mac	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
	all-ports	Specify all-ports to view information for all ports.

Restrictions

None.

Example

To display MAC interface settings, enter:

```
cmts show mac all-ports
```


The following displays:

CMTS MAC Parameters

Port: cm.5.1

Capabilities	:	None
Sync Interval	:	10 MilliSeconds
UCD Interval	:	2000 MilliSeconds
Max Service IDs	:	16383
Ranging Invitation Attempts	:	16
Map Length	:	4000 Microseconds
Map Lead Time	:	6000 Microseconds
Initial Maintenance Length	:	2000 Microseconds
Insertion Interval	:	500 MilliSeconds
UCC Retry Interval	:	2000 MilliSeconds
Max UCC Retries	:	3

Port: cm.6.1

Capabilities	:	None
Sync Interval	:	10 MilliSeconds
UCD Interval	:	2000 MilliSeconds
Max Service IDs	:	16383
Map Length	:	4000 Microseconds
Map Lead Time	:	6000 Microseconds
Initial Maintenance Length	:	2000 Microseconds
Insertion Interval	:	500 MilliSeconds
UCC Retry Interval	:	2000 MilliSeconds
Max UCC Retries	:	3

cmts show map-stats

Mode
Enable

Format

cmts show map-stats <port-list | all-ports> [upstream <range> | all]

Description

This command displays map statistics.

Parameter	Value	Meaning
map-stats	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to show map statistics for all ports.
upstream		Specify upstream to display upstream map statistics
	<range>	The variable <i>range</i> takes a range of port numbers. This is the range of upstream ports that you want to display. For multiple port specification, you can use commas, ranges, or the * character.
	all	Specify all to display all ports.

Restrictions

None.

Example

To display map statistics enter:

```
cmts show map-stats all-ports
```

Here is an example of the output of the **cmts show map-stats** command:

```
Map Information
Port: cm.5.1
Maps 281850663 Late 1 LateTime 23264
CATV Upstream Channel: 1
Ack Reqs 0 Alloc 0 Full 0 NoSID 0
BW Reqs 0 Piggy 0 Slots 0 Alloc 0 Slots 0
BW Dup 0/0 Full 0 NoSID 0 MaxBW 0 MaxBurst 0
Map Full 0 RFull 0 NoSID 2162/260260 Ack 0 Age 0
Map DelayM 0 DelayG 0 UCDDGap 1
Map PerRng 0 IM 33 Reqs 86440/86440
Data: Alloc 1 Lost 1 FEC 0, HCS 0
Req: Alloc 86360 Coll 0 Error 0, NoEnergy 86360
ReqData: Alloc 0 Coll 0 Error 0, NoEnergy 0
Range: Req 0 Error 0
FECBlks: Tot 1 UnCor 0 Cor 0
CATV Upstream Channel: 2
Upstream State      : Off
CATV Upstream Channel: 3
Upstream State      : Off
CATV Upstream Channel: 4
Upstream State      : Off
```

Table 10-2 Display Field Descriptions for the cmts show map-stats Command

Field	Description
Maps	The number of upstream maps generated since the last time map statistics were cleared.
Late	The number of upstream maps that were delayed at generation.
LateTime	The delay time in <i>ticks</i> . (One tick is equal to 6.25 usec.)
CATV Upstream Channel:	
Ack Reqs	The number of requests for acknowledgement of a received data packet.
Alloc	The number of acknowledgements sent to modems.
Full	The number of acknowledgements that were not sent because the request queue was full.
NoSID	The number of acknowledgements that did not match a SID.
BW Reqs	The number of requests for bandwidth.
Piggy	The number of piggybacked requests for bandwidth.
Slots	The number of slots requested.
Alloc	The number of requests for bandwidth allocated.
Slots	The number of slots allocated for bandwidth.

Field	Description
BW Dup	The number of duplicated requests for bandwidth.
Full	The number of requests missed because the request queue was full
NoSID	The number of requests that did not match a SID.
MaxBW	The number of requests that exceeded the maximum bandwidth.
MaxBurst	The number of requests that exceeded the maximum burst.
Map Full	The number of full upstream maps.
RFull	The number of full maps exceeded by range requests.
NoSID	The number of null SIDs sent. / The number of slots used by null SIDs.
Ack	The number of bandwidth acknowledgements.
Age	The number of delayed requests for bandwidth.
Map DelayM	The number of requests for bandwidth that are delayed because the modem was not ready to transmit.
DelayG	The number of requests for bandwidth that are moved to the next map.
UCDGap	The number of gaps added to the map because of a change in UDC (Upstream Channel Descriptor).
Map PerRng	The number of modems that are periodic ranged.
IM	The number of initial maintenances.
Reqs	The number of multicasted requests sent. / The number of slots for these requests.
Data:	
Alloc	The number of packets allocated.
Lost	The number of data packets not received.
FEC	The number of errors with FEC.
HCS	The number of errors with HCS.
Req:	
Alloc	The number of request packets allocated.
Coll	The number of request packet collisions.
Error	The number of FEC errors.
NoEnergy	The number of request packets with no energy.
Range:	
Req	The number of ranging packets received.
Error	The number of FEC errors with ranging packets.
FECBlks:	

Field	Description
Tot	The number of FEC blocks received.
UnCor	The number of uncorrectable FEC blocks.
Cor	The number of correctable FEC blocks.

cmts show misc-stats

Mode
Enable

Format

cmts show misc-stats <port-list> | all-ports

Description

This command displays miscellaneous statistics.

Parameter	Value	Meaning
misc-stats	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm.7.1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to show miscellaneous statistics for all ports.

Restrictions

None.

Example

To display miscellaneous statistics for all ports enter:

```
cmts show misc-stats all-ports
```

Here is an example of the output of the **cmts show misc-stats** command:

```
Miscellaneous Statistics
Port: cm.5.1
DHCP Spoofs: 0
IP Spoofs: 0
Port: cm.5.2
DHCP Spoofs: 0
IP Spoofs: 0
```

cmts show modem

Mode

Enable

Format

cmts show modem <port-list | all-ports> macaddr <value | all-macs> [detailed]

Description

Displays modem parameters.

Parameter	Value	Meaning
modem	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
	all-ports	Specify all-ports to view information for all ports.
macaddr	<value>	The MAC address of the modem in the form XX:XX:XX:XX:XX:XX or XXXXXX:XXXXXX.
	all-macs	Specify all-macs to view information for all MAC addresses.
detailed		Displays detailed information

Restrictions

None.

Example

To display the modem parameters, enter:

```
cmts show modem all-ports
```

The following displays:

CMTS Modems Parameters						
Port: cm.5.1		Modems: 22				
MAC Addr	IP Addr	DS/US	En	Reg	BPI	SID
0000F0:26A2C1	50.2.1.14	1/1	X	X	-	178
0000F0:26BDA1	50.2.1.10	1/1	X	X	-	53
0000F0:26BDA9	50.2.1.26	1/1	X	X	-	79
001095:02CDCD	50.2.1.31	1/2	X	X	X	21
001095:02CDCE	50.2.1.29	1/3	X	X	X	81
005009:001DE9	50.2.1.53	1/1	X	X	X	59
0050DA:9D07D6	50.2.1.51	1/1	X	X	X	70
0050DA:A4FEDC	50.2.1.43	1/1	X	X	X	71
0050DA:A4FEE0	50.2.1.42	1/1	X	X	X	69
009083:3037E6	50.2.1.18	1/1	X	X	X	56
009083:3037E7	50.2.1.32	1/1	X	X	X	76
009083:32E1AB	50.2.1.28	1/1	X	X	X	189
009083:32E1AC	50.2.1.21	1/2	X	X	X	14 8192
009083:32E1AE	50.2.1.24	1/1	X	X	X	74
009096:00B2A1	50.2.1.47	1/1	X	X	X	77
009096:00F24A	50.2.1.50	1/2	X	X	X	8
00A073:16B0EC	50.2.1.17	1/1	X	X	X	57 8192
00E06F:000060	50.2.1.41	1/2	X	X	X	27
00E06F:0000B7	50.2.1.13	1/1	X	X	X	75
00E0CA:00917F	50.2.1.46	1/2	X	X	X	7
00E0CA:009180	50.2.1.45	1/3	X	X	X	9
Port: cm.6.1		Modems: 8				
MAC Addr	IP Addr	DS/US	En	Reg	BPI	SID
001095:02BE60	50.3.1.33	1/1	X	X	X	15 8192
001095:02CDEB	50.3.1.20	1/3	X	X	X	21 8192
001095:02CDF5	50.3.1.17	1/3	X	X	X	19
001095:02CE29	50.3.1.32	1/3	X	X	X	20
009083:32E1A8	50.3.1.19	1/1	X	X	X	59
009083:32E1AF	50.3.1.15	1/1	X	X	X	61
009083:32E1B0	50.3.1.16	1/1	X	X	X	60
00E0CA:00917E	50.3.1.42	1/3	X	X	X	67

cmts show modulation

Mode

Enable

Format

cmts show modulation <index | all-values> interval-usage-code <code-type> [verbose]

Description

Describes a modulation profile associated with one or more upstream channels.

Parameter	Value	Meaning
modulation	<index>	Specify a particular index.
	all-values	Specify all-values to display RFI upstream channel modulation profile settings for all index values.
interval-usage-code	<code-type>	Specify the type of codes to display.
	request	Displays request type int-usage-code.
	request-data	Displays request data type int-usage-code.
	initial-ranging	Displays initial ranging type int-usage-code.
	periodic-ranging	Displays periodic ranging type int-usage-code.
	short-data	Displays short data type int-usage-code.
	long-data	Displays long data type int-usage-code.
	all-values	Displays all values of int-usage-code.
verbose		Select verbose to view modulation data in detail.

Restrictions

None.

Example

To display modulation settings enter:

```
cmts show modulation all-values int-usage-code all-values
```

The following displays:

Cmts Modulation Settings												
Index	Int	Mod	Pre	Diff	Fec		Max	Gard	Last			
	Usag	Type	Len	Encl	Fec	Data	Brst	Time	Cdwd	Scr	Trun	Enbl
	Code			Enbl		Byte	Seed	Size	Size			
1	Req	Qpsk	64	Off	0	6	338	2	8	Fixed	On	
1	Reqdata	Qpsk	64	Off	0	6	338	2	8	Fixed	On	
1	Initrng	Qpsk	128	Off	5	34	338	0	48	Fixed	On	
1	Perrng	Qpsk	128	Off	5	34	338	0	48	Fixed	On	
1	Shtdata	Qpsk	72	Off	5	75	338	12	8	Fixed	On	
1	Lngdata	Qpsk	80	Off	8	220	338	0	8	Fixed	On	
2	Req	Qam16	64	Off	0	16	338	1	8	Fixed	On	
2	Reqdata	Qam16	64	Off	0	16	338	1	8	Fixed	On	
2	Initrng	Qam16	128	Off	5	34	338	0	48	Fixed	On	
2	Perrng	Qam16	128	Off	5	34	338	0	48	Fixed	On	
2	Shtdata	Qam16	72	Off	5	75	338	6	8	Fixed	On	
2	Lngdata	Qam16	80	Off	8	220	338	0	8	Fixed	On	
5	Req	Qpsk	64	Off	0	16	338	2	8	Fixed	On	
5	Reqdata	Qpsk	64	Off	0	16	338	1	8	Fixed	On	
5	Initrng	Qpsk	128	Off	5	34	338	0	48	Fixed	On	
5	Perrng	Qpsk	128	Off	5	34	338	0	48	Fixed	On	
5	Shtdata	Qam16	144	Off	5	78	338	8	8	Short	On	
5	Lngdata	Qam16	160	Off	10	235	338	0	8	Short	On	

cmts show multicast-ip

Mode

Enable

Format

cmts show multicast-ip <port-list | all-ports> ipaddr <value | all-ips> prefix-length
<value | all-length>

Description

This command displays multicast map attributes.

Parameter	Value	Meaning
multicast-ip	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
	all-ports	Specify all-ports to view all ports.
ipaddr	<value>	Specify the multicast IP address.
	all-ips	Specify all-ips to view all ip addresses.
prefix-length	<value>	Specify the multicast IP address prefix length. Valid values are 1 to 32.
	all-length	Specify all-length to view all IP addresses of any prefix length.

Restrictions

None.

cmts show multicast-sid

Mode

Enable

Format

cmts show multicast-sid <port-list | all-ports> macaddr <value | all-macs> sid <id | all-sids>

Description

This command displays multicast privacy attributes.

Parameter	Value	Meaning
multicast-sid	<port-list>	This is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
	all-ports	Specify all-ports to view all ports.
macaddr	<value>	Specify the multicast privacy MAC address in the form xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.
	all-macs	Specify all-macs to view all MAC addresses.
sid	<id>	Specify the multicast map SID. Valid ID values are 8192 to 16368.
	all-sids	Specify all-sids to view all ID values.

Restrictions

None.

cmts show packet-stats

Mode

Enable

Format

```
cmts show packet-stats <port-list | all-ports> {[all] | [downstream <range> | all] | [upstream <range> | all]}
```

Description

This command displays packet statistics.

Parameter	Value	Meaning
packet-stats	<port-list>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm. 7. 1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
	all-ports	Specify all-ports to show all ports.
all		Specify all to show all ports, both downstream and upstream.
downstream	<range>	Specify downstream to show downstream or transmit ports. The variable <i>range</i> takes a range of port numbers. This is the range of downstream ports that you want to display. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to display all downstream ports.
upstream	<range>	Specify upstream to show upstream or receive ports. The variable <i>range</i> takes a range of port numbers. This is the range of upstream ports that you want to display. For multiple port specification you can use commas, ranges, or the * character.
	all	Specify all to display all upstream ports.

Restrictions

None.

cmts show privacy

Mode
Enable

Format

cmts show privacy <port-list | all-ports>

Description

Displays the baseline privacy attributes of the CMTS.

Parameter	Value	Meaning
privacy	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
	all-ports	Specify all-ports to view all ports.

Restrictions

None.

Example

To display the baseline privacy settings, enter:

```
cmts show privacy all-ports
```

The following displays:

```
CMTS Base Parameters
Port: cm.5.1
  BPI State      : Enabled
  AK Lifetime    : 600
  TEK Lifetime   : 300
AK Requests     : 20
  AK Replies     : 20
  AK Rejects     : 0
  AK Invalids    : 0
Port: cm.6.1
  BPI State      : Enabled
  AK Lifetime    : 600
  TEK Lifetime   : 300
  AK Requests    : 20
  AK Replies     : 20
  AK Rejects     : 0
  AK Invalids    : 0
```

cmts show qosprofile

Mode

Enable

Format

```
cmts show qosprofile <port-list | all-ports> id <id | all>
```

Description

Displays the QOS profile settings.

Parameter	Value	Meaning
privacy	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7 . 1 .
	all-ports	Specify all-ports to view all ports.
id	<id>	Class of service ID. Valid values for <i>id</i> are 1 to 16.
	all	Specify all to display class of service settings for all service IDs.

Restrictions

None.

Example

To display a QOS profile, enter:

```
cmts show qosprofile all-ports id all
```


The following displays:

```
CMTS QoS Profile Settings
Port: cm.5.1
Index: 1
Relative Priority           : 1
Max Upstream Bandwidth     : 1000000    bps
Min Guaranteed Upstream Bandwidth : 0      bps
Max Downstream Bandwidth   : 1000000    bps
Max Mini-slot Burst        : No Limit
Baseline Privacy Enable    : On
Port: cm.6.1
Index: 1
Relative Priority           : 1
Max Upstream Bandwidth     : 1000000    bps
Min Guaranteed Upstream Bandwidth : 0      bps
Max Downstream Bandwidth   : 1000000    bps
Max Mini-slot Burst        : No Limit
Baseline Privacy Enable    : On
```

cmts show qosprofpermissions

Mode

Enable

Format

cmts show qosprofpermissions

Description

Displays the QOS profile permission settings.

Restrictions

None.

Example

To display the QOS profile permissions, enter:

```
cmts show qosprofpermissions
```

The following displays:

```
QOS Profile Permissions
Permission Type : Create by Modem
```

cmts show signalquality

Mode

Enable

Format

cmts show signalquality <port-list | all-ports> upstream <range | all>

Description

At the CM, **cmts show signalquality** describes the PHY signal quality of downstream channels. At the CMTS, this facility describes the PHY signal quality of upstream channels



Note The display when this show command is issued may exclude the field Contention Intervals.

Parameter	Value	Meaning
signalquality	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
	all-ports	Specify all-ports to view all ports.
upstream	<range>	Specify the upstream ports to be displayed. <range> is a range of ports to be displayed.
	all	Specify all to display all ports.

Restrictions

None.

cmts show service

Mode

Enable

Format

cmts show service *<port-list | all-ports>* id *<range | all-values>*

Description

Displays the attributes of upstream service queues in a CMTS.

Parameter	Value	Meaning
service	<i><port-list></i>	This is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
	all-ports	Specify all-ports to view all ports.
id	<i><range></i>	Specify the ID or range of service value IDs. The valid ID range is 1 to 16383.
	all-values	Specify all-values to display all id values.

Restrictions

None.

cmts show status

Mode

Enable

Format

cmts show status *<port-list | all-ports>*

Description

Shows RFI MAC layer status objects and counters settings.

Parameter	Value	Meaning
status	<i><port-list></i>	<i><port-list></i> is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm.7.1 .
	all-ports	Specify all-ports to view all ports.

Restrictions

None.

Example

To display port status enter:

```
cmts show status all-ports
```

The following displays:

```
CMTS Status Parameters
Port: cm.5.1
  Invalid Range Requests      : 8
  Aborted Range Attempts     : 0
  Invalid Registration Requests : 0
  Failed Registration Attempts : 0
  Invalid Data Requests       : 0
  T5 Timeouts                 : 0
Port: cm.6.1
  Invalid Range Requests      : 0
  Aborted Range Attempts     : 0
  Invalid Registration Requests : 0
  Failed Registration Attempts : 0
  Invalid Data Requests       : 0
  T5 Timeouts                 : 0
```

cmts show tek

Mode

Enable

Format

cmts show tek <port-list | all-ports> sid <value> | all-sids

Description

This command shows Traffic Encryption Keys (TEKs) used to encrypt upstream and downstream data traffic.

Parameter	Value	Meaning
tek	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
	all-ports	Specify all-ports to view all ports.
sid	<value>	Specify a SID to display it's traffic key values. The valid range is 1 to 16368.
	all-sids	Specify all-values to display the traffic key values for all service IDs.

Restrictions

None.

Example

To display the traffic encryption keys enter:

```
cmts show tek all-ports sid 1
```

The following displays:

```
CMTS Traffic Key Parameters
Port: cm.5.1          No Information
Port: cm.6.1          SID: 1
  TEK Lifetime       : 300
  TEK Gracetime      : 60
  TEK Old Expiration : 0
  TEK New Expiration : 144
  TEK Requests       : 24
  TEK Replies        : 24
  TEK Rejects        : 0
  TEK Invalids       : 0
  TEK Reject Error   : None
  TEK Invalid Error  : None
```


cmts show uschannel

Mode

Enable

Format

cmts show uschannel <port-list | all-ports> [upstream <range> | all]

Description

Displays a list of attributes for upstream channels.

Parameter	Value	Meaning
uschannel	<port-list>	Is a list of physical ports. Only one port per line card can be specified. For example, when a CMTS card is located in slot 7, specify the CMTS port-list as cm. 7. 1 .
	all-ports	Specify all-ports to view all ports.
upstream	<range>	Specify an upstream channel or range of upstream channels.
	all	Specify all to display information for all upstream channels.

Restrictions

None.

Example

To display the upstream channel parameter values enter:

```
cmts show uschannel all-ports upstream all
```

The following displays:

```
Upstream Channel Parameters
Port: cm.5.1   CATV Upstream Channel: 1
US Channel ID      : 81
US Channel Frequency : 10000000 Hz
US Channel Bandwidth : 1600000 Hz
US Channel Power    : 5 dBmV
Modulation Profile  : 5
US Channel Slot Size : 4
Tx Timing Offset    : 12050.00 MicroSeconds
Initial Ranging Backoff : 3
Final Ranging Backoff : 6
Initial Tx Backoff   : 3
Final Tx Backoff     : 10
Max Power Adjustment : 8
Upstream State       : On
Upstream Policing    : Off
Policing Alarm       : Off
Upstream QOS Confirm : Off
Max QOS Rate         : 25000000 bps
US Channel ID        : 82
Upstream State       : On
Port: cm.5.1   CATV Upstream Channel: 3
US Channel ID      : 83
Upstream State     : On
Port: cm.5.1   CATV Upstream Channel: 4
US Channel ID      : 84
Upstream State     : Off
Port: cm.6.1   CATV Upstream Channel: 1
US Channel ID      : 97
Upstream State     : On
Port: cm.6.1   CATV Upstream Channel: 2
US Channel ID      : 98
Upstream State     : On
Port: cm.6.1   CATV Upstream Channel: 3
US Channel ID      : 99
US Channel Frequency : 16400000 Hz
US Channel Bandwidth : 1600000 Hz
US Channel Power    : 5 dBmV
Modulation Profile  : 5
US Channel Slot Size : 4
Tx Timing Offset    : 6168.36 MicroSeconds
Final Ranging Backoff : 6
Initial Tx Backoff   : 3
Final Tx Backoff     : 10
Max Power Adjustment : 8
Upstream State       : On
Upstream Policing    : Off
Policing Alarm       : Off
Upstream QOS Confirm : Off
Max QOS Rate         : 25000000 bps
Port: cm.6.1   CATV Upstream Channel: 4
US Channel ID      : 100
Upstream State     : Off
```

cmts-diag set 3033

Mode

Enable

Format

cmts-diag set 3033 *<port-list>* reg_offset *<num>* | value *<num>*

Description

Use this command to set the Broadcom 3033 register.

Parameter	Value	Meaning
set 3033	<i><port-list></i>	The variable <i>port-list</i> is a list of physical ports. One port per CMTS line card can be specified in the list. For example, when a CMTS line card is located in slot 7, specify it as cm. 7. 1 . For multiple ports, you can use commas, ranges, or * in your specification. There is no maximum number of ports for the list. It is only limited by the number of CMTS ports on the router.
reg_offset	<i><num></i>	Enter the value to be set.
value	<i><num></i>	Enter the value to be set.

Restrictions

None.

11 COMMENT COMMANDS

Use the **comment** command to add user defined comment lines in the active configuration file. This command is useful for documenting configuration files.

11.1 COMMAND SUMMARY

The following table lists the **comment** commands. The sections following the table describe the command syntax.

<code>comment out <num></code>
<code>comment in <num></code>
<code>comment line <num> <string></code>
<code>comment move <num></code>

comment out

Mode

Configure

Format

comment out *<num>*

Description

Use the **comment out** command to negate an individual command or set of commands in a configuration file. Do this by specifying the line number of the command in *num*. When executed, the command will be left in the configuration file as a comment. Commenting out a command is also known as *negating* a command.

Parameter	Value	Meaning
out	<i><num></i>	Specifies the line number of the command to negate in the active configuration file. Specify in <i>num</i> a number starting from 1 up to the number of the last line in the file.

Restrictions

None.

Example

To negate (comment out) command number 10 in a configuration file:

```
rs(config)# comment out 10
```

comment in

Mode

Configure

Format

`comment in <num>`

Description

Use the **comment in** command to reactivate a command that was previously negated. Do this by specifying the line number of the negated command in *num*.

Parameter	Value	Meaning
in	<num>	Specifies the line number of the command to activate in the active configuration file. Specify in <i>num</i> a number starting from 1 up to the number of the last line in the file.

Restrictions

Only activate negated commands.

Example

To reactivate line 10 in the configuration file:

```
rs(config)# comment in 10
```

comment line

Mode

Configure

Format

```
comment line <num> <string>
```

Description

The **comment line** command adds comment lines to a configuration file. The comment line is added directly above the command that is currently occupying the line number. Comment lines are denoted with a C following the line number, and a !! before the comment. The comment line will appear as soon as the command is executed.

Parameter	Value	Meaning
line	<num>	Specifies the line number of the line to comment. Specify in <i>num</i> a number starting from 1 up to the number of the last line in the file.
	<string>	Specifies the comment (character string). Enclose the character string in quotation marks.

Restrictions

None.

Example

To specify a comment line **"test port"** for line 8-10:

```
rs(config)# comment line 8-10 "test port"
8C: !!test port
9 : interface create ip gig2 address-netmask 20.1.1.2/24 port gi.5.2
!
10C: !!test port
11 : interface create ip gig3 address-netmask 30.1.1.3/24 port gi.5.3
!
12C: !!test port
13 : interface create ip gig4 address-netmask 40.1.1.4/24 port gi.5.4
```

**Note**

The comment !!test port becomes line 8 while what used to be line 8 is now line 9. The same applies to line 9 and line 10.

comment move

Mode

Configure

Format

```
comment move <num>, <num2>
```

Description

Use the **comment move** command to move a comment line or range of comment lines from one line number to another line number within a configuration file.

Parameter	Value	Meaning
line	<num>	Specifies the line number of the line to move. Specify in <i>num</i> a number or numbers starting from 1 up to the number of the last line in the file. It can be one number or it can be a range of numbers using the format X-X.
	<num2>	Specifies the new line number. Specify in <i>num</i> a number starting from 1 up to the number of the last line in the file. It can be one number or it can be a range of numbers using the format X-X.

Restrictions

When moving a range of comment lines, the ranges of the source and destination line numbers must be the same size. For example, if three comment lines are to be moved, then a destination range of three line numbers must be specified.

Example

To move the comments in lines 1-2 to lines 7-8:

```
rs(config)# comment move 1-2,7-8
```


12 CONFIGURE COMMAND

configure

Mode

Enable

Format

configure

Description

The **configure** command places the CLI session in the configure mode. Use the configure mode to set and change RS parameters. To enter the configure mode type **config** at the enable prompt. To exit the configure mode, use the **exit** command.

Restrictions

The configure mode can only be entered from the enable mode.

13 COPY COMMAND

copy

Mode

Enable

Format

copy active | scratchpad | tftp-server | rcp-server | startup | *<filename>* | *<url>* to backup-CM | active | scratchpad | tftp-server | rcp-server | startup | ethers | *<filename>* | *<url>*

Description

The **copy** command is primarily for copying configuration files. Configuration files can be copied between the RS and external hosts using protocols such as TFTP or RCP. Within the RS, configuration files are copied between the RS file system, the scratchpad (configuration database), the active (running) configuration, or the startup configuration. Additionally, the **copy** command is used to make backup copies of a configuration file and copy startup configuration files from the primary Control Module to the secondary Control Module.

Parameter	Value	Meaning
copy		Copies configuration file.
	active	Specifies the running configuration file.
	scratchpad	Specifies the configuration file in the scratchpad.
	tftp-server	Specifies the TFTP server.
	rcp-server	Specifies the RCP server.
	startup	Specifies the startup configuration file.
	<i><filename></i>	Specifies the name of a file.
	<i><url></i>	Specifies a URL: • tftp://<host>/<filename> • rcp://<user>@<host>/<filename>
to		Specifies the destination.

Parameter	Value	Meaning
	backup-cm	Specifies that the startup configuration be copied to the backup Control Module. Specify the backup-cm parameter only as the destination and only with startup as the source. When startup is the destination, information is copied to the backup Control Module as well.
	ethers	Copies a list of MAC to IP address mappings that is user created with a text editor to the RS. The mappings are used by the RARP server on the RS. See the <i>Riverstone Networks RS Switch Router User Guide</i> for more information about defining MAC-to-IP address mappings for use with RARP.

Restrictions

The RS does not allow some combinations of source and destination pairs. Files can not be copied from one TFTP server directly to another TFTP server or copied from scratchpad to scratchpad. In addition, files can not be copied directly into the active configuration from anywhere except the scratchpad. All changes to the running system must come through the scratchpad. Additionally, a PC card slot can not be specified with the **copy** command. If files need to be copied between PC cards on the primary Control Module, or between the bootflash and a PC card on the primary Control Module, use the CLI **file copy** command.

Examples

To copy configuration information from the scratchpad to the active database, enter the following command:

```
rs# copy scratchpad to active
```

To copy the file config.one to config.two:

```
rs# copy config.one to config.two
```

To copy the startup configuration file to a TFTP server for backup purposes, enter the following command.

```
rs# copy startup to tftp-server
```

To copy a previously saved configuration from a TFTP server to the startup configuration file, enter the following command:

```
rs# copy tftp://10.1.2.3/backup/config.org to startup
```

To copy the active configuration to a remote server using RCP, enter the following command.

```
rs# copy active to rcp://john@server1/config/config.dec25
```

To copy the startup configuration of the primary Control Module to the secondary Control Module:

```
rs# copy startup to backup-CM
```


14 DHCP COMMANDS

The **dhcp** commands allow you to configure *scopes* (sets of IP address pools and network parameters) that are to be used by Dynamic Host Configuration Protocol (DHCP) clients and apply them to interfaces on the RS.

14.1 COMMAND SUMMARY

The following table lists the **dhcp** commands. The sections following the table describe the command syntax for each command.

dhcp <scope> attach superscope <superscope>
dhcp <scope> define parameters <parameter> <value>
dhcp <scope> define pool <ip-range>
dhcp <scope> define static-ip <ipaddr> mac-address <macaddr> [<parameter> <value>]
dhcp flush
dhcp global set commit-interval <hours>
dhcp global set lease-database <url>
dhcp show binding [active expired static]
dhcp show num-clients

dhcp attach superscope

Mode

Configure

Format

```
dhcp <scope> attach superscope <superscope>
```

Description

The **dhcp attach superscope** command allows you to create a “superscope,” a group of scopes that share a common physical interface. For example, you can define and group together scopes for different subnets that are accessed through a single port or VLAN.

Parameter	Value	Meaning
dhcp	<scope>	The name of a scope that was previously configured with the dhcp define commands.
superscope	<superscope>	The name of the group to which the specified scope is being attached.

Restrictions

None.

Examples

Consider the following example where the scopes ‘client1’ and ‘client2’ exist on the same interface. To group scopes ‘client1’ and ‘client2’ into the superscope ‘allclients’:

```
rs(config)# dhcp client1 attach superscope allclients
rs(config)# dhcp client2 attach superscope allclients
```

dhcp define parameters

Mode

Configure

Format

```
dhcp <scope> define parameters <parameter> <value> ...
```

Description

The **dhcp define parameters** command allows you to define a set of parameters that are to be used by clients when DHCP is enabled. The client uses these parameters to configure its network environment, for example, the default gateway and DNS domain name. The DHCP server on the RS supports parameters used by Windows 95/98/NT and MacOS clients.

Parameter	Value	Meaning
dhcp	<scope>	The name that refers to this set of client parameters.
parameters	<parameter> <value>	You can specify one or more of the following client parameters and values:
address-mask	<address> <netmask>	(Required) Specifies the address and netmask of the scope's subnet.
 Note The address-mask parameter is <i>required</i> and must be defined <i>before</i> any other client parameters are specified.		
broadcast	<broadcastaddr>	Specify the broadcast address.
bootfile	<filename>	Specify the client's boot filename.
dns-domain	<domain>	Specify the DNS domain name.
dns-server	<dnsipaddr>	Specify the IP address of the DNS server.
gateway	<gwipaddr>	Specify the IP address of the default gateway.
lease-time	<hours>[:<minutes>]	Specify how long the lease is valid. (A lease is the amount of time that an assigned IP address is valid for a client system.) Specify the number of hours and, optionally, the number of minutes in the format <hours>[:<minutes>].
netbios-name-server	<nbipaddr>	Specify the IP address of the NetBIOS name server or WINS server.
netbios-node-type	<nodetype>	Specify the NetBIOS node type of the client.
netbios-scope	<netbiosscope>	Specify the NetBIOS scope of the client.

Restrictions

None.

Examples

The following command configures a group of network parameters for the scope 'finance':

```
rs(config)# dhcp finance define parameters address-netmask 10.33.0.0/16 dns-server  
10.3.2.1 dns-domain acme.com gateway 10.33.1.1 netbios-node-type b-node lease-time 90  
netbios-name-server 10.33.44.55 netbios-scope acme-finance
```

dhcp define pool

Mode

Configure

Format

```
dhcp <scope> define pool <ip-range>
```

Description

The **dhcp define pool** command allows you to define a pool of IP addresses that can be used by DHCP clients. An IP address pool, along with a set of parameters defined with the **dhcp define parameters** command, make up a DHCP “scope”.

Parameter	Value	Meaning
dhcp	<scope>	A name that refers to the specified pool of addresses.
pool	<ip-range>	The range of IP addresses to be used by the clients. Use a hyphen (-) to designate the range. If you have more than one pool of IP addresses to specify or if the addresses are not contiguous, specify additional addresses using multiple dhcp define pool commands.

Restrictions

None.

Examples

To specify the addresses between 10.1.1.1 to 10.1.1.20 as the pool of IP addresses for the scope ‘clients’:

```
rs(config)# dhcp clients define pool 10.1.1.1-10.1.1.20
```

To specify two separate pools of IP addresses for the scope ‘clients’:

```
rs(config)# dhcp clients define pool 10.1.1.1-10.1.1.20
rs(config)# dhcp clients define pool 10.1.1.30-10.1.1.40
```

dhcp define static-ip

Mode

Configure

Format

```
dhcp <scope> define static-ip <ipaddr> mac-address <macaddr> [<parameter> <value> ...]
```

Description

The **dhcp define static-ip** command allows you to configure a static IP address for a specific MAC address. For example, you can define a static IP address for a printer's MAC address to ensure that the printer always receives the same IP address from the DHCP server. Static IP addresses can be used for BOOTP clients as well as DHCP clients.

If you want a single MAC address to have different static IP addresses, depending upon which subnet or interface the machine is on, you can configure different scopes with different IP addresses that map to the same MAC address.

A client configured for a static IP address inherits the client parameters that are configured for the scope. If you want to configure a specific group of parameters for a static IP address, specify those parameters with the **dhcp define static-ip** command.

Parameter	Value	Meaning
dhcp	<scope>	A name that refers to the specified static IP address.
static-ip	<ipaddr>	The static IP address.
mac-address	<macaddr>	The MAC address to which the specified static IP address is to be mapped.
	<parameter> <value>	Specifies the client parameters and values for this static IP address. You can specify one or more of the following client parameters and values:
broadcast	<broadcastaddress>	Specify the broadcast address.
bootfile	<filename>	Specify the client's boot filename.
dns-domain	<domain>	Specify the DNS domain name.
dns-server	<dnsipaddr>	Specify the IP address of the DNS server.
gateway	<gwipaddr>	Specify the IP address of the default gateway.
lease-time	<hours>[:<minutes>]	Specify how long the lease is valid. (A lease is the amount of time that an assigned IP address is valid for a client system.) Specify the number of hours and, optionally, the number of minutes in the format <hours>[:<minutes>].
netbios-name-server	<nbipaddr>	Specify the IP address of the NetBIOS name server or WINS server.

Parameter	Value	Meaning
netbios-node-type	<i><nodetype></i>	Specify the NetBIOS node type of the client.
netbios-scope	<i><netbiosscope></i>	Specify the NetBIOS scope of the client.

Restrictions

None.

Examples

To specify a static IP address 10.1.44.55 to the MAC address 08:00:20:12:34:56 for the scope 'servers':

```
rs(config)# dhcp servers define static-ip 10.1.44.55 mac-address 08:00:20:12:34:56
```

To specify a static IP address 10.1.44.55 to the MAC address 08:00:20:12:34:56 for the scope 'servers' and give it a specific default gateway address:

```
rs(config)# dhcp servers define static-ip 10.1.44.55 mac-address 08:00:20:12:34:56  
gateway 10.1.1.2
```

To define two different scopes ('public' and 'private') with two different static IP addresses (10.1.44.55 and 10.2.10.23) that map to the MAC address 08:00:20:12:34:56:

```
rs(config)# dhcp public define static-ip 10.1.44.55 mac-address 08:00:20:12:34:56  
rs(config)# dhcp private define static-ip 10.2.10.23 mac-address 08:00:20:12:34:56
```

dhcp flush

Mode

Enable

Format

dhcp flush

Description

The DHCP server normally updates its lease database at the intervals specified with the **dhcp global set commit-interval** command. While the DHCP server is running, you can force the server to immediately update its lease database by using the **dhcp flush** command.

Restrictions

None.

dhcp global set commit-interval

Mode

Configure

Format

dhcp global set commit-interval <minutes>

Description

After each client transaction, the DHCP server does not immediately update the information in the lease database. Lease update information is stored in flash memory and flushed to the database at certain intervals. You can use the **dhcp global set commit-interval** command to specify this interval.



Note Writing to flash memory can be time-consuming if there are many clients on the network.

Parameter	Value	Meaning
commit-interval	<hours>	The interval, in hours, that the DHCP server updates the lease database. The default value is 1 hour. You can specify a value between 1-48.

Restrictions

None.

Examples

To configure the DHCP server to update the lease database once every 2 hours:

```
rs(config)# dhcp global set commit-interval 2
```

dhcp global set lease-database

Mode

Configure

Format

```
dhcp global set lease-database <url>
```

Description

By default, the RS stores the clients' lease information (the lease database) in its flash memory. You can use the `dhcp global set lease-database` command to specify a TFTP or RCP server where the lease database is to be periodically backed up.

Parameter	Value	Meaning
lease-database	<url>	The TFTP or RCP server where the lease-database is to be backed up.

Restrictions

None.

Examples

To configure the lease database to be on a TFTP server (10.50.89.88) with the file name 'lease-db':

```
rs(config)# dhcp global set lease-database tftp://10.50.89.88/lease-db
```

To configure the lease database to be on an RCP server (10.50.89.89) with the user name 'john' and the file name 'lease-db':

```
rs(config)# dhcp global set lease-database rcp://john@10.50.89.89/lease-db
```

dhcp show binding

Mode

Enable

Format

```
dhcp show binding [active|expired|static]
```

Description

The **dhcp show** command displays information from the lease database. If you do not specify any parameters, the DHCP server displays the entire lease database.

Parameter	Value	Meaning
active		Displays currently active leases only.
expired		Displays expired leases only.
static		Displays leases with static IP address assignments only.

Restrictions

None.

Examples

To display information from the lease database:

```
rs# dhcp show binding
IP address Hardware Address Lease Expiration Type
-----
10.20.1.22 00:40:05:41:f1:2d 1999-05-24 17:45:06 dynamic
10.20.1.23 00:00:b4:b1:29:9c 1999-05-24 17:45:04 dynamic
10.20.1.21 00:00:b4:b0:f4:83 1999-05-24 17:45:01 dynamic
10.20.1.20 00:80:c8:e1:20:8a 1999-05-24 09:24:30 dynamic
10.30.7.9 08:00:20:11:22:33 --- static
10.30.7.44 08:00:20:44:55:66 --- static
```

dhcp show num-clients

Mode

Enable

Format

dhcp show num-clients

Description

This **dhcp show** command displays the number of allocated bindings for the DHCP server and the maximum number allowed.

Restrictions

None.

Examples

To display information:

```
rs# dhcp show num-clients
15 current clients (253 maximum)
```

15 DIFF COMMAND

diff

Mode

Configure

Format

diff configuration <filename>|startup

Description

The **diff configuration** command compares the active configuration with the specified configuration file.

Parameter	Value	Meaning
configuration	<filename>	Name of a configuration file.
	startup	The Startup configuration file.

Restrictions

None.

Example

To compare the active configuration with the Startup configuration file:

```
rs# diff startup
```


16 DVMRP COMMANDS

The **dvmrp** commands let you configure and display information about Distance Vector Multicast Routing Protocol (DVMRP) interfaces.

16.1 COMMAND SUMMARY

The following table lists the **dvmrp** commands. The sections following the table describe the command syntax for each command.

dvmrp accept noaccept route <IPaddr/mask> [exact] [interface <IPaddr> [router <IPaddr>]]
dvmrp advertise noadvertise route <IPaddr/mask> [exact] [interface <IPaddr>]
dvmrp create tunnel <name> local <IPaddr> remote <IPaddr>
dvmrp enable no-pruning
dvmrp enable interface <IPaddr> <interface-name> <tunnel-name>
dvmrp set interface <IPaddr> <hostname> [metric <num>] [neighbor-timeout <seconds>] [prunetime <seconds>] [rate <num>] [scope <IPaddr/mask>] [threshold <num>]
dvmrp show interface [<IPaddr>]
dvmrp show routes [host <IPaddr> interface <IPaddr> net <netaddr> router <IPaddr> subordinates permission]
dvmrp show rules
dvmrp start

dvmrp accept route

Mode

Configure

Format

```
dvmrp accept|noaccept route <IPaddr/mask> [exact] [interface <IPaddr> [router <IPaddr>]]
```

Description

The **dvmrp accept route** command allows you to specify particular routes that can be learned from DVMRP neighbors.

A route is always accepted from a DVMRP neighbor unless you use the **dvmrp noaccept route** to prevent it from being accepted. You can use the **dvmrp accept route** command along with the **dvmrp noaccept route** command to filter the routes accepted from DVMRP neighbor routers.

Parameter	Value	Meaning
accept		Allows the specified route to be accepted from DVMRP neighbor routers.
noaccept		Prevents the specified route from being accepted from DVMRP neighbor routers.
route	<IPaddr/mask>	Is the IP address and mask of the route prefix to be accepted.
exact		Causes only routes exactly matching the prefix to be accepted.
interface	<ipAddr>	Is the IP address of the interface to which you are applying this filter.
router	<IPaddr>	Is the IP address of a DVMRP neighbor router.

Restrictions

None.

Examples

To cause the RS to accept only prefix 20.30.40.0/24, and filter out all other routes:

```
rs(config)# dvmrp noaccept route 0/0 interface customer1
rs(config)# dvmrp accept route 20.30.40.0/24 interface customer1
```

If interface customer1 breaks subnet 20.30.40.0/24 into smaller subnets, you can filter out routes from these subnets with the following commands:

```
rs(config)# dvmrp noaccept route 0/0 interface customer1
rs(config)# dvmrp accept route 20.30.40.0/24 interface customer1 exact
```


dvmrp advertise route

Mode

Configure

Format

```
dvmrp advertise|noadvertise route <IPaddr/mask> [exact] [interface <IPaddr>]
```

Description

The **dvmrp advertise route** command allows you to specify particular routes that can be advertised to DVMRP neighbors. A route is always advertised to a DVMRP neighbor unless you use the **dvmrp noadvertise route** command to prevent it from being advertised. You can use the **dvmrp advertise route** command along with **dvmrp noadvertise route** to filter the routes advertised to DVMRP neighbor routers.

Parameter	Value	Meaning
advertise		Allows the specified route to be advertised to DVMRP neighbor routers.
noadvertise		Prevents the specified route from being advertised to DVMRP neighbor routers.
route	<IPaddr/mask>	Is the IP address and mask of the route prefix to be advertised.
exact		Causes only routes exactly matching the prefix to be advertised.
interface	<ipAddr>	Is the IP address of the interface to which you are applying this filter.

Restrictions

None.

Examples

To prevent route 10.0.0.0/8 from being advertised on interface mbone (all other routes are advertised):

```
rs(config)# dvmrp noadvertise route 10/8 interface mbone
```

To advertise only route 20.20.20.0/24 to its neighbors on interface mbone:

```
rs(config)# dvmrp noadvertise route 0/0 interface mbone
rs(config)# dvmrp advertise route 20.20.20.0/24 interface mbone
```

dvmrp create tunnel

Mode

Configure

Format

```
dvmrp create tunnel <name> local <ipAddr> remote <ipAddr>
```

Description

The **dvmrp create tunnel** command creates a DVMRP tunnel for sending multicast traffic between two end points.

Parameter	Value	Meaning
tunnel	<name>	Name of this DVMRP tunnel.
local	<ipAddr>	IP address of the local end point of this tunnel.
 Note The local IP address must already be configured on the RS.		
remote	<ipAddr>	IP address of the remote end point of this tunnel.

Restrictions

- Tunnels use unicast routing principles. Make sure a route exists between the tunnel source and destination (local <ipAddr> and remote <ipAddr>) you specify.
- An IP interface has to exist before a tunnel can be created from it.
- A good way to confirm that a tunnel exists is to ping the other end of the tunnel.
- Tunnels cannot be created between two endpoints (that is, on the same subnet).
- A maximum of eight tunnels are allowed.

Example

To create a DVMRP tunnel called *tun12* between 10.3.4.15 (the local end of the tunnel) and 10.5.3.78 (the remote end of the tunnel):

```
rs(config)# dvmrp create tunnel tun12 local 10.3.4.15 remote 10.5.3.78
```

dvmrp enable no-pruning

Mode

Configure

Format

dvmrp enable no-pruning

Description

Disable DVMRP pruning.



Note

Pruning is enabled by default. The current DVMRP specification requires pruning capability. Unless you have a good reason for disabling pruning, Riverstone recommends that you leave it enabled.

Restrictions

None.

dvmrp enable interface

Mode
Configure

Format

dvmrp enable interface <ipAddr/name>|<tunnel-name>

Description

The **dvmrp enable interface** command enables DVMRP on the specified interface.

Parameter	Value	Meaning
interface	<ipAddr/name>	IP address of the interface on which you are enabling DVMRP. If you are enabling DVMRP on an interface that does not have a tunnel, specify its name or IP address.
	<tunnel-name>	Tunnel name of the interface on which you are enabling DVMRP. If you are enabling DVMRP on an interface that has a tunnel, specify the tunnel name.

Restrictions



Note The Control Module’s en0 interface is never used for multicast traffic.

DVMRP does not run on multiple IP subnets if created on an interface. Currently, the RS automatically picks up the first subnet to run DVMRP on it. However any one particular subnet can be picked up by enabling it. But before doing that, no subnet should already be enabled on that interface. The RS supports a maximum of 64 DVMRP and IGMP interfaces.



Note The **igmp enable interface** command has a similar restriction of using only one subnet.

Examples

To enable DVMRP on the IP interface with IP address 10.50.78.2:

```
rs(config)# dvmrp enable interface 10.50.78.2
```

To enable tunnel tun12:

```
rs(config)# dvmrp enable interface tun12
```

dvmrp set interface

Mode

Configure

Format

```
dvmrp set interface <IPAddr/name> [metric <num>] [neighbor-timeout <seconds>] [prunetime <seconds>] [rate <num>] [scope <IPAddr/mask>] [threshold <num>]
```

Description

The **dvmrp set interface** command sets DVMRP parameters on an IP interface.

Parameter	Value	Meaning
interface	<ipAddr/name>	IP address or name of the interface on which you are configuring DVMRP parameters.
metric	<num>	The metric (cost) of this interface. Specify a number in the range 1 – 16. The default is 1. Normally you should not change this setting unless the network topology requires it.
neighbor-timeout	<num>	The number of seconds after which the RS will consider the neighbor to be down. Specify a number in the range 40 – 400. The default is 35.
 Note If you have some old routers, this value should be increased to accommodate them because they don't send probes or route updates at 40-second intervals.		
prunetime	<seconds>	The multicast prunetime of this interface. Specify a number in the range 300 – 7200. The default is 3600 seconds (one hour).
rate	<num>	The multicast rate of this interface in kbps. Specify a number in the range 1 – 10000. The default is 500.
 Note The option applies only to tunnels.		

Parameter	Value	Meaning
scope	<IPaddr/mask>	The multicast scope of this interface. The purpose of this option is to disallow the groups specified by a scope from being forwarded across an interface. This option therefore is a filtering mechanism. The threshold and the scope are two common mechanisms for implementing local simple filtering of a multicasting data. Specify an IP address and network mask. Example: 239.0.0.0/8.
threshold	<num>	The multicast threshold of this interface. The purpose of this option is to allow forwarding of a packet on a multicast interface only if the packet's threshold is at least the configured value. The threshold and the scope are two common mechanisms for implementing local simple filtering of a multicasting data. Specify a number in the range 1 – 255. The default is 1.

Restrictions

None.

Examples

To configure the interface 10.50.89.90 to have a metric of 5 and a threshold of 16:

```
rs(config)# dvmp set interface 10.50.89.90 metric 5 threshold 16
```

dvmrp show interface

Mode
Enable

Format

dvmrp show interface [<IPaddr>]

Description

The **dvmrp show interface** command displays the state of an interface running DVMRP, along with other neighbor-related information. Neighbors are displayed with their DVMRP version and capability flags and Generation IDs; this information can help in debugging. If rules are in effect for an interface, they are indicated by **ExportPol** or the **ImportPol** flags.

Parameter	Value	Meaning
interface	<IPaddr>	Displays DVMRP information for the specified interface.

Restrictions

None.

Examples

Here is an example of the **dvmrp show interface** command.

```
rs# dvmrp show interface
Address: 10.50.1.1          Subnet: 10.50.1/24      Met: 1   Thr: 1
Name   : pc                State: Dn   Igmp  Dvmrp

Address: 207.135.89.10     Subnet: 207.135.89.0/27 Met: 1   Thr: 1
Name   : corp              State: Up   Igmp  Dvmrp Querier ExportPol
Peer   : 207.135.89.1      Version:   3.255        Flags:0xe  GID:
0x31a

Address: 10.55.89.101      Subnet: 10.55.89/24      Met: 1   Thr: 1
Name   : lab                State: Up   Dvmrp

Peer   : 10.55.89.100      Version:   3.255        Flags:0xe  GID:
0x179

Address: 207.135.89.10     Remote: 207.137.137.1    Met: 1   Thr: 1
Rate: 1000
Name   : mbone              State: Tunnel Up   Dvmrp ExportPol
Peer   : 207.137.137.1     Version:   3.8          Flags:0xe  GID:
0x6c19d135
```


Table 16-1 Display field descriptions for the dvmrp show interface command

FIELD	DESCRIPTION
Address	IP address of the interface
Subnet	Subnet of the interface
Met	DVMRP cost of the interface
Thr	Time-To-Live (TTL) Threshold of the interface. Any incoming packets with a TTL that is less than or equal to the threshold may be consumed locally but will not be forwarded.
Name	Name of the interface
State	Up—Indicates that this interface is up Dn—Indicates that this interface is down Querier—Indicates that this interface is an IGMP querier Leaf—Indicates that this interface is a leaf node in the multicast distribution tree Igmp—Indicates that IGMP is enabled on this interface Dvmrp—Indicates that DVMRP is enabled on this interface ExportPol—Indicates that advertise rules are in effect ImportPol—Indicates that accept rules are in effect
Peer	IP address of DVMRP peer(s)
Flags	Flags in the DVMRP probe message that the listed peer sent
Version	Version of DVMRP that the listed peer is running
GID	Peer's Generation ID—changes every time the router reboots or DVMRP restarts

dvmrp show routes

Mode

Enable

Format

```
dvmrp show routes [host <IPaddr>|interface <IPaddr>|net <netaddr>|router <IPaddr>|subordinates|permission]
```

Description

The **dvmrp show routes** command displays the contents of the DVMRP unicast routing table.

DVMRP routes show the topology information for internet multicasting sites. It is independent of IP unicast routing table or protocol. In this table, the information is presented about an address prefix (in the form of network-address/network-mask length), the interface and the uplink (parent) router through which this subnet can be reached. This table also shows information about any routers/interfaces which consider this router as their uplink (that is, those routers which depend on this router if traffic were to originate from this subnet). These routers/interfaces are shown as children of the parent router.



Note

This command only shows DVMRP routes and does not display information about current multicast sessions. For information about current multicast sessions, use the **multicast show mroutes** command.

Parameter	Value	Meaning
host	<IPaddr>	Displays the route to the specified uplink host address
interface	<IPaddr>	Displays the interface address of the specified uplink interface
net	<netaddr>	Displays the route to the specified prefix (or subnets falling within the prefix)
router	<IPaddr>	Displays the route to the specified router
subordinates		Displays a list of downstream routers
permissions		Displays those routes affected by rules. Routes marked NoAdv are not advertised.



Note The **dvmp show routes** command output is a superset of the outputs generated using any of its optional arguments. Using the additional arguments of this command filters out entries from the **dvmp show routes** output by matching on specific fields

Use this argument:	To match on this field in the dvmp show route output:
host	Any route in the routing table where the specified host matches the uplink host address
interface	Any route in the routing table where the specified interface address matches the parent
network	Any route in the routing table where the specified network matches the subnet
permission	Any route in the routing table that is affected by rules
router	Any route in the routing table where the specified IP address matches the gateway
subordinates	Any route in the routing table that has children

Restrictions

None.

Examples

The following is a sample command output with field explanations:

```
fk-r4# dvmp show routes
DVMRP Routing Table (4 routes)
Net: 10.10.1/24      Gateway: ----      Met: 1   Age:--
Parent: icast_svr    Children: 2_fk-r5

Net: 130.1/16        Gateway: 120.1.1.2  Met: 2   Age:10
Parent: 2_fk-r5      Children: icast_svr leaf

Net: 120.1/16        Gateway: ----      Met: 1   Age:--
Parent: 2_fk-r5      Children: icast_svr leaf

Net: 12/8            Gateway: 120.1.1.2  Met: 3   Age:10
Parent: 2_fk-r5      Children: icast_svr leaf

Total Routes Printed: 4
```

Table 16-2 Display field descriptions for the dvmrp show routes command

FIELD	DESCRIPTION
Net	The route is to this subnet
Gateway	Displays the gateway for this route if its is indirectly connected. Displays nothing if this subnet is directly connected.
Met	DVMRP cost to the attaching interface
Age	Age of this route in seconds. None for directly-connected subnets. If this route is indirectly connected through a gateway, displays the amount of time since the gateway last refreshed this route.
Parent	The interface through which this subnet can be reached. For directly-connected subnets, lists a local interface. For indirect routes, lists the interface to the gateway.
Children	Interface(s) which consider this router their uplink (that is, those routers which depend on this router if traffic were to originate from this subnet).
leaf	Indicates that there is no downstream neighbor on this interface

The following output displays the result of queries for DVMRP routes offered by the next-hop router 207.137.137.1. Note that all the entries in the output have 207.137.137.1 as the gateway.

:

```

rs# dvmrp show routes router 207.137.137.1
DVMRP Routing Table (4232 routes, 8 hold-down-routes)
Net: 128.119.3.16/29      Gateway: 207.137.137.1    Met: 9   Age: 35
Parent: mbone             Children: corp
                           lab
Net: 128.119.3.8/29       Gateway: 207.137.137.1    Met: 9   Age: 35
Parent: mbone             Children: corp
                           lab
Net: 209.12.162.16/28     Gateway: 207.137.137.1    Met: 26  Age: 35
Parent: mbone             Children: corp
                           lab
Net: 208.197.171.112/28   Gateway: 207.137.137.1    Met: 7   Age:
35                         Children: corp
Parent: mbone             lab
Net: 208.151.215.240/28   Gateway: 207.137.137.1    Met: 7   Age:
35                         Children: corp
Parent: mbone             lab
Net: 208.151.215.192/28   Gateway: 207.137.137.1    Met: 7   Age:
35                         Children: corp
Parent: mbone             lab
Net: 208.151.215.96/28    Gateway: 207.137.137.1    Met: 7   Age: 35
Parent: mbone             Children: corp

```

To show non-advertised routes on interface lab:

```

rs# dvmrp show routes interface lab permission
DVMRP Routing Table (4232 routes, 5 hold-down-routes)
Net: 100.100.100/24      Gateway: 10.55.89.100    Met: 2   Age: 25
Parent: lab              Children: corp
                           mbone          leaf NoAdv
Net: 20.20.20/24         Gateway: 10.55.89.100    Met: 2   Age: 25
Parent: lab              Children: corp
                           mbone          leaf NoAdv
Net: 10.55.89/24         Gateway: ----            Met: 1   Age: --
Parent: lab              Children: corp
                           mbone          leaf NoAdv
                           leaf NoAdv
Total Routes Printed: 3

```

dvmrp show rules

Mode

Enable

Format

dvmrp show rules

Description

The **dvmrp show rules** command displays the filtering rules in effect for DVMRP routes. Once you have set rules with the **dvmrp accept** and **dvmrp advertise** commands, you can display the active rules by entering the **dvmrp show rules** command.

Restrictions

None.

Example

In this example, the following rules are in effect:

```
dvmrp advertise route 207.135.89.0/24 interface mbone
dvmrp noadvertise route 0/0 interface mbone
dvmrp advertise route 207.135.88.0/24 interface mbone
dvmrp noadvertise route 10/8 interface corp
```

To display information about these rules:

```
# dvmrp show rules
NoAdvertise: 10.0.0.0/8          IF: corp
Advertise   : 207.135.89.0/24    IF: mbone
Advertise   : 207.135.88.0/24    IF: mbone
NoAdvertise: default            IF: mbone
```

These rules would affect the routing table as follows:

```
# dvmrp show route net 10/8 permissions

Net: 10.55.89/24      Gateway: ----      Met: 1   Age:  --
Parent: lab           Children: corp      leaf NoAdv
                        mbone      leaf NoAdv
```

These rules prevent a directly connected route on this router from being visible to interface corp and mbone. The **leaf** flag indicates there is no downstream neighbor on the interface.

dvmrp start

Mode

Configure

Format

dvmrp start

Description

The **dvmrp start** command starts DVMRP multicast routing on the configured multicast-enabled interfaces and tunnels.



Note

Because DVMRP is the only multicasting protocol on the RS, IGMP starts and stops along with DVMRP. If you want to start IGMP on local interfaces, you still must use this command.

DVMRP is by default not running. DVMRP does not interact with any unicast protocol. However if you need to run a tunnel, make sure that the tunnel is reachable by a unicast routing mechanism.

Restrictions

None.

17 ENABLE COMMAND

enable

Mode

User

Format

enable

Description

The **enable** command switches your CLI session from User mode to Enable mode. After you issue the command, the CLI will prompt you for a password if a password is configured. If no password is configured, a warning message advising you to configure a password is displayed.

If a password is configured and you do not know your password or pressing Return does not work, see the administrator for the RS.

To exit from the Enable mode and return to the User mode, use the **exit** command. To proceed from the Enable mode into the Configure mode, use the **configure** command.

Restrictions

None.

enable

enable Command

18 ERASE COMMAND

erase

Mode

Configure

Format

erase scratchpad|startup

Description

The **erase scratchpad** command erases the contents of the RS's command scratchpad. The **erase startup** command erases the Startup configuration from the Control Module's NVRAM.

Parameter	Value	Meaning
scratchpad		Erases the contents of the scratchpad. The scratchpad contains configuration commands that you have issued but have not yet activated.
startup		Erases the contents of the Startup configuration. The Startup configuration is the configuration the RS uses to configure itself when you reboot it. When you erase the Startup configuration, then reboot immediately, the RS restarts without any configuration information.

Restrictions

The **erase** commands do not delete other types of files. To delete a file, use the **file del** command.

19 EXIT COMMAND

exit

Mode

All modes

Format

exit

Description

The **exit** command exits the current CLI mode to the previous mode. For example, if you are in the Enable mode, **exit** returns you to the User mode. If you are in Configure mode, **exit** returns you to Enable mode. If you are in User mode, **exit** closes your CLI session and logs you off the RS.

Restrictions

None.

20 FILE COMMANDS

The **file** commands enable you to list and manipulate configuration files in bootflash or on a PC card in the primary Control Module. You cannot use these commands on the backup Control Module.

20.1 COMMAND SUMMARY

The following table lists the **file** commands. The sections following the table describe the command syntax for each command.

file copy [<i><device1>:</i>] <i><source-filename></i> [<i><device2>:</i>] <i><dest-filename></i>
file delete [<i><device>:</i>] <i><file-name></i>
file dir <i><device-name></i>
file reformat <i><device-name></i>
file rename [<i><device>:</i>] <i><source-filename></i> <i><dest-filename></i>
file type [<i><device>:</i>] <i><file-name></i>

file copy

Mode

Enable

Format

file copy [<device1>:]<source-filename> [<device2>:]<dest-filename>

Description

The **file copy** command copies a configuration file between devices on the primary Control Module.

Parameter	Value	Meaning
copy	<device1> <device2>	Name of the device where the file to be copied resides or where the file is to be copied. This can be slot0 , slot1 , or bootflash . If a device name is not specified, it is assumed to be the bootflash device. (The bootflash device is the default device for storing configuration files.)
	<source-filename>	Name of the file to be copied. This can be any filename listed with the file dir command.
	<dest-filename>	New name for the file.

Restrictions

The source and destination devices must be on the primary Control Module. If you need to copy configuration files between the primary and backup Control Modules, or between the RS file system and an external host, use the CLI **copy** command instead.

Examples

To copy the startup configuration file from **slot0** to **slot1** in the primary Control Module:

```
rs# file copy slot0:startup slot1
```

To copy the startup.bak configuration file from **slot0** to the startup file in **bootflash** in the primary Control Module:

```
rs# file copy slot0:startup.bak startup
```


file delete

Mode

Enable

Format

```
file delete [<device>:]<filename>
```

Description

The **file delete** command deletes the specified configuration file in the primary Control Module. A device name can optionally be specified. By default, if a device name is not specified, it is assumed to be the **bootflash:** device which is where all configuration files are stored.

Parameter	Value	Meaning
delete	<device>	Name of the device where the file to be deleted resides. This can be slot0 , slot1 , or bootflash . If a device name is not specified, it is assumed to be the bootflash device. (The bootflash device is the default device for storing configuration files.)
	<filename>	Name of the file to delete. This can be any filename listed with the file dir command.

Restrictions

The file to be deleted must reside on a device in the primary Control Module.

Examples

To delete the configuration file **config.old** file in the **bootflash** in the primary Control Module:

```
rs# file delete config.old
```

To delete the configuration file **config.old** in the PC card in **slot0** in the primary Control Module:

```
rs# file delete slot0:config.old
```

file dir

Mode

User or Enable

Format

file dir <device-name>

Description

The **file dir** command displays a directory of the files on the specified storage device in the primary Control Module.

Parameter	Value	Meaning
dir	<device-name>	Device name. You can specify one of the following:
	bootflash:	The Control Module's NVRAM.
	slot0:	The PC card in slot 0.
	slot1:	The PC card in slot 1.

Restrictions

The files to be displayed must be in the primary Control Module.

Examples

To display the contents of the **bootflash** device in the primary Control Module:

```
rs# file dir bootflash:
Version: 1 Blocks total: 756, used: 15
-rw-rw-rw-    0    0    7496    (1430)  2000-10-30 12:42:53  bootlog
-rw-rw-rw-    0    0     901     (339)  2000-07-28 09:56:45  startup
-rw-rw-rw-    0    0     958     (354)  2000-07-28 09:56:45  kg.bak
drwxrwxrwx    0    0        1           2000-10-17 08:46:38  ssh/
-rw-rw-rw-    0    0     958     (354)  2000-11-01 14:00:00  startup.bak
```

file reformat

Mode

User or Enable

Format

file reformat <device-name>

Description

The **file reformat** command reformats the file system on the specified storage device in the primary Control Module. All files are erased.

Parameter	Value	Meaning
reformat	<device-name>	Device name. You can specify one of the following:
	slot0:	The PC card in slot 0.
	slot1:	The PC card in slot 1.

Restrictions

The device to be reformatted must be in the primary Control Module.

Examples

To erase all files on the PC card in **slot1** in the primary Control Module:

```
rs# file reformat slot1:
```

file rename

Mode
Enable

Format

file rename [*<device>:*]*<source-filename>* *<dest-filename>*

Description

The **file rename** command renames a file. The source and destination filenames must reside on the same device in the primary Control Module. If you need to move a file from one device to another, use the **file copy** command.

Parameter	Value	Meaning
rename	<i><device>:</i>	Name of the device where the file to be renamed resides. This can be slot0 , slot1 , or bootflash . If a device name is not specified, it is assumed to be the bootflash device. (The bootflash device is the default device for storing configuration files.)
 Note You cannot specify different devices for the source and destination filenames.		
	<i><source-filename></i>	Name of the file to be renamed. This can be any filename listed with the file dir command.
	<i><dest-filename></i>	New name for the file.

Restrictions

The source and destination filenames must be on the same device and must be in the primary Control Module.

Examples

To rename the configuration file **config** to **config.old** on the **bootflash**:

```
rs# file rename config config.old
```

To rename the configuration file **startup.bak** to **startup** in **slot0**:

```
rs# file rename slot0:startup.bak startup
```

file type

Mode

Enable

Format

file type [*<device>:*]*<filename>*

Description

The **file type** command displays the contents of a file in the primary Control Module.

Parameter	Value	Meaning
type	<i><device></i>	Name of the device where the file to be displayed resides. This can be slot0 , slot1 , or bootflash . If a device name is not specified, it is assumed to be the bootflash device. (The bootflash device is the default device for storing configuration files.)
	<i><filename></i>	Name of the file to display. This can be any filename listed with the file dir command.

Restrictions

The file whose contents you want to see must be on in bootflash or on a PC card in the primary Control Module.

Examples

To display the contents of the file **startup** (the startup configuration file):

```
rs# file type startup
!
! Last modified from Telnet (134.141.173.222) on 2000-07-28 09:56:40
!
version 6.2

(rest of startup configuration is displayed)
```


21 FILTERS COMMANDS

The **filters** commands let you create and apply the following types of security filters:

- Address filters block traffic based on a frame's source MAC address, destination MAC address, or both. Address filters are always configured and applied on the input port.
- Static entry filters allow or force traffic to go to a set of destination ports based on a frame's source MAC address, destination MAC address, or both. Static entry filters are always configured and applied on the input port. You can configure source static entry filters, destination static entry filters, and flow static entry filters. Source static entry filters allow or disallow frames based on their source MAC address; destination static entry filters allow or disallow frames based on their destination MAC address. Flow static entries allow or disallow traffic based on their source *and* destination MAC addresses.
- Port-to-address lock filters “lock” a user to a port or set of ports, disallowing them access to other ports.
- Secure port filters shut down Layer 2 access to the RS from a specific port or drop all Layer 2 packets received by a port. Used by themselves, secure ports secure unused RS ports. When used in conjunction with static entry filters, secure ports drop all received or sent traffic (depending on the static entry filter) except traffic forced to or from the port by the static entry filter.

21.1 COMMAND SUMMARY

The following table lists the **filters** commands. The sections following the table describe the command syntax for each command.

<code>filters add address-filter name <name> source-mac <MACaddr> source-mac-mask <MACaddr> dest-mac <MACaddr> dest-mac-mask <MACaddr> vlan <VLAN-num> in-port-list <port-list></code>
<code>filters add port-address-lock name <name> source-mac <MACaddr> vlan <VLAN-num> in-port-list <port-list></code>
<code>filters add secure-port name <name> direction source destination vlan <VLAN-num> in-port-list <port-list></code>
<code>filters add static-entry name <name> restriction allow disallow force source-mac <MACaddr> source-mac-mask <MACaddr> dest-mac <MACaddr> dest-mac-mask <MACaddr> vlan <VLAN-num> in-port-list <port-list> out-port-list <port-list></code>
<code>filters show address-filter [all-source all-destination all-flow] [source-mac <MACaddr> dest-mac <MACaddr>] [ports <port-list>] [vlan <VLAN-num>]</code>

```
filters show port-address-lock ports [ports <port-list>] [vlan <VLAN-num>]  
[source-mac <MACaddr>]
```

```
filters show secure-port
```

```
filters show static-entry [all-source|all-destination|all-flow] ports <port-list>  
vlan <VLAN-num> [source-mac <MACaddr> dest-mac <MACaddr>]
```


filters add address-filter

Mode

Configure

Format

```
filters add address-filter name <name> source-mac <MACaddr> source-mac-mask <MACaddr>  
dest-mac <MACaddr> dest-mac-mask <MACaddr> vlan <VLAN-num> in-port-list <port-list>
```

Description

The **filters add address-filter** command blocks traffic based on a frame's source MAC address (**source-mac**), destination MAC address (**dest-mac**), or a flow (specified using both a source MAC address and a destination MAC address).

Parameter	Value	Meaning
name	<name>	Specifies the name of the filter. This parameter must be less than 25 characters.
source-mac	<MACaddr> any	Specifies the source MAC address. Specify any to allow any MAC address as the source-mac . Use this option for source or flow address filters.
source-mac-mask	<MACaddr>	Specifies the source MAC Mask address. Use this option for source or flow address filters.
dest-mac	<MACaddr> any	Specifies the destination MAC address. Specify any to allow any MAC address as the dest-mac . Use this option for destination or flow address filters.
dest-mac-mask	<MACaddr>	Specifies the destination MAC Mask address. Use this option for destination or flow static entries.
vlan	<VLAN-num> any	Specifies the VLAN. Specify any to allow any VLAN.
in-port-list	<port-list>	Specifies the ports to which you want to apply the filter.

Restrictions

You should apply flow filters (specified using both a source MAC address and a destination MAC address) only to ports that are using flow-based bridging.

filters add port-address-lock

Mode

Configure

Format

```
filters add port-address-lock name <name> source-mac <MACaddr> vlan <VLAN-num>  
in-port-list <port-list>
```

Description

The **filters add port-address-lock** command locks a user (identified by the user's MAC address) to a specific port or set of ports. The source MAC address will be allowed to reach only those stations and other ports that are connected to a port specified by **in-port-list**.

Parameter	Value	Meaning
name	<name>	Specifies the name of the lock filter. This parameter must be less than 25 characters.
source-mac	<MACaddr>	Specifies the source MAC address.
vlan	<VLAN-num>	Specifies the VLAN.
in-port-list	<port-list>	Specifies the ports to which you want to apply the lock.

Restrictions

None.

filters add secure-port

Mode

Configure

Format

```
filters add secure-port name <name> direction source|destination vlan <VLAN-num>  
in-port-list <port-list>
```

Description

The **filters add secure-port** command shuts down Layer 2 access to the RS from the ports specified by **in-port-list**. The RS drops all traffic received from these ports.



Note

You can use port-to-address lock filters to force traffic to a port secured by the **filters add secure-port** command.

Parameter	Value	Meaning
name	<name>	Specifies the name of the filter. This parameter must be less than 25 characters.
direction	source destination	Specifies whether the filter is to secure a source port or a destination port.
vlan	<VLAN-num>	Specifies the VLAN.
in-port-list	<port-list>	Specifies the ports to which you want to apply the filter.

Restrictions

None.

filters add static-entry

Mode

Configure

Format

```
filters add static-entry name <name> restriction allow|disallow|force source-mac  
<MACaddr> source-mac-mask <MACaddr> dest-mac <MACaddr> dest-mac-mask <MACaddr> vlan  
<VLAN-num> in-port-list <port-list> out-port-list <port-list>
```

Description

The **filters add static-entry** command allows, disallows, or forces traffic to go to a set of destination ports based on a frame's source MAC address (**source-mac**), destination MAC address (**dest-mac**), or a flow (specified using both a source MAC address and a destination MAC address).

Parameter	Value	Meaning
name	<name>	Specifies the name of the static-entry filter. This parameter must be less than 25 characters.
restriction		Specifies the forwarding behavior of the static entry, which can be one of the following keywords:
	allow	Allows packets to go to the set of ports specified by out-port-list .
	disallow	Prohibits packets from going to the set of ports specified by out-port-list .
	force	Forces packets to go to the set of ports specified by out-port-list , despite any port locks in effect on the ports.
source-mac	<MACaddr> any	Specifies the source MAC address. Specify any to allow any MAC address as the source-mac . Use this option for source or flow static entries.
source-mac-mask	<MACaddr>	Specifies the source MAC address. Use this option for source or flow static entries.
dest-mac	<MACaddr> any	Specifies the destination MAC address. Specify any to allow any MAC address as the dest-mac . Use this option for destination or flow static entries.
vlan	<VLAN-num> any	Specifies the VLAN number. Specify any to allow any VLAN.
dest-mac-mask	<MACaddr>	Specifies the destination MAC address. Use this option for destination or flow static entries.

Parameter	Value	Meaning
in-port-list	<port-list>	Specifies the ports to which you want to apply the static entry.
out-port-list	<port-list>	Specifies the ports to which you are allowing, disallowing, or forcing packets.

Restrictions

You should apply flow filters (specified using both a source MAC address and a destination MAC address) only to ports that are using flow-based bridging.

filters show address-filter

Mode

Enable

Format

```
filters show address-filter [all-source|all-destination|all-flow] [source-mac <MACaddr>  
dest-mac <MACaddr>] [ports <port-list>] [vlan <VLAN-num>]
```

Description

The **filters show address-filter** command displays the address filters currently configured on the RS.

Parameter	Value	Meaning
address-filter	all-source all-destination all-flow	Specifies the types of filters you want to display.
source-mac	<MACaddr>	Restricts the display to only those address filters that have been applied to this source MAC address.
dest-mac	<MACaddr>	Restricts the display to only those address filters that have been applied to this destination MAC address.
ports	<port-list>	Restricts the display to only those address filters that have been applied to the specified ports.
vlan	<VLAN-num>	Restricts the display to only those address filters that have been applied to the specified VLANs.

Restrictions

None.

filters show port-address-lock

Mode

Enable

Format

```
filters show port-address-lock [ports <port-list>] [vlan <VLAN-num>]  
[source-mac <MACaddr>]
```

Description

The **filters show port-address-lock** command displays the port-address-lock filters currently configured on the RS.

Parameter	Value	Meaning
ports	<port-list>	Restricts the display to only those port address locks that have been applied to the specified ports.
vlan	<VLAN-num>	Restricts the display to only those port address locks that have been applied to the specified VLANs.
source-mac	<MACaddr>	Restricts the display to only those port address locks that have been applied to this source MAC address.

Restrictions

None.

filters show secure-port

Mode

Enable

Format

```
filters show secure-port
```

Description

The **filters show secure-port** command displays the secure-port filters currently configured on the RS.

Restrictions

None.

filters show static-entry

Mode

Enable

Format

```
filters show static-entry [all-source|all-destination|all-flow] ports <port-list>  
vlan <VLAN-num> [source-mac <MACaddr> dest-mac <MACaddr>]
```

Description

The **filters show static-entry** command displays the static-entry filters currently configured on the RS.

Parameter	Value	Meaning
static-entry	all-source all-destination all-flow	Specifies the types of static entries you want to display.
ports	<port-list>	Restricts the display to only those static entries that have been applied to the specified ports.
vlan	<VLAN-num>	Restricts the display to only those static entries that have been applied to the specified VLANs.
source-mac	<MACaddr>	Restricts the display to only those static entries that have been applied to this source MAC address.
dest-mac	<MACaddr>	Restricts the display to only those static entries that have been applied to this destination MAC address.

Restrictions

None.

22 FRAME-RELAY COMMANDS

The following commands allow you to define frame relay service profiles, and specify and monitor frame relay High-Speed Serial Interface (HSSI) and standard serial ports.

22.1 COMMAND SUMMARY

The following table lists the **frame-relay** commands. The sections following the table describe the command syntax for each command.

frame-relay apply service <i><service name></i> ports <i><port list></i>
frame-relay clear stats-counter [frame-drop-qdepth-counter] [max-frame-enqueued-counter] [frame-drop-red-counter] [rmon] ports <i><port list></i>
frame-relay create vc <i><port></i>
frame-relay define service <i><service name></i> [Bc <i><number></i>] [Be <i><number></i>] [becn-adaptive-shaping <i><number></i>] [cir <i><number></i>] [high-priority-queue-depth <i><number></i>] [low-priority-queue-depth <i><number></i>] [med-priority-queue-depth <i><number></i>] [red on off] [red-maxTh-high-prio-traffic <i><number></i>] [red-maxTh-low-prio-traffic <i><number></i>] [red-maxTh-med-prio-traffic <i><number></i>] [red-minTh-high-prio-traffic <i><number></i>] [red-minTh-low-prio-traffic <i><number></i>] [red-minTh-med-prio-traffic <i><number></i>] [rmon on off]
frame-relay set fr-encaps-bgd ports <i><port list></i>
frame-relay set lmi [error-threshold <i><number></i>] [full-enquiry-interval <i><number></i>] [monitored-events <i><number></i>] [polling-interval <i><number></i>] [state enable disable] [type ansi617d-1994 q933a rev1] ports <i><port list></i>
frame-relay set payload-compression [type frf9_mode1_stac] port <i><port list></i>
frame-relay set peer-addr <i><IP address></i> ports <i><port list></i>
frame-relay show service <i><service name></i> all
frame-relay show stats ports <i><port name></i> [last-error] [lmi] [mibII]
frame-relay show stats ports <i><port name></i> summary

frame-relay apply service

Mode

Configure

Format

frame-relay apply service *<service name>* **ports** *<port list>*

Description

Issuing the **frame-relay apply service** command applies a previously defined service profile to a given Frame Relay virtual circuit (VC).

Parameter	Value	Meaning
service	<i><service name></i>	The name of the previously defined service profile applied to the given port(s) or interface(s).
ports	<i><port list></i>	The port(s) which to apply the pre-defined service profile. Specify a single VC or a comma-separated list of VCs.

Restrictions

Usage is restricted to Frame Relay VCs and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To apply the service “s1” to slot 2, VC 100 on serial ports 1 and 2:

```
rs(config)# frame-relay apply service s1 ports se.2.1.100,se.2.2.100
```

frame-relay clear stats-counter

Mode

Enable

Format

```
frame-relay clear stats-counter [frame-drop-qdepth-counter] [max-frame-enqueued-counter]
[frame-drop-red-counter] [rmon] ports <port list>
```

Description

The **frame-relay clear stats-counter** command specifies a particular statistic counter and resets those statistics to zero. There are statistic counters on each WAN or channelized T1/T3 port. Use the **frame-relay clear stats-counter** to clear the counter for an individual WAN port or for a group of ports.

Parameter	Value	Meaning
frame-drop-qdepth-counter		Specify this optional parameter to reset the frame drop counter to zero.
max-frame-enqueued-counter		Specify this optional parameter to reset the max enqueuedframes counter to zero.
frame-drop-red-counter		Specify this optional parameter to reset the packet drop counter to zero.
rmon		Specify this optional parameter to reset the rmon counter to zero.
	<i><port list></i>	The WAN or channelized T1/T3 port counter to clear.

Restrictions

Usage is restricted to Frame Relay VCs and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To clear the frame drop counter to zero on WAN port hs.3.1:

```
rs# frame-relay clear frame-drop-qdepth-counter port hs.3.1
```

frame-relay create vc

Mode

Configure

Format

frame-relay create vc <port>

Description

The **frame-relay create vc** command allows you to create a frame-relay virtual circuit (VC) on a slot and port location specified in the command line.

Parameter	Value	Meaning
port	<port>	The port on which to create a Frame Relay virtual circuit. Specify the port in the following format: <media>.<slot>.<port>.<dlci>.
	<media>	Media type.
	<slot>	Slot number where the module is installed.
	<port>	Port number.
	<dlci>	Data link connection identifier. Specify any number between 16 and 1007.

Restrictions

Usage is restricted to Frame Relay VCs and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To create a Frame Relay virtual circuit with a DLCI of 100 on serial port 1 of slot 3:

```
rs(config)# frame-relay create vc port se.3.1.100
```

frame-relay define service

Mode

Configure

Format

```
frame-relay define service <service name> [bc <number>] [be <number>]
[becn-adaptive-shaping <number>] [cir <number>] [high-priority-queue-depth <number>]
[low-priority-queue-depth <number>] [med-priority-queue-depth <number>] [red on | off]
[red-maxTh-high-prio-traffic <number>] [red-maxTh-low-prio-traffic <number>]
[red-maxTh-med-prio-traffic <number>] [red-minTh-high-prio-traffic <number>]
[red-minTh-low-prio-traffic <number>] [red-minTh-med-prio-traffic <number>]
[rmon on | off] [de-mark on | off]
```

Description

The **frame-relay define service** command specifies the following attributes for a newly created service profile:

- Number of bits per second contained in a committed burst for Frame Relay virtual circuits.
- Number of bits per second contained in an excessive burst for Frame Relay virtual circuits.
- Whether or not to simultaneously enable and specify the threshold at which adaptive shaping will activate when receiving BECN frames.
- The committed information rate (in bits per second) for Frame Relay virtual circuits.
- The allowable queue depth for high-, low-, and medium-priority frames on Frame Relay VCs.
- Activation or deactivation of Random Early Discard (RED) for Frame Relay circuits.
- The maximum and minimum threshold values for RED high-, low-, and medium-priority traffic.



Note

In general, Riverstone recommends that the maximum threshold values be less than or equal to the respective high-, low-, or medium-priority queue depth. The minimum threshold values should be one-third of the respective maximum threshold.

- Activation and deactivation of RMON for Frame Relay VCs. Note that before you can view RMON statistics such as ethernet statistics and history for Frame Relay ports, RMON has to be activated.

Parameter	Value	Meaning
service	<service name>	The name you assign to the newly created service profile.
Bc	<number>	The number of bits per second contained in a committed burst for a Frame Relay virtual circuit. Specify a number between 1 and 2,147,483,646 bits per second.

Parameter	Value	Meaning
be	<i><number></i>	The number of bits per second contained in an excessive burst for a Frame Relay virtual circuit. Specify a number between 1 and 2,147,483,646 bits per second.
becn-adaptive-shaping	<i><number></i>	The threshold (number of frames) at which adaptive shaping will activate when receiving BECN frames. Specify a number between 1 and 100,000 frames.
cir	<i><number></i>	The committed information rate (in bits per second) for Frame Relay virtual circuits. You can specify a number between 1 and 2,147,483,646 bits.
high-priority-queue-depth	<i><number></i>	The number of high-priority frames allowed in the frame relay queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 - 100 item range. The default value is 20.
low-priority-queue-depth	<i><number></i>	The number of low-priority frames allowed in the Frame Relay queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 to 100 item range. The default value is 20.
med-priority-queue-depth	<i><number></i>	The number of medium-priority frames allowed in the Frame Relay queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 to 100 item range. The default value is 20.
red	<i>on off</i>	Specifying the on keyword enables RED for Frame Relay ports. Specifying the off keyword disables RED for Frame Relay ports.
red-maxTh-high-prio-traffic	<i><number></i>	The maximum allowable number of frames for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-maxTh-low-prio-traffic	<i><number></i>	The maximum allowable number of frames for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-maxTh-med-prio-traffic	<i><number></i>	The maximum allowable number of frames for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-minTh-high-prio-traffic	<i><number></i>	The minimum allowable number of frames for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
red-minTh-low-prio-traffic	<i><number></i>	The minimum allowable number of frames for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
red-minTh-med-prio-traffic	<i><number></i>	The minimum allowable number of frames for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.

Parameter	Value	Meaning
rmon	on off	Specifying the on keyword enables RMON for Frame Relay VCs. Specifying the off keyword disables RMON for frame relay VCs.
de-mark	on off	Specifying the on keyword enables DE marking for best traffic. Specifying the off keyword disables DE marking for best traffic. Default is off .

Restrictions

When defining a value for **bc**, you must also be sure to define an appropriate value for **cir**. When defining a value for **cir**, you must also be sure to define an appropriate value for **bc**.

Examples

Specify a Frame Relay virtual circuit with the following attributes:

- Committed burst value of 35 million and excessive burst value of 30 million.
- BECN active shaping at 65 thousand frames.
- Committed information rate (CIR) of 120 million bits per second.
- Leave high-, low-, and medium-priority queue depths set to factory defaults.
- Random Early Discard (RED) disabled.
- RMON enabled.

The command line necessary to set up a service profile with the above attributes would be as follows:

```
rs(config)# frame-relay define service profile1 Bc 35000000 Be 30000000  
becn-adaptive-shaping 65000 cir 120000000 red off rmon on
```

frame-relay set fr-encaps-bgd

Mode

Configure

Format

frame-relay set fr-encaps-bgd ports *<port list>*

Description

Issuing the **frame-relay set fr-encaps-bgd** command forces ingress packets to be encapsulated in the bridged format on a given Frame Relay VC.

Parameter	Value	Meaning
ports	<i><port list></i>	The port(s) on which you use bridged encapsulation. You can specify a single VC or a comma-separated list of VCs.

Restrictions

Usage is restricted to Frame Relay VCs and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To force the bridged encapsulation to slot 2, VC 100 on serial ports 1 and 2:

```
rs(config)# frame-relay fr-encaps-bgd ports se.2.1.100,se.2.2.100
```

frame-relay set lmi

Mode

Configure

Format

```
frame-relay set lmi [error-threshold <number>] [full-enquiry-interval <number>]
[monitored-events <number>] [polling-interval <number>] [state enabled | disabled]
[type ansi617d-1994 | q933a | rev1] ports <port list>
```

Description

The **frame-relay set lmi** command specifies the following local management interface (LMI) attributes:

- The number of times the router will attempt to poll an LMI interface before declaring it down. Define a value between 1 and 10, inclusive.
- The number of status enquiries that will be sent before a full status enquiry is requested. Define a value between 1 and 255, inclusive.
- The number of status enquiries over which various pieces of LMI information can be collected and tabulated. For example, you can tabulate the number of times an interface was declared down/lost due to a lack of proper responses to status enquiries. Define a value between 1 and 10, inclusive.
- The number of seconds that pass between successive status enquiry messages. Define a value between 5 and 30, inclusive.
- Whether or not LMI messages are sent. LMI messages are not sent by default.
- The LMI type for frame relay WAN ports.

Parameter	Value	Meaning
error-threshold	<number>	The number of unanswered status enquiries that the router will make before declaring an interface to be down.
full-enquiry-interval	<number>	The number of status enquiries that will be sent before a full report on status is compiled and transmitted.
monitored-events	<number>	The number of status enquiries over which collection and tabulation of various pieces of LMI information will take place.
polling-interval	<number>	The amount of time (in seconds) that will pass before a subsequent status enquiry takes place.
state	enabled disabled	Enables the sending and receiving of LMI messages. If LMI messages are enabled, the operational status of each VC is determined by the LMI messages. If LMI messages are disabled, each VC is assumed to be operationally “up”. LMI messages are disabled by default.

Parameter	Value	Meaning
type	ansi617d-1994 q933a rev1	The LMI type for frame relay WAN ports. You can only specify the ansi617d-1994 , q933a , or rev1 keywords to define as the LMI type for WAN ports.
ports	<port list>	The port or ports that will assume the LMI service profile behavior.

Restrictions

None.

Examples

To set the number of status enquiries that will be sent before compilation and transmission of a full status report for serial port 2 of slot 2 to 75 enquiries:

```
rs(config)# frame-relay set lmi full-enquiry-interval 75 ports se.2.2
```

frame-relay set payload-compress

Mode

Configure

Format

```
frame-relay set payload-compress [type frf9_mode1_stac] ports <port list>
```

Description

The **frame-relay set payload-compress** command enables packet compression according to Mode 1 of FRF 9. If this command is not configured, packet compression is not enabled.

Parameter	Value	Meaning
type	frf9_mode1_stac	Specifies the Stacker FRF 9, Mode 1 compression algorithm. This is the default value.
ports	<port list>	The port(s) on which you enable packet compression. You can specify a single VC or a comma-separated list of VCs.

Restrictions

Usage is restricted to Frame Relay VCs and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To enable Stacker FRF 9, Mode 1 packet compression on slot 3, VC 300 on serial port 1:

```
rs(config)# frame-relay set payload-compress ports se.3.1.300
```

frame-relay set peer-addr

Mode

Configure

Format

frame-relay set peer-addr *<IP address>* **ports** *<port list>*

Description

Issuing the **frame-relay set peer-addr** command sets the peer address if it can't be resolved by InArp.

Parameter	Value	Meaning
peer - addr	<i><IP address></i>	The IP or IPX address you use.
ports	<i><port list></i>	The location of the port to which you assign the address.

Restrictions

Usage is restricted to Frame Relay VCs and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To assign an IP address 10.1.1.1/16 to slot 2, VC 100 on serial port 1:

```
rs(config)# frame-relay set peer-addr ip-addr 10.1.1.1/16 ports se.2.1.100
```

frame-relay show service

Mode

Enable

Format

frame-relay show service *<service name>* | **all**

Description

The **frame-relay show service** command displays the available Frame Relay service profiles.

Parameter	Value	Meaning
service	<i><service name></i>	The name of a particular pre-defined service profile.
	all	Displays all of the available Frame Relay service profiles.

Restrictions

None.

Example

To display the available Frame Relay service profiles named “prof1”:

```
rs# frame-relay show service prof1
```

frame-relay show stats

Mode

Enable

Format

```
frame-relay show stats ports <port name> [last-error] [lmi] [mibII]
```

Description

The **frame-relay show stats** command displays the following Frame Relay port statistics for the given port:

- The last reported Frame Relay error.
- The active Frame Relay LMI parameters.
- The MIBII statistics for Frame Relay WAN ports.
- Statistics for channelized T1/T3 ports.

Parameter	Value	Meaning
ports	<i><port name></i>	The port or ports for which you want to display statistics.
last-error		Specifying the last-error keyword displays the last reported frame relay error for the given port.
lmi		Specifying the lmi keyword displays the active frame relay LMI parameters.
mibII		Specifying the mibII keyword displays the MIBII statistics for frame relay WAN ports.

Restrictions

The **last-error**, **mibii**, and **lmi** keywords are for ports only (no VC designators allowed). Otherwise, the port name may have the “VC” designator.

Examples

To display the last recorded error and MIB II statistics for serial port 1 of slot 3:

```
rs# frame-relay show stats ports se.3.1 last-error mibII
```

To display the VC statistics for serial port 1, slot 3, VCs 1-10:


```
rs# frame-relay show stats ports se.3.1.1-10
```

frame-relay show stats summary

Mode

Enable

Format

frame-relay show stats summary port *<port name>*

Description

The **frame-relay show stats summary** command displays all of the summary information for VC statistics.

Parameter	Value	Meaning
ports	<i><port name></i>	The port or ports for which you wish to display summary statistics.

Restrictions

None.

Example

To display summary statistics for serial port 1 of slot 4, VC 100:

```
rs# frame-relay show stats summary ports se.4.1.100
```

23 GARP COMMANDS

The **garp** commands set and show the timers for the Generic Attribute Registration Protocol (GARP).

23.1 COMMAND SUMMARY

The following table lists the `garp` commands. The sections following the table describe the command syntax.

<code>garp set timers leaveall <number> leave <number> join <number></code>
<code>garp show timers</code>

garp set timers

Mode

Configure

Format

```
garp set timers leaveall <number>|leave <number>|join <number>
```

Description

The **garp set timers** command lets you set values for the different GARP timers.

Parameter	Value	Meaning
leaveall	<number>	Sets the LeaveAll timer in milliseconds.
leave	<number>	Sets the Leave timer in milliseconds. It should be three times more than the join timer.
join	<number>	Sets the Join timer in milliseconds.

Restrictions

None.

garp show timers

Mode

Enable

Format

garp show timers

Description

The **garp show timers** command lets you display the GARP timers.

Restrictions

None.

Example

The sample output shows the values set for the Leave All, Leave and Join timers.

```
rs# garp show timers
GARP Timers:
  Leave All Timer: 10000 milliseconds
  Leave Timer    : 600 milliseconds
  Join Timer     : 200 milliseconds
rs#
```


24 GVRP COMMANDS

The **gvrp** commands lets you set parameters for the GARP VLAN Registration Protocol (GVRP).

24.1 COMMAND SUMMARY

The following table lists the `gvrp` commands. The sections following the table describe the command syntax.

<code>gvrp clear statistics <port> all-ports</code>
<code>gvrp enable dynamic-vlan-creation</code>
<code>gvrp enable ports</code>
<code>gvrp set applicant-status non-participant</code>
<code>gvrp set registration-mode forbidden ports <port-list> all-ports</code>
<code>gvrp show applicant-status</code>
<code>gvrp show error-statistics</code>
<code>gvrp show registration-mode</code>
<code>gvrp show statistics</code>
<code>gvrp show status</code>
<code>gvrp show used attributes</code>
<code>gvrp start</code>

gvrp clear statistics

Mode

Enable

Format

gvrp clear statistics <port>|all-ports

Description

The **gvrp clear statistics** command clears various GVRP statistics on the specified ports.

Parameter	Value	Meaning
statistics	<port>	Clears GVRP statistics on the port specified.
	all-ports	Clears GVRP statistics on all ports.

Restrictions

None.

gvrp enable dynamic-vlan-creation

Mode

Configure

Format

```
gvrp enable dynamic-vlan-creation
```

Description

The **gvrp enable dynamic-vlan-creation** command enables VLANs to be dynamically created through GVRP.

Restrictions

None.

gvrp enable ports

Mode

Configure

Format

gvrp enable ports *<port-list>*

Description

The **gvrp enable ports** command enables GVRP on the specified ports.

Parameter	Value	Meaning
ports	<i><port-list></i>	Enables GVRP on the ports specified.

Restrictions

None.

gvrp set applicant-status

Mode

Configure

Format

```
gvrp set applicant-status non-participant ports <port-list> | all-ports
```

Description

The **gvrp set applicant-status** command sets a port's status to non-participant, preventing it from sending GARP PDUs.

Parameter	Value	Meaning
ports	<port-list>	Specifies the ports that will be set to non-participant status.
	all-ports	Specifies that all ports will be set to non-participant status.

Restrictions

None.

gvrp set registration-mode

Mode

Configure

Format

```
gvrp set registration-mode forbidden ports <port-list>|all-ports
```

Description

The **gvrp set registration-mode** command sets the port(s) to forbidden registration mode. This mode deregisters all VLANs on the specified port and prevents any VLAN creation or registration on that port.

Parameter	Value	Meaning
ports	<port-list>	Sets the specified port(s) to forbidden registration mode.
	all-ports	Sets <i>all</i> ports to forbidden registration mode.

Restrictions

None.

gvrp show applicant status

Mode

Enable

Format

gvrp show applicant-status ports <port-list>|all-ports

Description

The **gvrp show applicant-status** command displays the applicant status of ports.

Parameter	Value	Meaning
ports	<port-list>	Specifies the ports for which the applicant status will be displayed.
	all-ports	Specifies that the applicant status of all ports will be displayed.

Restrictions

None.

Example

The sample output shows that port gi.3.1's applicant status is set to non-participant and all the other ports participate in GVRP.

```
rs# gvrp show applicant-status ports all-ports
Port: gi.3.1 - Non-Participant
Port: gi.3.2 - Participant
Port: gi.3.3 - Participant
Port: gi.3.4 - Participant
Port: gi.3.5 - Participant
Port: gi.3.6 - Participant
Port: gi.3.7 - Participant
Port: gi.3.8 - Participant
rs#
```

gvrp show error-statistics

Mode

Enable

Format

gvrp show error-statistics <port-list>|all-ports

Description

The **gvrp show error-statistics** command displays the GVRP errors of ports.

Parameter	Value	Meaning
error statistics	<port-list>	Specifies the ports for which GVRP errors will be displayed.
	all-ports	Specifies that GVRP errors for <i>all</i> ports will be displayed.

Restrictions

None.

Example

The **gvrp show error-statistics** command displays the number and type of GVRP errors encountered by each port on which GVRP is enabled.

```
rs# gvrp show error-statistics all-ports
GVRP Error statistics:
-----
Legend:
  INVPROT  : Invalid Protocol Id      INVPLEN : Invalid PDU Length
  INVATYP  : Invalid Attribute Type   INVALEN : Invalid Attribute Length
  INVAVAL  : Invalid Attribute Value  INVEVENT: Invalid Event

Port      INVPROT  INVPLEN  INVATYP  INVALEN  INVAVAL  INVEVENT
-----
gi.3.1    0         0        0         0         0         0
gi.3.2    0         0        0         0         0         0
gi.3.3    0         0        0         0         0         0
gi.3.4    0         0        0         0         0         0
gi.3.5    0         0        0         0         0         0
gi.3.6    0         0        0         0         0         0
gi.3.7    0         0        0         0         0         0
gi.3.8    0         0        0         0         0         0
rs#
```

gvrp show registration-mode

Mode

Enable

Format

gvrp show registration-mode ports *<port-list>* | all-ports

Description

The **gvrp show registration-mode** command displays whether the ports are in normal registration mode, fixed registration mode, or forbidden registration mode.

Parameter	Value	Meaning
ports	<i><port-list></i>	Specifies the ports for which the registration mode will be displayed.
	all-ports	Specifies that the registration mode of <i>all</i> ports will be displayed.

Restrictions

None.

Example

Registration modes are set on a port/VLAN basis. The sample output displays the following:

- Port gi.3.1 is in fixed registration mode for VID 3. But for all other VLANs, port gi.3.1 is in normal mode.
- Port gi.3.2 was set to forbidden mode. It is in fixed registration mode for VID4 because this VLAN was explicitly configured.
- Port gi.3.3 is in normal mode for all VIDs except VID 4 because this VLAN was explicitly.

1

```
rs# gvrp show registration-mode ports all-ports
Port: gi.3.1, vid: 3, Fixed
Port: gi.3.1, vid: 4, Normal
Port: gi.3.1, vid: 5, Normal
Port: gi.3.1, vid: 6, Normal
Port: gi.3.1, vid: 7, Normal
Port: gi.3.2, vid: 3, Forbidden
Port: gi.3.2, vid: 4, Fixed
Port: gi.3.2, vid: 5, Forbidden
Port: gi.3.2, vid: 6, Forbidden
Port: gi.3.2, vid: 7, Forbidden
Port: gi.3.3, vid: 3, Normal
Port: gi.3.3, vid: 4, Fixed
Port: gi.3.3, vid: 5, Normal
Port: gi.3.3, vid: 6, Normal
Port: gi.3.3, vid: 7, Normal
.
.
.
```


gvrp show statistics

Mode

Enable

Format

gvrp show statistics <port-list>|all-ports

Description

The **gvrp show statistics** command displays the GVRP statistics of the ports.

Parameter	Value	Meaning
statistics	<port-list>	Specifies the ports for which GVRP statistics will be displayed.
	all-ports	Specifies that GVRP statistics will be displayed for <i>all</i> ports.

Restrictions

None.

Example

The **gvrp show statistics** command displays the number and type of GARP PDUs that were received and sent on each port.

```
rs# gvrp show statistics all-ports
GVRP statistics:
-----
Legend:
  rJE : Join Empty Received      rJIn: Join In Received
  rEmp : Empty Received          rLIn: Leave In Received
  rLE : Leave Empty Received     rLA : Leave All Received
  sJE : Join Empty Sent          sJIn: Join In Sent
  sEmp : Empty Sent              sLIn: Leave In Sent
  sLE : Leave Empty Sent         sLA : Leave All Sent
```

Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
----	---	----	----	----	---	---	---	----	---	----	---	---
gi.3.1	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.2	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.3	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.4	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.5	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.6	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.7	0	0	0	0	0	0	0	0	0	0	0	0
gi.3.8	0	0	0	0	0	0	0	0	0	0	0	0
.												
.												
.												

gvrp show status

Mode

Enable

Format

gvrp show status

Description

The `gvrp show status` command displays the ports' GVRP status.

Restrictions

None.

Example

The **gvrp show status** command shows the following:

- whether GVRP was enabled on the RS,
- the ports on which GVRP was enabled,
- the ports that were set to non-participant status, and
- the ports that were set to forbidden registration mode.

```
rs# gvrp show status
GVRP Status
-----

GVRP is started
Dynamic Vlan Creation is Enabled
Ports GVRP enabled on: gi.3.(1-8)
Applicant Mode set to Non-Participant on Ports: gi.3.1
Registrar Mode set to Forbidden on Ports: gi.3.2
rs#
```

gvrp start

Mode

Configure

Format

gvrp start

Description

The **gvrp start** command enables GVRP on the RS.

Restrictions

None.

25 HRT COMMAND

Use the **hrt** commands to set Hardware Routing Table (HRT) parameters.

25.1 COMMAND SUMMARY

The following table lists the **hrt** commands. The sections following the table describe the command syntax for each command.

<code>hrt enable slot <number> [all]</code>
<code>hrt set icmp icmp-redirect-count <number></code>

hrt enable

Mode

Configure

Format

```
hrt enable slot <number> | [all]
```

Description

Hardware Routing Table (HRT) is disabled by default on the RS. Use the **hrt enable** command to enable HRT on a specific line card or on all line cards. HRT is disabled by negating the command in the configuration file. When HRT is disabled, the RS uses L-3 flows to forward packets.

Parameter	Value	Meaning
slot	<number>	Specifies the slot number that contains the ports on which HRT will be enabled. <number> is the slot number. Specify a value between 1 and 32.
all		Specify all to enable HRT on all slots.

Restrictions

None.

Example

To enable HRT on all slots:

```
hrt enable slot all
```

hrt set icmp icmp-redirect-count

Mode

Configure

Format

```
hrt set icmp icmp-redirect-count <number>
```

Description

An RS may receive packets that contain the same source and destination port. When it does, the CPU sends an ICMP redirect message to the originating device. The message contains new source and destination addresses, used to redirect the packets. Use the **hrt set icmp** command to set the number of packets that an RS receives before it sends the ICMP redirect message.

Parameter	Value	Meaning
icmp-redirect-count	<number>	Specifies the number of packets with the same entry and exit port that the RS receives before it sends an ICMP redirect message. For <number>, specify a value from 0 to 65535.

Restrictions

None.

Example

To redirect after five packets:

```
hrt set icmp icmp-redirect-count 5
```


26 IGMP COMMANDS

The **igmp** commands let you display and set IGMP parameters.

26.1 COMMAND SUMMARY

The following table lists the **igmp** commands. The sections following the table describe the command syntax for each command.

<code>igmp enable interface <name/ipAddr></code>
<code>igmp enable vlan <vlan-name></code>
<code>igmp join group <ipAddr> interface <name/ipAddr></code>
<code>igmp set interface <name/ipAddr> [allowed-groups <group-list> not-allowed-groups <group-list>] [use-all-ports]</code>
<code>igmp set queryinterval <num></code>
<code>igmp set responsetime <num></code>
<code>igmp set vlan <vlan-name> [host-timeout <num>] [querier-timeout <num>] [router-timeout <num> leave-timeout <num>]</code>
<code>igmp show interfaces [group <ipAddr> interface <name/ipAddr>]</code>
<code>igmp show memberships [group <ipAddr> port <num>]</code>
<code>igmp show timers</code>
<code>igmp show vlans</code>
<code>igmp start-snooping</code>

igmp enable interface

Mode

Configure

Format

```
igmp enable interface <name/ipAddr>
```

Description

The **igmp enable interface** command enables IGMP on the specified interface.

Parameter	Value	Meaning
interface	<name/ipAddr>	Name or IP address of the interface on which you are enabling IGMP.

Restrictions

IGMP is not enabled on tunnels.

Example

To enable IGMP on interface 10.50.1.2:

```
rs(config)# igmp enable interface 10.50.1.2
```

igmp enable vlan

Mode

Configure

Format

igmp enable vlan <vlan-name>

Description

The **igmp enable vlan** command enables IGMP snooping on a specified VLAN. By default, IGMP snooping is disabled on all VLANs.

Parameter	Value	Meaning
vlan	<vlan-name>	Is the name of the VLAN where IGMP snooping is to be enabled.

Restrictions

Layer 3 multicasting and layer-2 snooping cannot be run simultaneously on the same VLAN.

Example

To enable igmp snooping on VLAN blue:

```
rs(config)# igmp enable vlan blue
```

igmp join group

Mode

Configure

Format

```
igmp join group <ipAddr> interface <name/ipAddr>
```

Description

The **igmp join group** command allows an interface to join an IGMP group statically. Most interfaces join IGMP groups dynamically, outside the control of the user. This command allows the user to configure an IGMP group onto an interface statically.

Parameter	Value	Meaning
group	<ipAddr>	Specifies the multicast address.
interface	<name/ipAddr>	Specifies the interface name or IP address.

Restrictions

None.

Examples

To configure the IGMP group '255.2.0.0' on interface 200.1.1.1:

```
rs(config)# igmp join group 255.2.0.0 interface 200.1.1.1
```

igmp set interface

Mode

Configure

Format

igmp set interface <name/ipAddr> [allowed-groups <group-list> | not-allowed-groups <group-list>]
[use-all-ports]

Description

Sets IGMP parameters on a per-interface basis to control group restrictions and optimization.

Parameter	Value	Meaning
interface	<name/ipAddr>	Interface name or IP address.
allowed-groups	<group-list>	Restricts the groups to only those specified.
not-allowed-groups	<group-list>	Allows any groups besides those specified.
Note Specify only one of the above two options, as they are mutually exclusive.		
use-all-ports		Disables per-port IGMP control. By default, per-port IGMP control is enabled.
Note If the traffic is being supplied by a dvmrp tunnel, which uses CPU-based switching, then for efficiency reasons, port based optimization is not used by this traffic.		

Restrictions

None.

Examples

The following is an example of the **igmp set interface** command::

```
rs(config)# igmp set interface 200.1.1.1 allowed-groups 225.2.0.0/16
```

The above command will allow only memberships to groups falling in the specified range. Outside this range, all groups are implicitly ignored.

igmp set queryinterval

Mode

Configure

Format

```
igmp set queryinterval <num>
```

Description

Sets the IGMP Host Membership Query time interval. The interval you set applies to all ports on the RS.

Parameter	Value	Meaning
queryinterval	<num>	A value from 20 – 3600 seconds. The default is 125 seconds.

Restrictions

None.

Example

To set the query interval to 30 seconds:

```
rs(config)# igmp set queryinterval 30
```

igmp set responsetime

Mode

Configure

Format

```
igmp set responsetime <num>
```

Description

Sets the wait time for IGMP Host Membership responses. The wait time you set applies to all ports on the RS.

Parameter	Value	Meaning
responsetime	<num>	Response wait time in seconds. Specify a number from 10 – 3599. The default is 10.

Restrictions

None.

Examples

To set the Host Membership response wait time to 20 seconds:

```
rs(config)# igmp set responsetime 20
```

igmp set vlan

Mode

Configure

Format

```
igmp set vlan <vlan-name> [host-timeout <num>] [querier-timeout <num>] [router-timeout <num> leave-timeout <num>] [filter-ports <port-list>] [permanent-ports <port-list>]
```

Description

The **igmp set vlan** command allows you to set parameters for VLAN-based IGMP snooping.

Parameter	Value	Meaning
vlan	<vlan-name>	Name of VLAN.
host-timeout	<num>	Allows adjusting to long host timeout values that may have been set up for the IGMP querier. The default value is 250 seconds.
querier-timeout	<num>	Allows adjusting to long timeout values that may have been set up for the IGMP querier. The default value is 260 seconds.
router-timeout	<num>	Allows adjusting to long timeout values that may have been set up for the routers. Different versions of DVMRP can have different timeouts. The default value is 140 seconds.
leave-timeout	<num>	Allows quicker timeout if IGMP v2 leave messages are used. The value is nominally 10 seconds.
filter-ports	<port-list>	Allows forced filtering of certain ports from multicast data. Setting ports as filter ports ensures that no host there will join any memberships. A port can optionally be either a permanent port or a filter port, but not both.
permanent-ports	<port-list>	Allows forcing of mulicast data if present on certain ports. A port can optionally be either a permanent port or a filter port, but not both.

Restrictions

None.

Example

To set parameters for IGMP snooping on the VLAN blue:

```
rs(config)# igmp set vlan blue host-timeout 125 querier-timeout 130 router-timeout 70
```


igmp show interfaces

Mode

Enable

Format

```
igmp show interfaces [group <ipAddr>|interface <name/ipAddr>]
```

Description

The **igmp show interfaces** command shows memberships on a specified interface or for a particular multicast group address. Using the command to show interfaces by group will list all the interfaces that belong to the group.



Note

This command is similar to **igmp show memberships**, except where the **igmp show interfaces** command shows interface details, the **igmp show memberships** command shows ports.

Parameter	Value	Meaning
group	<ipAddr>	Address of a multicast group.
interface	<name/ipAddr>	Name or address of an interface.

Restrictions

None.

Example

To show information about the interfaces running IGMP:

```
rs# igmp show interfaces

Address: 172.1.1.10 Subnet: 172.1.1/24 Met: 1 Thr: 1
Name : mls15 State: Up Querier Leaf Igmp Dvmrp

Address: 207.135.89.64 Subnet: 207.135.89.0/25 Met: 1 Thr: 1
Name : company State: Up Querier Leaf Igmp Dvmrp
Groups : 224.0.1.12
224.1.127.255
224.0.1.24
224.2.127.253
224.2.127.254

Address: 10.135.89.10 Subnet: 10.135.89.0/25 Met: 1 Thr: 1
Name : test State: Up Querier Igmp Dvmrp

Address: 207.135.122.11 Subnet: 207.135.122.8/29 Met: 1 Thr: 1
Name : mbone State: Up Igmp Dvmrp
Groups : 224.0.1.11
224.0.1.12
224.2.127.254
239.255.255.255
224.2.127.253
```

Table 26-1 Display field descriptions for the igmp show interface command

FIELD	DESCRIPTION
Address	IP address of the interface
Subnet	Subnet of the interface
Met	DVMRP cost of the interface
Thr	Time-To-Live (TTL) Threshold of the interface. Any incoming packets with a TTL that is less than or equal to the threshold may be consumed locally but will not be forwarded.
Name	Name of the interface
State	Up—Indicates that this interface is up Dn—Indicates that this interface is down Querier—Indicates that this interface is an IGMP querier Leaf—Indicates that this interface is a leaf node in the multicast distribution tree Igmp—Indicates that IGMP is enabled on this interface Dvmrp—Indicates that DVMRP is enabled on this interface
Groups	List of the groups that are present on this interface. If no groups are listed, it means that there are no multicast receivers on this interface.

igmp show memberships

Mode

Enable

Format

```
igmp show memberships [group <ipAddr>|port <num>]
```

Description

The **igmp show memberships** command displays IGMP host members on a specific interface and/or for a particular multicast group.

Parameter	Value	Meaning
group	<ipAddr>	Address of the multicast group for which to display host memberships.
port	<num>	Port numbers on which the members reside.

Restrictions

None.

Examples

To display host members for multicast group 225.0.1.20:

```
rs(config)# igmp show memberships group 225.0.1.20
```

To display host members for multicast group 225.0.1.20 on port et.1.1:

```
rs(config)# igmp show memberships group 225.0.1.20 port et.1.1
```

The following is a fuller example:

```
rs(config)# igmp show memberships

Group : 224.0.1.11 Ports: et.1.1
Group : 224.0.1.12 Ports: et.1.1
et.5.1
Group : 224.0.1.24 Ports: et.5.1
Group : 224.1.127.255 Ports: et.5.1
Group : 224.2.127.253 Ports: et.1.1
et.5.1
Group : 224.2.127.254 Ports: et.1.1
et.5.1
Group : 239.255.255.255 Ports: et.1.1
```

igmp show timers

Mode
Enable

Format

igmp show timers

Description

The **igmp show timers** command displays global IGMP timer properties, as well as statistics for each IGMP interface.

Restrictions

None.

Example

The following is a sample output display:

fk-r4# igmp show timers		
Query Timer= 125,	Group Expire Timer= 260	
Querier Timeout = 255	Host Report Delay = 10	
Name : icast_svr	Address: 10.10.1.10	Querier
Joins :3	Expires: 1	Next Query in 16 seconds

Table 26-2 Display field descriptions for the igmp show timers command

FIELD	DESCRIPTION
Query Timer	How long the router waits, in seconds, before sending out the next query
Group Expire Timer	How long the router waits, in seconds, for a response to its query before marking a group as expired
Querier Timeout	On multiaccess local area networks (LANs), there can be multiple IGMP queriers. In this case, one router can be elected among all the queriers to be the default querier. The other routers will suppress their queries as long as they see continuous queries from the elected querier. The querier timeout is how long, in seconds, the other routers will wait for action from the elected querier before assuming that it is down and reelecting among themselves for a new default querier.
Host Report Delay	The time, in seconds, within which hosts have to respond to a query
Name	Name of the interface
Address	Address of the interface

Table 26-2 Display field descriptions for the igmp show timers command (Continued)

FIELD	DESCRIPTION
Querier	Indicates that this interface is an IGMP querier
Joins	The number of multicast groups that have been joined on this interface
Expires	The number of multicast groups that have expired on this interface

igmp show vlans

Mode
Enable

Format

igmp show vlans [detail] [name <name>] [timers]

Description

The **igmp show vlans** command displays port, querier, multicast group, and group membership information for each VLAN. If you start IGMP snooping on a VLAN using the **igmp start-snooping** command, you can use this command to view the resulting statistics. For more information on IGMP snooping, refer to the *Riverstone Networks RS Switch Router User Guide* .

Parameter	Value	Meaning
detail		Shows all IGMP membership information.
name	<name>	Shows IGMP membership information for the specified VLAN.
timers		Shows all IGMP L2 snooping related timers.

Restrictions

None.

Example

The following is a sample output display:

fk-r4# igmp show vlans		
Vlan: mcast	VLAN-ID: 100	Ports: et.2.(5-8)
Querier Ports: et.2.5		
Group: 224.2.127.254	Ports:et.2.(5-6,8)	
Group: 225.1.10.10	Ports:et.2.(5-6,8)	

Table 26-3 Display field descriptions for the igmp show vlans command

FIELD	DESCRIPTION
Vlan	Name of the VLAN
VLAN- ID	VLAN's id

Table 26-3 Display field descriptions for the igmp show vlans command (Continued)

FIELD	DESCRIPTION
Ports	The ports that belong to this VLAN
Querier Ports	The port(s) that the IGMP snoop has determined to be the querier port(s) on this VLAN. (Through traffic monitoring, the snoop process has noticed these ports emitting queries.)
Group	Address of the multicast group
Ports	The port(s) that the IGMP snoop has determined to have membership in the listed multicast group. (Through traffic monitoring, the snoop process has noticed these ports responding to queries for this multicast group.)

igmp start-snooping

Mode

Configure

Format

```
igmp start-snooping
```

Description

The **igmp start-snooping** command starts IGMP snooping on enabled VLANs, a process which allows the switch on a VLAN to determine the

- IGMP querier ports on the VLAN
- Multicast groups on the VLAN, and the
- VLAN Ports that belong to those multicast groups

by monitoring L2 traffic on the VLAN.

This task is independent of L3 multicasting.

Restrictions

None.

27 INTERFACE COMMANDS

The **interface** commands let you create IP and IPX interfaces, add network mask and broadcast address information to existing IP interfaces, and display configuration information for IP and IPX interfaces.

27.1 COMMAND SUMMARY

The following table lists the **interface** commands. The sections following the table describe the command syntax for each command.

interface add ip <InterfaceName> address-netmask <ipAddr-mask> peer-address [<ipAddr>] [broadcast <ipAddr>]
interface add ipx <InterfaceName> address <ipAddr> [peer-address <netaddr>.<macaddr>] [output-mac-encapsulation <MACencap>]
interface create ip <InterfaceName> address-netmask <ipAddr-mask> [broadcast <ipAddr>] vlan <name> port <port> mtu <num> [output-mac-encapsulation <MACencap>] [up down] [mac-addr <MACaddr-spec>] [type broadcast point-to-point] [unnumbered <InterfaceName>] [unnumbered-addr <ipaddr>]
interface create ipx <InterfaceName> address <ipxAddr> vlan <name> port <port> [output-mac-encapsulation <MACencap>] [up down] [mac-addr <MACaddr-spec>] [mtu <num>]
interface show ip <InterfaceName> all [brief]
interface show ipx <InterfaceName> all [brief]

interface add ip

Mode
Configure

Format

interface add ip *<InterfaceName>* **address-netmask** *<ipAddr-mask>* **peer-address** [*<ipAddr>*]
[broadcast *<ipAddr>*]

Description

The **interface add ip** command configures secondary addresses for an existing IP interface. Use this command to configure a secondary IP address and netmask, a secondary peer-address, and a secondary broadcast address.



Note The interface must already exist. To create an interface, enter the **interface create ip** command.

Parameter	Value	Meaning
ip	<i><InterfaceName></i>	Name of the IP interface; for example, int4.
address-netmask	<i><ipAddr-mask></i>	Secondary IP address and netmask of this interface. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the RS uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).
peer - address	<i><ipAddr></i>	Secondary IP address of the peer for this port. Primarily used for setting up connection with another WAN port or setting up a VC with another ATM port. For WAN and ATM ports only.
broadcast	<i><ipAddr></i>	Secondary broadcast address of this interface.

Restrictions

You can use this command only on an interface that has already been created using the **interface create ip** command.

Example

To configure a secondary address of 10.23.4.36 with a 24-bit netmask (255.255.255.0) on the IP interface int4:

```
rs(config)# interface add ip int4 address-mask 10.23.4.36/24
```

interface add ipx

Mode

Configure

Format

```
interface add ipx <InterfaceName> address <ipxAddr> [peer-address <netaddr>.<macaddr>]  
[output-mac-encapsulation <MACencap>]
```

Description

The **interface add ipx** command configures secondary addresses for an existing IPX interface.

**Note**

The interface must already exist. To create an interface, enter the **interface create ipx** command.

Parameter	Value	Meaning
ipx	<InterfaceName>	Name of the IP interface; for example, int4.
address	<ipxAddr>	Secondary IPX network address of this interface, specified in a hexadecimal number.
peer - address	<netaddr>.<macaddr>	Secondary IPX address of the peer for this port. Primarily used for setting up connection with another WAN port. The peer - address contains the network address, a period (.), then the mac address. This can be illustrated as follows: a1b2c3d4.aa:bb:cc:dd:ee:ff For WAN ports only.
output-mac-encapsulation	<MACencap>	The output MAC encapsulation associated with this interface. You can specify one of the following:
	ethernet_ii	The default.
	ethernet 802.3	
	ethernet_snap	
	ethernet_802.2_ipx	

Restrictions

You can use this command only on an interface that has already been created using the **interface create ipx** command.

Example

To configure a secondary address of 10 (hexadecimal) on the IPX interface int4 with an 802.3 output encapsulation scheme:

```
rs(config)# interface add ipx int4 address 10 output-mac-encapsulation  
ethernet_802.3
```

interface create ip

Mode

Configure

Format

```
interface create ip <interface-name> address-netmask <ipAddr-mask> [broadcast <ipaddr>]
[peer-address <ipaddr>] vlan <name>|port <port> mtu <num> [output-mac-encapsulation
<MACencap>] [up|down] [mac-addr <MACaddr-spec>] [type broadcast|point-to-point]
[unnumbered <string>] [unnumbered-addr <ipaddr>]
```

Description

The **interface create ip** command creates and configures an IP interface. Configuration of an IP interface can include information such as the interface's name, IP address, netmask, broadcast address, and so on. You can also create an interface in a disabled (**down**) state instead of the default enabled (**up**) state.

The RS is pre-allocated a pool of 64 MAC addresses. By default, each new IP interface is automatically configured with the lowest MAC address in the pool (the “base” MAC address). However, you can assign an interface a different MAC address by using the **mac-addr** option.

Interfaces on the RS are logical interfaces. Therefore, you can associate an interface with a single port or with multiple ports.

- To associate an interface with a single port, use the **port** option with the **interface create** command.
- To associate an interface with multiple ports, first create an IP VLAN and add ports to it, then use the **vlan** option with the **interface create** command.



Note You must use either the **port** option or the **vlan** option with the **interface create** command.

Parameter	Value	Meaning
ip	<InterfaceName>	Name of the IP interface; for example, int4.
address-netmask	<ipAddr-mask>	IP address and netmask of this interface. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the RS uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).

Parameter	Value	Meaning
broadcast	<i><ipAddr></i>	IP address and netmask of this interface. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the RS uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).
peer - address	<i><ipAddr></i>	IP address of the peer for this port. Primarily used for setting up connection with another WAN port or setting up a VC with another ATM port. For WAN and ATM ports only.
vlan	<i><name></i>	Name of the VLAN associated with this interface.
port	<i><port></i>	Port associated with this interface.
mtu	<i><num></i>	Sets the Maximum Transmission Unit (MTU) for this interface.
up		Sets the state of the interface to up. (This is the default state.)
down		Sets the state of the interface to down.
output - mac - encapsulation	<i><MACencap></i>	The output MAC encapsulation associated with this interface.
	ethernet_ii	The default.
	ethernet_snap	

Parameter	Value	Meaning
mac - addr	<i><MACaddr-spec></i>	- Sets the MAC address for this interface. You can specify one of the following: - A specific MAC address – specify the entire MAC address as follows: xx:xx:xx:xx:xx:xx - An offset from the base MAC address in the pool – specify the offset. For example, to specify an offset of 10 from the base MAC address, enter “10”. For example, if the base MAC address is 00:E0:63:02:00:00 and you specify an offset of 10, the RS assigns MAC address 00:E0:63:02:00:0A to the interface. - The base MAC address – specify the basemac keyword. By default the "interface create" command already assigns the router's base MAC address to the newly created interface. This "basemac" option is available only to make the selection explicit. Note that the router has a pool of 64 MAC addresses (base -> base+63). One of these MACs is reserved for the en0 10base-T interface on the CPU module (base+1); IPX by default uses (base+2) as its default MAC address, if you want to use one of the available MAC addresses from the router pool, enter a number (1-61) and the interface MAC will be ((IPXbase)+number). You also have the option to create an arbitrary MAC address. This is the default.
type		Sets the type of interface. Specify one of the following:
	broadcast	The default.
	point-to-point	The default for ATM and PPP.
unnumbered	<i><InterfaceName></i>	An unnumbered interface borrows the IP address from another interface already configured on the RS. Specify the name of the interface from which you are borrowing the IP address.
unnumbered - addr	<i><ipaddr></i>	Identify the IP address to be borrowed if the interface from which the address is being borrowed has more than one address.

Restrictions

For Cisco HDLC WAN ports, the following rules apply:

- The IP address of the local interface and the peer must be in the same subnet.
- If the IP address of the local interface is 1, then the IP address of the peer must be 2, and vice versa.
For example:

local interface address: 123.45.67.1/24

peer address: 123.45.67.2

Examples

To create a VLAN called IP3, add ports et.3.1 through et.3.4 to the VLAN, then create an IP interface on the VLAN:

```
rs(config)# vlan create IP3 ip  
rs(config)# vlan add ports et.3.1-4 to IP3  
rs(config)# interface create ip int3 address-mask 10.20.3.42/24 vlan IP3
```

To create an interface called “int7” with the address 10.50.89.88 and a 16-bit subnet mask, enter the following command. The interface is associated with port et.1.3.

```
rs(config)# interface create ip int7 address-mask 10.50.89.88/16 port et.1.3
```

To create an interface called “int1” with a broadcast address of 10.10.42.255, enter the following command. The interface is associated with the VLAN called “marketing”. The interface is created in the down (disabled) state.

```
rs(config)# interface create ip int1 address-mask 10.10.42.17/255.255.255.0 broadcast 10.10.42.255 vlan marketing down
```

To create an interface on a Cisco HDLC port called “cisco_hdlc”, on subnet 123.45.6.0:

```
rs(config)# interface create ip cisco_hdlc address-netmask 123.45.6.1/24 peer-address 123.45.6.2 port hs.3.2
```


interface create ipx

Mode

Configure

Format

```
interface create ipx <InterfaceName> address <ipxAddr> peer-address [<netaddr>.<macaddr>]
vlan <name> | port <port> [output-mac-encapsulation <MACencap>] [up|down] [mac-addr
<MACaddr-spec>] [mtu <num>]
```

Description

The **interface create ipx** command creates and configures an IPX interface. Configuration of an IPX interface can include information such as the interface's name, IPX address, VLAN, port, and output MAC encapsulation. You can also create an interface in the disabled (down) state instead of the default enabled (up) state.

The RS is pre-allocated a pool of 64 MAC addresses. By default, each new IPX interface is automatically configured with the lowest MAC address in the pool (the "base" MAC address). However, you can assign an interface a different MAC address by using the **mac-addr** option.

Parameter	Value	Meaning
ipx	<InterfaceName>	Name of the IPX interface; for example, int9.
address	<ipxAddr>	IPX address of this interface.
peer - address	<netaddr>.<macaddr>	IPX address of the peer for this port. Primarily used for setting up connection with another WAN port. The peer - address contains the network address, a period (.), then the mac address. This can be illustrated as follows: a1b2c3d4 . aa : bb : cc : dd : ee : ff For WAN ports only.
vlan	<name>	Name of the VLAN associated with this interface.
port	<port>	Port associated with this interface.
output-mac-encapsulation	<MACencap>	The output MAC encapsulation associated with this interface. You can specify one of the following:
	ethernet_ii	The default.
	ethernet_snap	
	ethernet_802.2_ipx	
up		Sets the state of the interface to up. (This is the default state.)
down		Sets the state of the interface to down.

Parameter	Value	Meaning
mac - addr	<i><MACaddr-spec></i>	Sets the MAC address for this interface. You can specify one of the following: - A specific MAC address – specify the entire MAC address as follows: xx:xx:xx:xx:xx:xx - An offset from the base MAC address in the pool – specify the offset. For example, to specify an offset of 10 from the base MAC address, enter “10”. For example, if the base MAC address is 00:E0:63:02:00:00 and you specify an offset of 10, the RS assigns MAC address 00:E0:63:02:00:0A to the interface. - The base MAC address – specify the basemac keyword. By default the interface create command already assigns the RS's base MAC address to the newly created interface. This basemac option is available only to make the selection explicit. Note that the RS has a pool of 64 MAC addresses (base -> base+63). One of these MACs is reserved for the en0 10base-T interface on the CPU module (base+1); IPX by default uses (base+2) as its default MAC address. If you want to use one of the available MAC addresses from the RS pool, enter a number (1-61) and the interface MAC will be (IPXbase)+number. You also have the option to create an arbitrary MAC address. This is the default.
mtu	<i><num></i>	Sets the maximum transmission units in bytes. You can specify any value between 72 and 65535.

Restrictions

None.

Examples

The following commands create a VLAN called IPX10, add all the ports on the line card in slot 1 to the VLAN, and create an IPX interface called “int10” with the IPX address a98d7c6f, associated with VLAN IPX10.

```
rs(config)# vlan create IPX10 ipx
rs(config)# vlan add ports et.1.* to IPX10
rs(config)# interface create ipx int10 address a98d7c6f vlan IPX10
```

The following command creates an interface called “int5” with the IPX address 82af3d57 for port et.1.3. The interface is added in the down (disabled) state.

```
rs(config)# interface create ipx int5 address 82af3d57 port et.1.3 down
```

To create an interface called “int6” with the MAC address 00:01:02:03:04:05 and IPX address 82af3d58 for port et.1.4.

```
rs(config)# interface create ipx int6 address 82af3d58 port et.1.4 mac-addr  
00:01:02:03:04:05
```

To create an interface called “int7” for a VLAN called “IPX-VLAN” on port et.1.4 with the MAC address at the base of the RS’s MAC address pool:

```
rs(config)# interface create ipx int7 address 82af3d59 vlan IPX-VLAN et.1.4 mac-addr  
basemac
```

The following command creates an interface called “int7” for a VLAN called “IPX-VLAN” on port et.1.4 with a MAC address offset by 10 from the base of the RS’s MAC address pool. If the base MAC address in the RS’s MAC address pool is 00:E0:63:02:00:00, the offset of 10 gives the interface the MAC address 00:E0:63:02:00:0A.

```
rs(config)# interface create ipx int7 address 82af3d59 vlan IPX-VLAN et.1.4 mac-addr  
10
```

interface show ip

Mode
Enable

Format

```
interface show ip <InterfaceName> | all [brief]
```

Description

The **interface show ip** command displays configuration information for an IP interface.



Note You can display exactly the same information from within the **ip** facility using the **ip show interfaces** command.

Parameter	Value	Meaning
ip	<InterfaceName> all	Name of the IP interface; for example, int4. Specify all to show configuration information about all the IP interfaces on the RS.
brief		Shows a brief summary of the interface in tabular form.

Restrictions

None.

Examples

To display configuration information for the IP interface called “int7”:

```
rs# interface show ip int7
```

.To display configuration information for all IP interfaces:

```
rs# interface show ip all
```

interface show ipx

Mode

Enable

Format

```
interface show ipx <InterfaceName> | all [brief]
```

Description

The **interface show ipx** command displays configuration information for an IPX interface.



Note

You can display exactly the same information from within the **ip** facility using the **ipx show interfaces** command.

Parameter	Value	Meaning
ipx	<i><InterfaceName></i> all	Name of the IPX interface; for example, int9. Specify all to show configuration information about all the IPX interfaces on the RS.
brief		Shows a brief summary of the interface in tabular form.

Restrictions

None.

Examples

To display configuration information for the IPX interface called “int8”:

```
rs# interface show ipx int8
```

To display configuration information for all IPX interfaces:

```
rs# interface show ipx all
```


28 IP COMMANDS

The **ip** commands let you display route table entries and various IP related tables.

28.1 COMMAND SUMMARY

The following table lists the ip commands. The sections following the table describe the command syntax for each command.

<code>ip add route <ipAddr-mask> default gateway <hostname-or-IPAddr> [host] [interface <hostname-or-IPAddr>] [preference <num>] [retain] [reject] [no-install] [blackhole] [gate-list <gateway list>] [ping-interval <num>] [ping-retries <num>] [intf-list <ipaddr-list>] [monitor-gateways]</code>
<code>ip apply custom-forwarding-mode <string> slot <number></code>
<code>ip bgp-accounting start accounting dscp_accounting</code>
<code>ip clear bgp-actg</code>
<code>ip clear reverse-flows</code>
<code>ip community-list <identifier> deny permit <community-string></code>
<code>ip define custom-forwarding-profile <string> sip-host-wildcard dip-host-wildcard proto-wildcard dst-sock-wildcard src-sock-wildcard tos-wildcard</code>
<code>ip disable dns-lookup fast-icmp forwarding icmp-redirect interface <name> all proxy-arp interface <name> all source-routing icmp-message echo-reply timestamp-reply time-exceeded destination-unreachables default-route-check</code>
<code>ip disable webcache-actg</code>
<code>ip dos disable port-attack-protection directed-broadcast-protection</code>
<code>ip dos enable fragments-attack-protect</code>
<code>ip dos rate-limit [icmp <num> default disable] [bgp <num> disable] [ospf <num> disable] [rip <num> disable] [vrrp <num> default disable] [ldp-hello <num> disable] [ldp-session <num> disable] [rsvp <num> disable]</code>
<code>ip enable bgp-actg-on <interface list> all</code>
<code>ip enable custom-forwarding-mode port <port-list></code>
<code>ip enable directed-broadcast interface <interface name> all</code>
<code>ip enable reverse-flow {all policy NAT load-balance normal}</code>

ip enable reverse-path-forwarding interface <name>
ip helper-address interface <interface-name> <helper-address> all-interfaces [<udp-port#>]
ip-l3-deep-hashing module <num> all set on
ip l3-hash module <num> all variant <num>
ip set data-receive-size <num> control-receive-size <num>
ip set multipath-hash-variant <num> disable
ip set port <port-list> forwarding-mode [destination-based host-flow-based]
ip show community-list <list-number>
ip show connections [no-lookup]
ip show custom-forwarding-mode slot <number> all
ip show custom-forwarding-profile <string> all
ip show dos rate-limit
ip show hash-variant <num> all
ip show helper-address
ip show interfaces [<interface-name>] [brief]
ip show mode port <port-list>
ip show reverse-flows
ip show routes [show-protocol aggregate direct default ospf ospf-ase rip bgp static isis-level-1 isis-level-2] [show-arp] [show-multicast] [show-summary] [verbose]
ip show stack-queues

ip add route

Mode

Configure

Format

```
ip add route <ipAddr-mask>|default gateway <hostname-or-IPaddr> [host] [interface
<hostname-or-IPaddr>] [preference <num>] [retain] [reject] [no-install] [blackhole]
[monitor-gateways ] [gate-list <gateway list>] [intf-list <IPaddr list>] [ping-interval <sec>]
[ping-retries <retries>]
```

Description

The **ip add route** command creates a static route entry in the route table. The static route can be a default route, a route to a network, or a route to a specific host.



Note If route-type is either **blackhole** or **reject**, a gateway does not need to be specified.

Parameter	Value	Meaning
route	<ipAddr-mask>	IP address and netmask of the destination. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the RS uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).
gateway	<hostname-or-IPaddr>	IP address or hostname of the next hop router for this route.
host		Specifies that this route is a route to a host.
interface	<hostname-or-IPaddr>	The next hop interface associated with this route. When this option is specified, gateways are only considered valid when they are on one of these interfaces.
preference		The preference of this static route. The preference controls how this route competes with routes from other protocols. The parameter takes a value between 0-255. The default preference is 60.
retain	<num>	If specified, this option prevents this static route from being removed from the forwarding table when the routing service (ROSRD) is gracefully shutdown. Normally ROSRD removes all routes except interface routes during a graceful shutdown. The retain option can be used to insure that some routing is available even when ROSRD is not running.

Parameter	Value	Meaning
reject		If specified, install this route as a reject route. Instead of forwarding a packet like a normal route, reject routes cause packets to be dropped and unreachable messages to be sent to the originator of the packet.
no-install		If specified, the route will not be installed in the forwarding table when it is active but will be eligible for exporting to other protocols.
blackhole		This option is the same as the reject option with the exception that unreachable messages are not sent.
intf-list	<IPaddr list>	Allows you to specify the next-hop interfaces associated with the route. When this option is specified, the gateways are only considered valid when they are on one of these interfaces. This option cannot be used with the gateway or the interface options. Specify one or more IP addresses separated by spaces and enclosed in quotation marks.
monitor-gateways		If specified, monitor gateways and remove the route entry when the next hop gateway is down. The gate-list parameter must also be specified.
gate-list	<gateway list>	Allows you to specify up to four gateways for a particular destination host or network.
ping-interval	<sec>	The number of seconds between pings that are sent to monitor gateways. The default is 5 seconds. Specify a value between 1-255.
ping-retries	<retries>	The number of retries to ping a gateway before the gateway is considered “down.” The default is 4 times. Specify a value between 1-255.

Restrictions

None

Examples

To configure the router 10.4.1.1 as the default gateway for this RS:

```
rs(config)# ip add route default gateway 10.4.1.1
```

To configure the gateway 10.4.78.11 as the gateway for any packet destined for the subnet 10.4.14.0/24:

```
rs(config)# ip add route 10.4.14.0/24 gateway 10.4.78.11
```

To configure the gateway 10.4.78.11 as the gateway for any packet destined for the subnet 10.4.14.0/24:

```
rs(config)# ip add route 10.4.14.0/24 gateway 10.4.78.11
```

To configure the gateway 10.4.16.99 as the gateway to the host 10.4.15.2:

```
rs(config)# ip add route 10.4.15.2 host gateway 10.4.16.99
```

To configure a reject route entry for packets destined for the subnet 10.14.3.0/24:

```
rs(config)# ip add route 10.14.3.0/24 gateway 10.1.16.99 reject
```

ip apply custom-forwarding-mode

Mode
Configure

Format

ip apply custom-forwarding-mode <string> slot <number>

Description

Once a custom forwarding profile is created, it can be applied to a slot. This command is used to apply a custom forwarding profile to a slot. This means that all the ports in the channel will use this profile for flow lookup.

**Note** A slot is a logical set of ports. The maximum number of ports in a slot is 16.

Parameter	Value	Meaning
custom-forwarding-mode	<string>	This is an alphanumeric character string typed in by the user. Use it to name the custom profile that you want to apply.
slot	<number>	This is the number of the slot you want to apply the custom profile. Specify a number between 1 and 16.

Restrictions

None.

Examples

To apply the profile officePoolA to slot 1:

```
ip apply custom-forwarding-mode officePoolA 1
```

ip bgp-accounting

Mode

Configure

Format

```
ip bgp-accounting start accounting|dscp-accounting
```

Description

The **ip bgp-accounting start** command starts the collection of BGP traffic information on the RS. To use BGP accounting, assign traffic buckets to the traffic of a particular customer with the **set-traffic-index** option of the **route-map** command. Enable BGP accounting on the specified interface(s) (or on all interfaces) with the **ip enable bgp-actg-on** command. See the *Riverstone Networks RS Switch Router User Guide* for configuration examples.

You can specify one of two modes of traffic information collection: collecting information on all BGP traffic or collecting information about traffic according to DSCP values in packets. While you can use the **ip bgp-accounting start** command to change the mode of traffic information collection, note the following:

- If you change from DSCP accounting to “regular” BGP accounting, all traffic counters are aggregated to their respective traffic indexes. For example, with DSCP accounting, packets for traffic index ‘10’ for DSCP values 4, 5, and 6 are counted separately. If you then change to “regular” BGP accounting, the packets for traffic index 10 are aggregated.
- If you change from “regular” BGP accounting to DSCP accounting, all traffic counters are reset to zero.

Parameter	Value	Meaning
start		Starts BGP accounting.
	accounting	Starts collection of BGP traffic information.
	dscp-accounting	Starts collection of BGP traffic information according to Differentiated Services Code Point (DSCP),formerly known as Type of Service (ToS), values. Note If you specify the dscp-accounting parameter, only packets with DSCP values between 0-63 are counted. Packets with DSCP values less than 0 or greater than 63 are not counted.

Restrictions

None

Example

To enable and start BGP accounting on interfaces int1, int2, and int3:

```
rs(config)# ip enable bgp-actg-on int1,int2,int3
rs(config)# ip bgp-accounting start accounting
```

ip clear bgp-actg

Mode

Enable

Format

ip clear bgp-actg

Description

The **ip clear bgp-actg** command deletes all BGP accounting statistics. BGP accounting allows you to collect statistics according to route-specific traffic.

Parameter	Value	Meaning
clear	bgp-actg	Clears all BGP accounts.

Restrictions

None

Example

To clear BGP accounting statistics:

```
rs# ip clear bgp-actg
```

ip clear reverse-flows

Mode

Enable

Format

```
ip clear reverse-flows
```

Description

The **ip clear reverse-flows** command deletes all reverse flow statistics. Reverse flows are IP traffic flows in the opposite direction, where source information becomes destination information and vice versa.

Restrictions

None

Example

To clear the reverse flow statistics:

```
rs# ip clear reverse-flows
```


ip community-list

Mode

Configure

Format

```
ip community-list <identifier> deny|permit <community-string>
```

Description

The **ip community-list** command rejects or allows a community to a community list.

Parameter	Value	Meaning
community-list	<identifier>	Specifies the identifier of the community list.
deny permit	<community-string>	Quoted string of communities like "a:b c:d" where a,c are the AS portion of a community split and b,d are the community identifier portion of a community split.

Restrictions

None

ip define custom-forwarding-profile

Mode

Configure

Format

```
ip define custom-forwarding-profile <string> sip-host-wildcard | dip-host-wildcard |  
proto-wilcard |dst-sock-wildcard |src-sock-wildcard | tos-wildcard
```

Description

A custom forwarding profile is a user-defined list of wildcard flow lookup fields. Wildcard fields are those fields of a packet that are to be used for custom forwarding flow lookup. There are six fields:

- SIP (Source IP Address)
- DIP (Destination IP Address)
- Protocol
- Source Socket
- Destination Socket
- TOS (Type of Service)

One or more fields up to all can be chosen for each profile. One profile is assigned to one port. See **ip show custom-forwarding-profile** for an example of a profile.

Parameter	Value	Meaning
custom-forwarding-profile	<string>	This is a alphanumeric character string typed in by the user. Use it to name the custom profile. The maximum character string length is 256.
sip-host-wildcard		This will set the source IP address field as a wildcard.
dip-host-wildcard		This will set the destination IP address field as a wildcard.
proto-wilcard		This will set the protocol field as a wildcard.
dst-sock-wildcard		This will set the destination socket field as a wildcard.
src-sock-wildcard		This will set the source socket field as a wildcard.
tos-wildcard		This will set the type of service field as a wildcard.

Restrictions

TOS wildcarding will not work with the following boards: G8M-HTXB2-16 (for RS 8000 and RS 8600 systems), G3M-HTXB2-16 (for RS 3000 systems), and R32-HTXC2-24 and R32-HTXC3-32 (for RS 32000 systems).

Examples

To define a profile with all wildcards:

```
ip define custom-forwarding-profile officePoolA sip-host-wildcard |  
dip-host-wildcard | proto-wilcard |dst-sock-wildcard |src-sock-wildcard  
| tos-wildcard
```

To define a profile with select wildcards:

```
ip define custom-forwarding-profile officePoolB sip-host-wildcard |  
tos-wildcard
```

ip disable

Mode

Configure

Format

```
ip disable dns-lookup|fast-icmp|forwarding {icmp-redirect interface
<name>|all|proxy-arp interface <name>|all| source-routing|icmp-message echo-reply
timestamp-reply time-exceeded destination-unreachables|default-route-check
```

Description

The **ip disable** command allows you to disable features that are enabled by default on the RS.

Parameter	Value	Meaning
dns-lookup		Disables DNS name lookup for all commands. Sometimes a DNS server is too slow to respond and this can cause a command that displays information about many hosts to take a long time to finish. Disabling DNS lookup displays all host addresses as IP addresses instead of host names.
fast-icmp		Disables the fast ICMP feature on the RS. By default, the RS installs ICMP flows to be switched along the fast path in hardware if the ICMP flow is meant to be routed. ICMP echo requests are installed as control priority for packets destined for the RS. When this feature is disabled, all ICMP packets are handled via the slow path in software.
forwarding		Disables the router's ability to forward IP packets. No IP packets will be forwarded to any IP interface if this command is used.
icmp-redirect interface	<interface name> all	Disables ICMP redirection on the specified IP interface. If you specify the all keyword, ICMP redirection is disabled for all network interfaces.
proxy-arp interface	<name> all	Disables the proxy ARP feature on the specified IP interface. By default, the RS acts as a proxy for ARP requests with destination addresses of hosts to which the RS can route traffic. Unless you actually require the use of proxy ARP, it is advisable to disable it on the RS. If you specify the all keyword, the proxy ARP feature is disabled for all network interfaces.
source-routing		Causes the RS to drop packets that have the SOURCE_ROUTE option set in the IP header. By default, packets that have the SOURCE_ROUTE option set are forwarded using the next-hop address in the IP packet.

Parameter	Value	Meaning
icmp-message		Disables the ability to send out ICMP messages. ICMP messages are used to communicate errors in packet traffic to other routers. You can disable the following ICMP response messages: echo-reply, timestamp-reply, time-exceeded, and destination-unreachables:
	echo-reply	
	timestamp-reply	
	time-exceeded	
	destination-unreachables	
default-route-check		Allows a default route to be set through the management (en0) interface.

Restrictions

None

Examples

To disable ICMP redirection on the “int4” network interface:

```
rs(config)# ip disable icmp-redirect int4
```

To disable DNS name lookup for all commands:

```
rs(config)# ip disable icmp-redirect dns-lookup
```

To prevent the RS from acting as a proxy for ARP requests with destination addresses of hosts to which the RS can route traffic:

```
rs(config)# ip disable proxy-arp interface all
```

ip disable webcache-actg

Mode

Configure

Format

```
ip disable webcache-actg
```

Description

The `ip disable webcache-actg` command disables the collection of web cache statistics.

Restrictions

None.

ip dos disable

Mode

Configure

Format

```
ip dos disable directed-broadcast-protection|port-attack-protection
```

Description

This command disables denial of service (DOS) features on the RS. By default, the RS installs flows in the hardware so that packets sent as directed broadcasts are dropped in hardware if directed broadcast is not enabled on the interface where the packet is received. You can disable this behavior with the

ip dos disable directed-broadcast-protection command.

Similarly, the RS installs flows to drop packets destined for the RS for which service is not provided by the RS. This prevents packets for unknown services from slowing the CPU. You can disable this behavior with the

ip dos disable port-attack-protection command, causing these packets to be processed by the CPU.

Parameter	Value	Meaning
disable	directed-broadcast-protection	Disables the directed-broadcast-protection feature of the RS. By default the RS drops packets sent as directed broadcasts if directed broadcast is not enabled on the interface where the packet is recieved. This command causes directed broadcast packets to be processed on the RS even if directed broadcast is not enabled on the interface receiving the packet.
	port-attack-protection	Disables the port-attack-protection feature of the RS. By default, packets that are destined for the RS, but do not have a service defined for them on the RS, are dropped. This prevents packets for unknown services from slowing the RS's CPU. This command disables this behavior, allowing packets destined for the RS that do not have a service defined for them on the RS to be processed by the RS's CPU.

Restrictions

None

Examples

To cause directed broadcast packets to be processed on the RS, even if directed broadcast is not enabled on the interface receiving the packet:

```
rs(config)# ip dos disable directed-broadcast-protection
```

To allow packets destined for the RS, but do not have a service defined for them on the RS, to be processed by the RS's CPU:

```
rs(config)# ip dos disable port-attack-protection
```


ip dos enable

Mode

Configure

Format

```
ip dos enable fragments-attack-protect
```

Description

The **ip dos enable** command allows you to enable Denial of Service features to protect the RS from attacks from unknown sources.

IP fragmentation attacks target packet filters, since these filters denies access based upon IP packet information. All IP fragments do not contain all specific information to filter upon, thus allowing a possible security risk. Enabling fragment attack protection should resolve this risk.

Parameter	Value	Meaning
enable	fragments-attack-protect	Enables the Denial of Service feature to prevent attacks from IP fragments.

Restrictions

None

Examples

To enable protection against IP fragment attacks on the RS:

```
rs(config)# ip dos enable fragments-attack-protect
```

ip dos rate-limit

Mode

Configure

Format

```
ip dos rate-limit [icmp <num> | default | disable] [[bgp <num> | disable] [[ospf <num> | disable]
|[rip <num> | disable] [vrrp <num> | default | disable] [ldp-hello <num> | disable] [ldp-session
<num> | disable] [rsvp <num> | disable]
```

Description

The **ip dos rate-limit** command allows you to rate limit certain types of traffic to help prevent Denial of Service attacks. The traffic types are ICMP, BGP, OSPF, RIP, VRRP, LDP and RSVP.

Parameter	Value	Meaning
icmp	<num>	<num> is the rate limit in bps. The range of values for this field is 25000 to 5000000. This value is required
	default	Specify default to rate limit at the default rate, 25000.
	disable	Specify disable to disable ICMP rate limiting.
bgp	<num>	<num> is the rate limit in bps. The range of values for this field is 128000 to 5000000. The default is no rate limiting.
	disable	Specify disable to disable BGP rate limiting.
ospf	<num>	<num> is the rate limit in bps. The range of values for this field is 128000 to 5000000. The default is no rate limiting.
	disable	Specify disable to disable OSPF rate limiting.
rip	<num>	<num> is the rate limit in bps. The range of values for this field is 50000 to 5000000.
	disable	Specify disable to disable BGP rate limiting. The default is no rate limiting.
vrrp	<num>	<num> is the rate limit in bps. The range of values for this field is 25000 to 5000000.
	default	Specify default to rate limit at the default rate, 25000.
	disable	Specify disable to disable ICMP rate limiting.
ldp-hello	<num>	<num> is the rate limit in bps. The range of values for this field is 128000 to 5000000.
	disable	Specify disable to disable LDP hello (UDP) rate limiting.

Parameter	Value	Meaning
ldp-session	<num>	<num> is the rate limit in bps. The range of values for this field is 128000 to 5000000.
	disable	Specify disable to disable LDP session (TCP) rate limiting.
rsvp	<num>	<num> is the rate limit in bps. The range of values for this field is 128000 to 5000000.
	disable	Specify disable to disable RSVP rate limiting.

Restrictions

None.

Examples

To rate limit ICMP traffic:

```
rs(config)# ip dos rate-limit icmp 4000000
```

ip enable bgp-actg-on

Mode

Configure

Format

```
ip enable bgp-actg-on <interface list>|all
```

Description

This command is used to configure the router to perform BGP accounting on one or more interfaces. BGP accounting can be used to track BGP traffic. For example, if you are an ISP, you can use BGP accounting to assess the BGP resource usage by a particular customer. To use BGP accounting, assign traffic buckets to the traffic of a particular customer with the **set-traffic-index** option of the **route-map** command. After you enable BGP accounting on the specified interface(s), start the collecting of information with the **ip bgp-accounting start** command.

Parameter	Value	Meaning
bgp-actg-on	<interface list> all	This is a comma-separated list of interface names on which BGP accounting will be enabled. If you specify the all keyword, BGP accounting is enabled for all network interfaces except loopback and the management interfaces

Restrictions

None.

Examples

To enable BGP accounting on interfaces int1, int2, and int3:

```
rs(config)# ip enable bgp-actg-on int1, int2, int3
```

ip enable custom-forwarding-mode

Mode

Configure

Format

```
ip enable custom-forwarding-mode port <port-list>
```

Description

This command is used to enable custom forwarding on one or more ports in a slot.

Parameter	Value	Meaning
port	<port-list>	This is an alphanumeric character string typed in by the user. Use it to enable ports with custom forwarding The maximum number of names is defined by the card you are addressing.

Restrictions

None.

Examples

To enable four ports:

```
ip enable custom-forwarding-mode port gi.1.2,
```

ip enable directed-broadcast

Mode

Configure

Format

```
ip enable directed-broadcast interface <interface name>|all
```

Description

Directed broadcast packets are network or subnet broadcast packets which are sent to a router to be forwarded as broadcast packets. They can be misused to create Denial Of Service attacks. The RS protects against this possibility by **not** forwarding directed broadcasts, by default. To enable the forwarding of directed broadcasts, use the **ip enable directed-broadcast** command.

Parameter	Value	Meaning
interface	<interface name>	This is the name of the specified IP interface.
	all	If you specify the all keyword, directed broadcast forwarding is enabled for all network interfaces.

Restrictions

None

Examples

To enable directed broadcast forwarding on the “int4” network interface:

```
rs(config)# ip enable directed-broadcast interface int4
```

To enable directed broadcast forwarding for all network interfaces:

```
rs(config)# ip enable directed-broadcast interface all
```

ip enable reverse-flow

Mode

Enable

Format

```
ip enable reverse-flow {all|policy|NAT|load-balance|normal}
```

Description

This command allows you to set up reverse flows. Reverse flows in this case are Layer-3 flows heading in the opposite direction to the corresponding IP flows. IP flows are defined by the source and destination IP addresses, source and destination TCP/UDP port, Type of Service and transport protocol.

Parameter	Value	Meaning
reverse-flow	all policy NAT load-balance normal	Enables the ability to set up reverse flows. Specify all to enable any type of reverse flow to be set up. Specify policy to enable setting up reverse flows for policy routed packets. Specify NAT to enable setting up reverse flows for NAT packets. Specify load-balance to enable setting up reverse flows for load balance packets. Specify normal to enable setting up reverse flows for normally routed packets.

Restrictions

None.

Examples

To enable reverse flows for policy routed packets:

```
rs(config)# ip enable reverse-flow policy
```

ip enable reverse-path-forwarding

Mode

Configure

Format

```
ip enable reverse-path-forwarding interface <port-list>
```

Description

When reverse path forwarding is enabled on an interface, the router examines the unicast packets received on that interface. It verifies whether the incoming interface and the IP interface it would use to send packets to the source address match. Only packets that match this criterion are forwarded. Other packets are dropped.

Parameter	Value	Meaning
interface	<name>	Specifies the name of the interface on which reverse path forwarding is enabled.

Restrictions

None.

Examples

To enable reverse path forwarding on the “int2” interface:

```
rs(config)# ip enable reverse-path-forwarding interface int2
```


ip helper-address

Mode

Configure

Format

```
ip helper-address interface <interface-name> <helper-address>|all-interfaces [<udp-port#>]
```

Description

The **ip helper-address** command allows the user to forward specific UDP broadcast from one interface to another. Typically, broadcast packets from one interface are not forwarded (routed) to another interface. However, some applications use UDP broadcast to detect the availability of a service. Other services, for example BOOTP/DHCP require broadcast packets to be routed so that they can provide services to clients on another subnet. An IP helper can be configured on each interface to have UDP broadcast packets forwarded to a specific host for a specific service or forwarded to all other interfaces.

The **ip helper-address** command allows the user to specify a UDP port number for which UDP broadcast packets with that destination port number will be forwarded. By default, if no UDP port number is specified, the RS will forward UDP broadcast packets for the following six services:

- BOOTP/DHCP (port 67 and 68)
- DNS (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Parameter	Value	Meaning
interface	<interface-name>	Name of the IP interface where UDP broadcast is to be forwarded to the helper address.
	<helper-address> all-interfaces	Address of the host where UDP broadcast packets should be forwarded. If all-interfaces is specified, UDP broadcast packets are forwarded to all interfaces except the interface on which the broadcast packet was received.
	<udp-port>	Destination UDP port number of the broadcast packets to forward. If not specified, packets for the six default services will be forwarded to the helper address.

Restrictions

If you specify an interface name, the name must belong to an existing IP interface.

Examples

To forward UDP broadcast packets received on interface int1 to the host 10.1.4.5 for the six default UDP services:

```
rs(config)# ip helper-address interface int1 10.1.4.5
```

To forward UDP broadcast packets received on interface int2 to the host 10.2.48.8 for packets with the destination port 111 (port mapper):

```
rs(config)# ip helper-address interface int2 10.2.48.8 111
```

To forward UDP broadcast packets received on interface int3 to all other interfaces:

```
rs(config)# ip helper-address interface int3 all-interfaces
```

ip l3-deep-hashing

Mode

Configure

Format

```
ip l3-deep-hashing module <num>|all set on
```

Description

Use the **ip l3-deep-hashing** command to enable or disable deep hashing on a specified module.

Deep hashing allows for more than four hash buckets (levels within a particular entry for a hash value) within an entry in the L3 lookup table. Although hashing should cause a more even distribution across the lookup table, there is still a possibility that more than four flows may end up at a particular entry in the lookup table.

Allowing for more than four entries through deep hashing will prevent thrashing, but may cause less-than-wirespeed performance due to the extra amount of entries. This is because thrashing will reduce performance to a greater extent than deep hashing. But although deep hashing may result in less-than-wirespeed performance, it still performs much better than if it were thrashing.

Parameter	Value	Meaning
module	<num> all	Is a slot number on the RS. Specify any number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot. The all option causes the hashing algorithm to change on all ports on all slots.
set	on	Enables deep hashing on the module. Negate this command from active configuration to disable l3 deep hashing.

Restrictions

None.

Example

To enable deep hashing on slot 7:

```
rs(config)# ip l3-deep-hashing module 7 set on
```

ip l3-hash

Mode

Configure

Format

ip l3-hash module <num>|all variant <num>

Description

The RS’s L3 Lookup table is organized as a hash table. The hash function reduces the destination and source MAC addresses to 16-bit quantities each. The hashing algorithm generates a uniform distribution within the MAC address space. However, given a particular set of addresses, the distribution may cause addresses to clump together in the table. To minimize the risk of thrashing in the tables, three variations to the basic hashing algorithm are defined. Only one variation is in effect on a line card at any given time. You can use the **ip l3-hash** command to set which variation is in effect for a line card.

Swizzling shifts the hash value by a certain amount of bits, producing more random distribution across the L3 lookup table.

Auto-hashing periodically queries the L2 or L3 tables for hash bucket overflow on a port. If there are more overflows than a certain threshold level, auto-hashing will automatically change the hash mode for that port. Eventually a ‘best’ hash mode for the particular traffic will be found, which will provide a more even distribution across the L2 or L3 lookup table.

To see the effect changing the hashing algorithm has on the hash bucket, use the **statistics show l3-stat** command in the RS’s Diag mode.

Parameter	Value	Meaning
module	<num> all	Is a slot number on the RS. Specify any number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot. The all option causes the hashing algorithm to change on all ports on all slits.
variant	<num>	Causes a variation to the basic hashing algorithm to be made. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). If you specify 0, the default hashing algorithm is used.

Restrictions

None.

Example

To change the default hashing algorithm used for the L3 lookup table on all ports on slot 7:

```
rs(config)# ip l3-hash module 7 variant 1
```

ip set data-receive-size | control-receive-size

Mode

Configure

Format

```
ip set data-receive-size <num> | control-receive-size <num>
```

Description

The **ip set data-receive-size | control-receive-size** command allows you to tune the size of the stack data and control receive queues that reside between the IP stack and internal drivers on the Control Module.

Parameter	Value	Meaning
data-receive-size	<num>	Sets the size of the stack data receive queue. Specify a value from 256-1024 bytes. The default is 512 bytes.
control-receive-size	<num>	Sets the size of the stack control receive queue. Specify a value from 256-1024 bytes. The default is 512 bytes.

Restrictions

None.

Example

To set the size of the stack data receive queue to 1024 bytes:

```
rs(config)# ip set data-receive-size 1024
```

ip set multipath-hash-variant

Mode

Configure

Format

```
ip set multipath-hash-variant <num>| disable
```

Description

When there are multiple paths to a destination, the RS selects the route to use in a round-robin manner. Use the **ip set multipath-hash-variant** command to select a route when there are multiple paths to a destination. To select the route, the RS uses a hash function based on the source and destination IP address.

Parameter	Value	Meaning
multipath-hash-variant	<num>	Specify the hash variant to use for selecting the route. Enter a number between 1 and 4, inclusive.
	disable	Disables multipath forwarding using hash variants. Instead, routes are selected in a round-robin manner.

Restrictions

None.

Example

The following example sets the multipath-hash variant to 2:

```
rs(config)# ip set multipath-hash-variant 2
```

ip set port forwarding-mode

Mode

Configure

Format

```
ip set port <port-list> forwarding-mode destination-based|host-flow-based
```

Description

The RS's flow identifying logic normally extracts the complete application (layer-4) flow from an IP packet. The **ip set port forwarding-mode** command causes the RS to extract only certain flow-related fields from the packet's L3 header, rather than the full layer-4 flow. This allows ports to route packets based on destination address alone, or on destination and source address only. As a result, in environments that do not have any filtering or RSVP requirements, the flow table can be used much more efficiently.

Parameter	Value	Meaning
port	<port-list>	Modifies the flow extraction behavior on the specified ports. All ports must have an IP interface configured for them.
destination-based		If the packet is a unicast packet, causes the <i>destination IP address</i>, <i>TOS</i> and <i>L4 protocol</i> fields to be the only fields extracted from the IP packet. These fields and the <i>port of entry</i> field are set into the flow block being constructed. All of the other fields are set to zero. For L3 multicast packets, the <i>destination IP address</i>, <i>source IP address</i>, <i>TOS</i> and <i>L4 protocol</i> fields are the only fields extracted from the IP packet. These along with the <i>port of entry</i> are the only fields set in the flow block. The remaining fields are set to zero. The flow lookup then proceeds as normal.
host-flow-based		For both unicast and multicast packets, the <i>destination IP address</i> , <i>source IP address</i> , <i>TOS</i> and the <i>L4 protocol</i> are the only fields extracted from the IP packet. These along with the <i>port of entry</i> are set in the flow block. The remaining flow block fields are set to zero. The flow lookup then proceeds as normal.

Restrictions

None

Example

To cause the RS to extract only the *destination IP address*, *TOS*, and *L4 protocol* fields from a layer-4 flow when processing an IP packet on port et.1.1:

```
rs(config)# ip set port et.1.1 forwarding-mode destination-based
```

To cause the RS to extract only the *destination IP address*, *source IP address*, *TOS*, and *L4 protocol* type from a layer-4 flow when processing an IP packet on port et.1.1:

```
rs(config)# ip set port et.1.1 forwarding-mode host-flow-based
```


ip show community-list

Mode

Enable

Format

ip show community-list <list-number>

Description

The **ip show community-list** command displays the community list.

Parameter	Value	Meaning
community-list	<list-number>	The community list number. Specify a value between 1-99.

Restrictions

None.

ip show connections

Mode

Enable

Format

```
ip show connections [no-lookup]
```

Description

The **ip show connections** command displays all existing TCP and UDP connections to the RS as well as TCP/UDP services available on the RS.

Parameter	Value	Meaning
no-lookup		By default, when displaying an IP address, this command attempts to do a reverse DNS lookup to look for the hostname associated with the IP address and display the hostname instead. If you do not want the reverse DNS lookup to occur, specify the no-lookup option.

Restrictions

None.

Example

The following example displays all established connections and services of the RS.

```
rs# ip show connections
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp        0      0 *:rosrd-gii            *:.*                     LISTEN
tcp        0      0 *:http                  *:.*                     LISTEN
tcp        0      0 *:telnet                 *:.*                     LISTEN
udp        0      0 127.0.0.1:1025          127.0.0.1:162
udp        0      0 *:snmp                   *:.*
udp        0      0 *:snmp-trap             *:.*
udp        0      0 *:bootp-relay           *:.*
udp        0      0 *:route                  *:.*
udp        0      0 *:.*                     *:.*
```

ip show custom-forwarding-mode

Mode

Enable

Format

```
ip show custom-forwarding-mode slot <number> | all
```

Description

This command is used to display the custom forwarding profile applied to a slot or slots.

Parameter	Value	Meaning
slot	<number>	This is a numeric character string typed in by the user. Use it to identify the slot. Specify a number between 1 and 16.
	all	Use this keyword to display all the profiles on all of the slots. <number> and all are mutually exclusive. You can not use both within the same command. If you type in a <number> followed by all , the CLI will only recognize the <number> command.

Restrictions

None.

Examples

To display a single slot:

```
ip show custom-forwarding-mode slot 2
```

To display all slots:

```
ip show custom-forwarding-mode slot all
```

ip show custom-forwarding-profile

Mode
Enable

Format

```
ip show custom-forwarding-profile <string> | all
```

Description

This command is used to display the parameters of one or more custom forwarding profiles. Following is an example of a profile:

```
protocol wilddarding is disabled
sip wilddarding is enabled
dip wilddarding is disabled
dest socket wilddarding is disabled
dest socket wilddarding is disabled
TOS wilddarding is disabled
```

Parameter	Value	Meaning
custom-forwarding-profile	<string>	This is a alphanumeric character string typed in by the user. Use it to name the custom profile that you want to display. The maximum character string length is 256.
	all	Use this keyword to display all of the custom profiles. <string> and all are mutually exclusive. You can not use both within the same command. If you type in a <string> followed by all , the CLI will only see the <string> command as valid.

Restrictions

None.

Examples

To display a single profile:

```
ip show custom-forwarding-profile officially
```

To display all profiles:

```
ip show custom-forwarding-profile all
```

ip show dos rate-limit

Mode

Enable

Format

```
ip show dos rate-limit
```

Description

This command is used to display Denial of Service rate limiting.

Parameter	Value	Meaning
rate-limit		Displays the IP DoS rate limits.

Restrictions

None.

Examples

To display all the IP DoS rate limits:

```
rs2100# ip show dos rate-limit
Summary of IP dos configuration
-----
  ICMP traffic is rate limited to 25000 bps
  BGP traffic is not rate limited
  OSPF traffic is not rate limited
  RIP traffic is rate limited to 4000000 bps
  VRRP traffic is rate limited to 25000 bps
rs2100#
```

ip show hash-variant

Mode

Enable

Format

```
ip show hash-variant <num>|all
```

Description

The **ip show hash-variant** command displays hash variant information. There are a total of 16 modules using the hash variant feature (1-16).

Enabling hash variant causes a variation to the basic hashing algorithm. This variation will prevent clustering of hash values and will provide a more even distribution across the L3 lookup table. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). The default hashing algorithm is 0.

Swizzling shifts the hash value by a certain amount of bits, causing a more random distribution across the L3 lookup table. Auto-hashing allows the RS to auto-select a hashing algorithm optimized for 'best case' L3 table distribution.

Parameter	Value	Meaning
hash-variant	<num> all	Specifies the module. Specify any number between 1-16. Specify all to display hash variant information for all modules.

Restrictions

None.

Example

To display IP hash variant information on all 16 modules:

```
rs# ip show hash-variant all
```

IP Module	Hash Variant

Module 2	variant-0
Module 3	variant-0
Module 4	variant-0
Module 5	variant-1
Module 6	variant-0
Module 7	variant-0
Module 8	variant-2
Module 9	variant-0
Module 10	variant-7
Module 11	variant-0
Module 12	variant-6
Module 13	variant-0
Module 14	variant-0
Module 15	variant-0

ip show helper-address

Mode

Enable

Format

```
ip show helper-address [<interface-name>]
```

Description

The **ip show helper-address** command displays the configuration of IP helper addresses configured on the system. One can specify the optional parameter, *<interface-name>*, to show only the IP helper addresses configured for that interface. If the command is executed without specifying an interface name then the IP helper address configuration of all interfaces are shown.

Parameter	Value	Meaning
helper-address	<i><interface-name></i>	Name of the IP interface to display any configured IP helper addresses.

Restrictions

If you specify an interface name, the name must belong to an existing IP interface.

Example

The following example shows that interface int4 has one helper address configured while interface int3 has one helper address configured for the port mapper service (port 111).

rs# ip show helper-address		
Interface	IP address	Helper Address
-----	-----	-----
int6	10.1.17.1	none
int5	10.1.16.1	none
int4	10.1.15.1	10.4.1.45
int1	10.1.12.1	none
int0	10.1.11.1	none
int3	10.1.14.1	10.5.78.122(111)

ip show mode

Mode

Enable

Format

ip show mode <port-list>

Description

The **ip show mode** command displays the layer-3 mode for a port.

Parameter	Value	Meaning
mode	<port-list>	Specifies the port to display.

Restrictions

None.

Example

The following example displays the l3 mode for port et.2.1:

```
rs# ip show mode port et.2.1
Port      Mode
----      -
et.2.1    Flow(Default)
```

ip show interfaces

Mode

Enable

Format

```
ip show interfaces [<interface-name>] [brief]
```

Description

The **ip show interfaces** command displays the configuration of an IP interface. If you issue the command without specifying an interface name then the configuration of all IP interfaces is displayed. This command displays the same information as the **interface show ip** command.

Parameter	Value	Meaning
interfaces	<interface-name>	Name of the IP interface; for example, rs4. If you do not specify an interface name, the RS displays all the IP interfaces.
brief		Shows a brief summary of the interface in tabular form.

Restrictions

If you specify an interface name, the name must belong to an existing IP interface.

Example

To display the configuration of the IP interface “int1”:

```
rs# ip show interfaces int1
int1: flags=9862<BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,LINK0,MULTICAST>
      VLAN: IP2
      Ports:
      inet 10.1.12.1/24 broadcast 10.1.12.255
```

If BGP accounting is started with the **ip bgp-accounting start accounting** command, use the **bgp-actg** option of the **ip show interfaces** command to display BGP accounting information for the IP interface "int1":

```
rs#ip show interfaces int1 bgp-actg

Interface:int1 ①
  ②      ③      ④
Bucket  Packets  Bytes
0        0        0
1       111     14430
```

Legend:

1. Name of the interface for which BGP accounting information is displayed. Note that BGP accounting must be enabled for this interface. (Configuring and using BGP accounting is explained in the *Riverstone Networks RS Switch Router User Guide*.)
2. Bucket corresponds to the traffic index set with the **set-traffic-index** parameter of the **route-map permit/deny** command.

Bucket "0" is a special index that includes:

- traffic with a traffic index number greater than 25
- traffic with no traffic index number
- traffic with a traffic index number of 0

3. Number of packets sent on interface.
4. Number of bytes sent on interface.

If BGP accounting is started with the **ip bgp-accounting start dscp-accounting** command, use the **bgp-actg** option of the **ip show interfaces** command to display BGP accounting information for the IP interface "int1":

```
rs# ip show interfaces all bgp-actg
```

Interface:int1 ①				
②	③	④	⑤	
Bucket	DSCP	Packets	Bytes	
10	1	239376	15320064	
10	2	239201	15308864	
10	3	239001	15296064	
10	4	238801	15283264	
10	5	238601	15270464	
10	6	238401	15257664	
10	10	238254	15248256	
10	17	238401	15257664	
11	11	238189	15244096	
11	15	237801	15219264	
11	17	239206	15309184	
11	20	239387	15320768	
12	12	238176	15243264	
12	14	237601	15206464	
12	18	239001	15296064	

Legend:

1. Name of the interface for which BGP accounting information is displayed. Note that BGP accounting must be enabled for this interface. (Configuring and using BGP accounting is explained in the *Riverstone Networks RS Switch Router User Guide*.)
2. Bucket corresponds to the traffic index set with the **set-traffic-index** parameter of the **route-map permit/deny** command.
3. DSCP corresponds to the DSCP value in the counted packet. Packets with different DSCP values are counted separately, even if they all belong to the same traffic index. DSCP values 0 through 63 are counted.
4. Number of packets sent on interface per DSCP value for the bucket.
5. Number of bytes sent on interface per DSCP value for the bucket.

ip show reverse-flows

Mode

Enable

Format

ip show reverse-flows

Description

The **ip show reverse-flows** command displays the reverse flow statistics. Reverse flows are IP traffic flows in the opposite direction, where source information becomes destination information and vice versa. This command shows the number of reverse flow packets.

Restrictions

None

Example

To display the reverse flow statistics:

```
rs# ip show reverse-flows
IP Reverse Flow Statistics :
Total reverse-flow packets      : 0
Successful reverse-flow packets : 0
Unsuccessful reverse-flow packets : 0
Arphold packets                 : 0
Find Flow entry success packets : 0
Sum of arp hold and flow entry success packets : 0
```

ip show routes

Mode

Enable

Format

```
ip show routes [show-protocol  
direct|default|ospf|ospf-ase|rip|bgp|static|aggregate|isis-level-1|isis-level-2]  
[show-arps] [show-multicast] [show-summary] [verbose]
```

Description

The **ip show routes** command displays the IP routing table. Different command options can be used to show different aspects of the routing table.

Parameter	Value	Meaning
show-protocol		Shows only the IP routes that belong to one of these specified protocols:
	direct	Shows all direct routes.
	default	Shows all default routes.
	ospf	Shows all OSPF (Open Shortest Path First) routes.
	ospf-ase	Shows all OSPF (Open Shortest Path First) Autonomous System-External routes.
	rip	Shows all RIP (Routing Information Protocol) routes.
	bgp	Shows all BGP (Border Gateway Protocol) routes.
	isis-level-1	Shows all IS-IS (Intermediate System to Intermediate System) level 1 routes.
	isis-level-2	Shows all IS-IS (Intermediate System to Intermediate System) level 2 routes.
	static	Shows all manually defined routes.
	aggregate	Shows all aggregate routes.
show-arps		By default, ARP entries are not shown. To show ARP entries (if any are present), specify the show-arps option.
show-multicast		By default, routes to multicast destinations are not shown. To show routes to multicast destinations, specify the show-multicast option.
show-summary		Shows a summary of all route entries.
verbose		Show the routing table in verbose mode. The additional information is useful for debugging.

Restrictions

None.

Example

The following example displays the contents of the routing table. It shows that some of the route entries are for locally connected interfaces (“directly connected”), while some of the other routes are learned from RIP.

rs# ip show routes			
Destination	Gateway	Owner	Netif
-----	-----	-----	-----
10.1.0.0/16	50.1.1.2	RIP	to-linux2
10.2.0.0/16	50.1.1.2	RIP	to-linux2
10.3.0.0/16	50.1.1.2	RIP	to-linux2
10.4.0.0/16	50.1.1.2	RIP	to-linux2

ip show stack-queues

Mode

Enable

Format

ip show stack-queues

Description

The ip show stack-queues command displays IP stack queues.

Restrictions

None.

Example

Following is an example of the **ip show stack queues** command:

```
rs# ip show stack-queues
IP Stack Queue sizes are :
IP Control Queue Size    : 512
IP Control Queue Drops   : 0
IP Data Queue Size       : 512
IP Data Queue Drops      : 0
```


29 IP-POLICY COMMANDS

The **ip-policy** commands let you set up policies that cause the RS to forward packets to a specified IP address based on information in a packet's L3/L4 IP header fields.

29.1 COMMAND SUMMARY

The following table lists the **ip-policy** commands. The sections following the table describe the command syntax for each command.

<code>ip-policy <name> apply local interface <name> all</code>
<code>ip-policy clear all policy-name <name> all</code>
<code>ip-policy <name> deny acl <aclname> everything-else [sequence <num>]</code>
<code>ip-policy <name> permit acl <aclname> everything-else next-hop-list <ip-addr-list> null action policy-first policy-last policy-only [sequence <num>] [origin-as <num-list-or-range> everything-else]</code>
<code>ip-policy <name> set load-policy round-robin ip-hash sip dip both</code>
<code>ip-policy <name> set pinger on</code>
<code>ip-policy <policy-name> set pinger-options [port <port number>] [ping-int <num>] [ping-tries <num>] [app-int <num>] [app-tries <num>] [acv-command <string> acv-reply <string>] [acv-quit <string>] [read-till-index <num>] [app-check-on]</code>
<code>ip-policy show [all] [policy-name <name> all] [interface <name> all]</code>

ip-policy apply

Mode
Configure

Format

ip-policy <name> apply local|interface <InterfaceName>|all

Description

Once you have defined an IP policy, you use the **ip-policy apply** command to apply the IP policy to an interface. Once the IP policy is applied to the interface, packets start being forwarded using the policy.

Parameter	Value	Meaning
	<name>	Is the name of a previously defined IP policy.
local		Causes packets generated by the RS to be forwarded according to the IP policy.
interface	<interfacename>	Is the name of the inbound interface to which you are applying the IP policy. The interface name must be less than 32 characters.
all		Causes the IP policy to be applied to all IP interfaces.

Restrictions

IP policies can be applied to IP interfaces only.

Examples

To apply IP policy p1 to interface int4:

```
rs(config)# ip-policy p1 apply interface int4
```

To apply IP policy p2 to all IP packets generated on the RS:

```
rs(config)# ip-policy p2 apply local
```

ip-policy clear

Mode

Enable

Format

```
ip-policy clear all|policy-name <name>
```

Description

The **ip-policy clear** command is used in conjunction with the **ip-policy show** command, which gathers statistics about IP policies. The **ip-policy clear** command lets you reset IP policy statistics to zero.

Parameter	Value	Meaning
all		Causes statistics to be cleared for all IP policies.
policy-name	<name>	Is the name of an active IP policy.

Restrictions

None.

Examples

To clear statistics for IP policy p1:

```
rs# ip-policy clear policy-name p1
```

To clear statistics for all IP policies:

```
rs# ip-policy clear all
```

ip-policy deny

Mode
Configure

Format

```
ip-policy <name> deny acl <aclname>|everything-else [sequence <num>]
```

Description

The **ip-policy deny** command allows you to specifically prevent packets that match a profile from being forwarded with an IP policy. These packets are routed using dynamic routes instead.



Note Since there is an implicit deny rule at the end of all IP policies, all packets that do not match any policy are forwarded using dynamic routes.

Parameter	Value	Meaning
	<name>	Is the name of an IP policy.
acl	<aclname>	Is the name of the ACL profile of the packets to be excluded from IP policy-based forwarding. Profiles are defined with the acl command. The ACL may contain either permit or deny keywords. The ip-policy deny command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS.
everything-else		Keyword that specifies an action to be performed for packets that do not match any of the previously-defined ACLs. Specifies that packets that are not <i>specifically</i> permitted to use policy-based routing are forwarded using dynamic routes.
sequence	<num>	If an IP policy is composed of more than one ip-policy statement, specifies the order in which the statement is evaluated. Possible values are 1-65535. The ip-policy statement with the lowest sequence number is evaluated first.

Restrictions

ACLs for non -IP protocols cannot be used for IP policy routing.

Examples

To create a profile called “prof1” for telnet packets from 9.1.1.5 to 15.1.1.2:

```
rs(config)# acl prof1 permit ip 9.1.1.5 15.1.1.2 any any telnet 0
```



Note See "[acl permit|deny ip](#)" for more information on creating profiles for IP policy routing.

To create an IP policy called “p3” that prevents packets matching prof1 (that is, telnet packets from 9.1.1.5 to 15.1.1.2) from being forwarded using an IP policy:

```
rs(config)# ip-policy p3 deny acl prof1
```

To create a policy called “p4” that prevents all packets that have not been specifically permitted to use policy-based routing (using the **ip-policy permit** command) from being forwarded using an IP policy:

```
rs(config)# ip-policy p4 deny acl everything-else
```

ip-policy permit

Mode

Configure

Format

```
ip-policy <name> permit acl <aclname>|everything-else next-hop-list <ip-addr-list>|null
action policy-first|policy-last|policy-only [sequence <num>] [origin-as
<num-list-or-range>|everything-else]
```

Description

The **ip-policy permit** command allows you to specify the next-hop gateway where packets matching a given profile should be forwarded. You can specify up to 16 next-hop gateways for an IP policy. Packets matching a profile you defined with an **acl** command are forwarded to the next-hop gateway.

You can specify when to apply the IP policy route with respect to dynamic or statically configured routes. You can cause packets to use the IP policy route first, then the dynamic route if the next-hop gateway is unavailable; use the dynamic route first, then the IP policy route; or drop the packets if the next-hop gateway is unavailable.

Parameter	Value	Meaning
	<name>	Is the name of an IP policy.
acl	<aclname>	Is the name of the ACL profile of the packets to be forwarded using an IP policy. Profiles are created with the acl command. The ACL may contain either permit or deny keywords. The ip-policy permit command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS.
everything-else		Specifies that all packets not <i>specified</i> using policy-based routing (i.e., with the ip-policy deny command) are forwarded to the next-hop gateway.
next-hop-list	<ip-addr-list>	Is the IP address of one or more next-hop gateways. Packets matching the profile specified in <aclname> are forwarded to one of the gateways specified here. You can specify up to 16 gateways for each profile. If you specify more than one gateway, enclose the list of IP addresses in quotes. You can define how the packet load is distributed among multiple gateways with the ip-policy set load-policy command.
	null	To drop packets that match the profile, use the null keyword.
action		Specifies how IP policies are applied with respect to dynamic or statically configured routes.

Parameter	Value	Meaning
	policy-first	Causes packets matching the specified profile to use the IP policy route first. If the next-hop gateway specified in the IP policy is not reachable, the dynamic route is used instead.
	policy-last	Causes packets matching the specified profile to be routed using dynamic routes first. If a dynamic route is not available, then all packets matching the profile are routed using the IP policy gateway.
	policy-only	Causes packets matching the specified profile to use the IP policy route. If the next-hop gateway specified in the IP policy is not reachable, then the packets are dropped.
sequence	<num>	If an IP policy is composed of more than one ip-policy statement, specifies the order in which the statement is evaluated. Possible values are 1-65536. The ip-policy statement with the lowest sequence number is evaluated first.
origin-as	<num-list-or-range>	Specify the origin AS number for matching flows. You can specify a list of numbers separated by commas or a range of numbers.
	everything-else	Specifies that the default action will be used.

Restrictions

ACLs for non IP protocols cannot be used for IP policy routing.

Examples

To create a profile called “prof1” for telnet packets from 9.1.1.5 to 15.1.1.2:

```
rs(config)# acl prof1 permit ip 9.1.1.5 15.1.1.2 any any telnet 0
```



Note See "[acl permit|deny ip](#)" for more information on creating profiles for IP policy routing.

To cause packets matching prof1 (that is, telnet packets from 9.1.1.5 to 15.1.1.2) to be forwarded to 10.10.10.10:

```
rs(config)# ip-policy p5 permit acl prof1 next-hop-list 10.10.10.10
```

To cause all packets that have not been specified using policy-based routing (using the **ip-policy deny** command) to be forwarded to 10.10.10.10:

```
rs(config)# ip-policy p5 permit acl everything-else next-hop-list 10.10.10.10
```

To cause packets matching prof1 to use dynamic routes if 10.10.10.10 is not available:

```
rs(config)# ip-policy p5 permit acl prof1 next-hop-list 10.10.10.10 action policy-first
```

To cause packets matching prof1 to be dropped if 10.10.10.10 is not available:

```
rs(config)# ip-policy p5 permit acl prof1 next-hop-list 10.10.10.10 action policy-only
```


ip-policy set load-policy

Mode

Configure

Format

```
ip-policy <name> set load-policy round-robin|ip-hash sip|dip|both
```

Description

If you specify more than one next-hop gateway in an IP policy, you can use the **ip-policy set** command to control how the load is distributed among the next-hop gateways. You can cause each new flow to use the first available next-hop gateway in the **ip-policy permit** statement, or you can cause flows to use all the next-hop gateways in the **ip-policy permit** statement sequentially. You can also control which information in the IP packet to use to determine the next-hop gateway.

Parameter	Value	Meaning
	<name>	Is the name of an IP policy.
load-policy		If an IP policy has more than one next-hop gateway, specifies how the packets are distributed among the gateways. Two options are available:
	round-robin	Uses a sequential order to pick the next gateway in the list for each new flow.
	ip-hash	Uses the following information in the IP packet to determine the next hop gateway:
	sip	Uses the source IP based selection.
	dip	Uses the destination IP based selection.
	both	Uses both source IP and destination IP for selection.

Restrictions

None.

Examples

To set up 10.10.10.10 and 10.10.10.5 as next-hop gateways for IP policy p6:

```
rs(config)# ip-policy p6 permit profile prof1 next-hop-list '10.10.10.10 10.10.10.5'
```

To distribute flows among these two next-hop gateways in a sequential manner:

```
rs(config)# ip-policy p6 set load-policy round-robin
```

ip-policy set pinger on

Mode
Configure

Format

ip-policy <name> set pinger on

Description

You can use the **ip-policy set pinger on** command to have the RS query the availability of the next-hop gateways specified in an IP policy. When this option is active, the RS periodically queries the next-hop gateways via ICMP_ECHO_REQUESTS. Only gateways that respond to these requests are used for forwarding packets.

Parameter	Value	Meaning
	<name>	Is the name of an IP policy.



Note Some hosts may have disabled responding to ICMP_ECHO packets. Make sure each next-hop gateway can respond to ICMP_ECHO packets before using this option.

Restrictions

None.

ip-policy set pinger-options

Mode

Configure

Format

```
ip-policy <policy-name> set pinger-options [port <port-number>] [app-check-on]
[ping-int <sec>] [ping-tries <num>] [app-int <sec>] [app-tries <num>] [acv-command
<command-string>] [acv-reply <verif-string>] [acv-quit <quit-command>] [read-till-index
<index>]
```

Description

The **ip-policy set pinger-options** command lets you set various options for checking the availability of next-hop gateways for the specified IP policy. You must have previously issued the **ip-policy set pinger on** command to enable checking of next-hop gateways.

Parameter	Value	Meaning
	<policy-name>	The name of the IP policy.
port	<port-number>	Use this parameter to set the port for availability checks. Specify a number between 1 and 65535.
app-check-on		Use this parameter to send TCP connection requests (instead of ICMP echo requests) to check the availability of next-hop gateways.
ping-int	<sec>	Use this parameter to set the ping interval (seconds) for next-hop gateways in this policy. Specify any value between 1 and 3600. The default value is 5.
ping-tries	<num>	Use this parameter to set the number of ping retries before marking the gateway down. Specify any value between 1 and 255. The default value is 4.
app-int	<sec>	Use this parameter to set the interval (seconds) between application checks. Specify any value between 1 and 3600. The default value is 15.
app-tries	<num>	Use this parameter to set the number of retries before marking the application down. Specify any value between 1 and 255. The default value is 4.
acv-command	<command-string>	Use this parameter to set the application content verification command.
acv-reply	<verif-string>	Use this parameter to set the application content verification reply.

Parameter	Value	Meaning
acv-quit	<i><quit-command></i>	Use this parameter to set the application content verification command to be sent before closing connection.
read-till-index	<i><index></i>	Specify this parameter to instruct checking until this index for the start of 'acv-reply'. Specify a number between 2 and 255.

Restrictions

None.

Example

To cause the RS to check the availability of next-hop gateways for the IP policy 'p1' by pinging every 10 seconds:

```
rs(config)# ip-policy p1 set pinger on
rs(config)# ip-policy set pinger-options p1 ping-int 10
```

ip-policy show

Mode

Enable

Format

```
ip-policy show [all] [local] [policy-name <name>|all] [interface <name>|all]
```

Description

The **ip-policy show** command displays information about active IP policies, including profile definitions, policy configuration settings, and next-hop gateways. The command also displays statistics about packets that have matched an IP policy statement as well as the number of packets that have been forwarded to each next-hop gateway.

Parameter	Value	Meaning
all		Displays information about all IP policies.
local		Displays information about IP policies applied to locally-generated frames
policy-name	<name> all	Is the name of an IP policy. Use the all keyword to display all active policies.
 Note The ip-policy show all command works identically to the ip-policy show policy-name all command.		
interface	<name> all	Displays information about IP policies that have been applied to a specified interface. If you use the all keyword, the command displays information about IP policies that have been applied to all interfaces (that is, by using the ip-policy apply interface all command).

Restrictions

None.

Example

The following displays information about IP policy p1:

```
rs# ip-policy show policy-name p1
```

IP Policy name		: p1				
Applied Interfaces		: int1				
Load Policy		: first available				
ACL	Source IP/Mask	Dest. IP/Mask	SrcPort	DstPort	TOS	Prot

prof1	9.1.1.5/32	15.1.1.2	any	any	0	IP
prof2	2.2.2.2/32	anywhere	any	any	0	IP
everything	anywhere	anywhere	any	any	0	IP
Next Hop Information						

Seq	Rule	ACL	Cnt	Action	Next Hop	Cnt Last

10	permit	prof1	0	Policy Only	11.1.1.2	0 Dwn
20	permit	prof2	0	Policy Last	1.1.1.1	0 Dwn
					2.2.2.2	0 Dwn
					3.3.3.3	0 Dwn
999	permit	everything	0	Policy Only	drop	N/A N/A
65536	deny	deny	0	N/A	normal fwd	N/A N/A

Table 29-1 Display Field Descriptions for the ip-policy show Command

FIELD	DESCRIPTION
IP Policy name	The name of the IP policy
Applied Interfaces	The interface where the IP policy was applied
Load policy	The load distribution setting for IP-policy statements that have more than one next-hop gateway; either first available (the default) or round-robin
ACL	The names of the profiles (created with an acl statement) associated with this IP policy
Source IP/Mask	The source address and filtering mask of this flow
Dest. IP/Mask	The destination address and filtering mask of this flow
SrcPort	For TCP or UDP, the number of the source TCP or UDP port
DstPort	For TCP or UDP, the number of the destination TCP or UDP port
TOS	The type of service value in the packet
Prot	The protocol of the profile (IP, ICMP, TCP UDP)

FIELD	DESCRIPTION
Seq	The sequence in which the statement is evaluated. IP policy statements are listed in the order they are evaluated (lowest sequence number to highest).
Rule	The rule to apply to the packets matching the profile: either permit or deny
ACL	The name of the profile (ACL) of the packets to be forwarded using an IP policy
Cnt	The number of packets that have matched the profile since the IP policy was applied (or since the ip-policy clear command was last used)
Action	The method by which IP policies are applied with respect to dynamic or statically configured routes; possible values are Policy First, Policy Only, or Policy Last.
Next Hop	The list of next-hop gateways in effect for the policy statement
Cnt	The number of packets that have been forwarded to this next-hop gateway
Last	The state of the link the last time an attempt was made to forward a packet; possible values are up, down, or N/A
65536 deny deny	Implicit deny rule that is always evaluated last, causing all packets that do not match one of the profiles to be forwarded normally (with dynamic routes)

30 IP-REDUNDANCY COMMANDS

The **ip-redundancy** commands let you display and configure the Virtual Router Redundancy Protocol (VRRP) on the RS. VRRP is defined in RFC 2338.

30.1 COMMAND SUMMARY

The following table lists the **ip-redundancy** commands. The sections following the table describe the command syntax for each command.

<code>ip-redundancy associate vrrp <vrid> interface <interface> id <vrid></code>
<code>ip-redundancy clear vrrp-stats interface <interface> id <vrid></code>
<code>ip-redundancy create vrrp <vrid> interface <interface></code>
<code>ip-redundancy set vrrp <vrid> interface <interface> <option></code>
<code>ip-redundancy set vrrp <vrid> interface <interface> [priority <num>] [adv-interval <num>] [preempt-mode enabled disabled] [auth-type none text] [auth-key <key>] [warmup-period <num>]</code>
<code>ip-redundancy start vrrp <vrid> interface <interface></code>
<code>ip-redundancy trace vrrp <option></code>

ip-redundancy associate

Mode

Configure

Format

```
ip-redundancy associate vrrp <vrid> interface <interface> address <ipaddr/mask>
```

Description

The **ip-redundancy associate** command adds an IP address to the list of IP addresses associated with a virtual router.

Parameter	Value	Meaning
vrrp	<vrid>	Is the identifier of a virtual router. Specify a number between 1-255.
interface	<interface>	Is the name of the interface where the virtual router resides.
address	<ipaddr/mask>	Is the IP address and subnet mask to be associated with the virtual router.

Restrictions

None

Example

To add IP address/mask 1.2.3.4/16 to the list of IP addresses associated with virtual router 1 on interface int1:

```
rs(config)# ip-redundancy associate vrrp 1 interface int1 address 1.2.3.4/16
```

ip-redundancy clear vrrp-stats

Mode

Enable

Format

```
ip-redundancy clear vrrp-stats interface <interface> [id <vrid>]
```

Description

The **ip-redundancy clear vrrp-stats** command clears statistics gathered for VRRP. This command is used in conjunction with the **ip-redundancy show vrrp** command, which displays information about the virtual routers associated with an interface. When you specify the **verbose** option with the **ip-redundancy show vrrp** command, additional statistics are shown, including the number of times a Backup router became the Master, the number of VRRP advertisements received, and counts of VRRP packets that contain errors. When you run the **ip-redundancy clear vrrp-stats** command, these statistics are reset to zero.

Parameter	Value	Meaning
interface	<interface>	Causes VRRP statistics to be cleared for all virtual routers on the specified interface.
id	<vrid>	Causes VRRP statistics to be cleared for the virtual router with the specified VRID. Enter a number between 1-255.

Restrictions

None.

Example

To clear statistics for virtual router 1 on interface int1:

```
rs# ip-redundancy clear vrrp-stats interface int1 id 1
```

ip-redundancy create

Mode

Configure

Format

```
ip-redundancy create vrrp <vrid> interface <interface>
```

Description

The **ip-redundancy create** command creates a virtual router on a specified interface.

Parameter	Value	Meaning
vrrp	<vrid>	Is the identifier of the virtual router to create. Specify a number between 1-255.
interface	<interface>	Is the interface on which to create the virtual router.

Restrictions

None.

Example

To create a virtual router with an identifier (VRID) of 1 on interface int1:

```
rs(config)# ip-redundancy create vrrp 1 interface int1
```

ip-redundancy set vrrp

Mode

Configure

Format

```
ip-redundancy set vrrp <vrid> interface <interface> [priority <num>] [adv-interval <num>]  
[preempt-mode enabled|disabled] [auth-type none|text] [auth-key <key>] [warmup-period  
<num>]
```

Description

The **ip-redundancy set** command lets you specify parameters for a virtual router, including backup priority, advertisement interval, whether the router can preempt a Master router that has a lower priority, the type of authentication used, and warm up time.

Parameter	Value	Meaning
vrrp	<vrid>	Is the identifier of a virtual router. Specify a number between 1-255.
interface	<interface>	Is the name of the interface where the virtual router resides.
priority	<num>	Specifies the backup priority to be used by this virtual router. This number must be between 1-254. The default is 100. The priority number applies only if the virtual router is not the IP address owner. The priority of the IP address owner is always 255 and cannot be changed.
adv-interval	<num>	Is the interval between VRRP advertisements in seconds. The default is 1 second.
preempt-mode		Specifies whether a backup router can preempt a Master router with a lower priority. Use one of the following keywords:
	enabled	Preempt mode is enabled. A backup router can pre-empt a lower-priority Master router.
	disabled	Pre-empt mode is disabled. A backup router cannot pre-empt a lower-priority Master router.
auth-type		Specifies the type of authentication used for VRRP exchanges between routers. Use one of the following keywords:
	none	VRRP exchanges are not authenticated (the default).
	text	VRRP exchanges are authenticated with a clear-text password.

Parameter	Value	Meaning
auth-key	<key>	Is the clear-text password used to authenticate VRRP exchanges. If you specify the text keyword, you must also specify the auth-key parameter.
warmup-period	<num>	Specifies the amount of delay (in seconds) before this virtual router is initialized, following a system reboot. Specify any number between 0 and 180. This delay is used to prevent a virtual router from preempting an existing Master before having received all of the routing updates from neighboring routers. (Default delay is 30 secs).

Restrictions

None.

Examples

To specify 200 as the priority used by virtual router 1 on interface int1:

```
rs(config)# ip-redundancy set vrrp 1 interface int1 priority 200
```

To set the advertisement interval to 3 seconds:

```
rs(config)# ip-redundancy set vrrp 1 interface int1 adv-interval 3
```

To prevent a Backup router from taking over as Master from a Master router that has a lower priority:

```
rs(config)# ip-redundancy set vrrp 1 interface int1 preempt-mode disabled
```

To authenticate VRRP exchanges on virtual router 1 on interface int1 with a password of 'yago':

```
rs(config)# ip-redundancy set vrrp 1 interface int1 auth-type text auth-key yago
```

ip-redundancy show vrrp

Mode

Enable

Format

```
ip-redundancy show vrrp interface <interface> [id <vrid>] [verbose]
```

Description

The **ip-redundancy show vrrp** command displays configuration information about virtual routers on an interface. You can display information for one virtual router or for all the virtual routers on an interface. If you specify the verbose option, additional statistics are shown, including the number of times a Backup router became the Master, the number of VRRP advertisements received, and counts of VRRP packets that contain errors. These statistics are gathered from the time you start the virtual router, or from the time you last ran the **ip-redundancy clear vrrp-stats** command.

Parameter	Value	Meaning
interface	<interface>	Is the name of the interface where the virtual router resides. If you do not specify the <vrid> parameter, information about all virtual routers on the interface is displayed.
id	<vrid>	Is the identifier of a virtual router. Specify a number between 1-255.
verbose		Causes VRRP statistics to be displayed for each virtual router.

Restrictions

None.

Examples

To display information about all virtual routers on interface int1:

```
rs# ip-redundancy show vrrp interface int1

VRRP Virtual Router 100 - Interface int1
-----
Uptime                0 days, 0 hours, 0 minutes, 17 seconds.
State                 Backup
Priority              100 (default value)
Virtual MAC address   00005E:000164
Advertise Interval    1 sec(s) (default value)
Preempt Mode         Enabled (default value)
Authentication        None (default value)
Primary Address       10.8.0.2
Associated Addresses  10.8.0.1
                    100.0.0.1

VRRP Virtual Router 200 - Interface int1
-----
Uptime                0 days, 0 hours, 0 minutes, 17 seconds.
State                 Master
Priority              255 (default value)
Virtual MAC address   00005E:0001C8
Advertise Interval    1 sec(s) (default value)
Preempt Mode         Enabled (default value)
Authentication        None (default value)
Primary Address       10.8.0.2
Associated Addresses  10.8.0.2
```


To display VRRP statistics for virtual router 100 on interface int1:

```
rs# ip-redundancy show vrrp 1 interface int1 verbose

VRRP Virtual Router 100 - Interface int1
-----
Uptime                0 days, 0 hours, 0 minutes, 17 seconds.
State                 Backup
Priority              100 (default value)
Virtual MAC address   00005E:000164
Advertise Interval    1 sec(s) (default value)
Preempt Mode          Enabled (default value)
Authentication        None (default value)
Primary Address       10.8.0.2
Associated Addresses  10.8.0.1
                     100.0.0.1

Stats:
  Number of transitions to master state      2
  VRRP advertisements rcvd                  0
  VRRP packets sent with 0 priority          1
  VRRP packets rcvd with 0 priority          0
  VRRP packets rcvd with IP-address list mismatch 0
  VRRP packets rcvd with auth-type mismatch  0
  VRRP packets rcvd with checksum error      0
  VRRP packets rcvd with invalid version     0
  VRRP packets rcvd with invalid VR-Id      0
  VRRP packets rcvd with invalid adv-interval 0
  VRRP packets rcvd with invalid TTL        0
  VRRP packets rcvd with invalid 'type' field 0
  VRRP packets rcvd with invalid auth-type  0
  VRRP packets rcvd with invalid auth-key   0
```

ip-redundancy start vrrp

Mode

Configure

Format

```
ip-redundancy start vrrp <vrid> interface <interface>
```

Description

The **ip-redundancy start vrrp** command starts a virtual router on the specified interface.

Parameter	Value	Meaning
vrrp	<vrid>	Is the identifier of a virtual router. Specify a number between 1-255.
interface	<interface>	Is the name of the interface where the virtual router resides.

Restrictions

None.

Example

To start virtual router 1 on interface int1:

```
rs# ip-redundancy start vrrp 1 interface int1
```

ip-redundancy trace

Mode

Configure

Format

```
ip-redundancy trace vrrp events|state-transitions|packet-errors
```

```
ip-redundancy trace vrrp all enabled|disabled
```

Description

The **ip-redundancy trace vrrp** command displays messages when certain VRRP events take place on the RS. Use this command to display messages when a virtual router changes from one state to another (i.e., from Backup to Master), a VRRP packet error is detected, or when any VRRP event occurs.

Parameter	Value	Meaning
events		Displays a message when VRRP receives any type of event. This option is disabled by default.
state-transitions		Displays a message when a VRRP router changes from one state to another. This option is enabled by default.
packet-errors		Displays a message when a VRRP packet error is detected. This option is enabled by default.
all	enabled disabled	Enables or disables all VRRP tracing.

Restrictions

None.

31 IP-ROUTER COMMANDS

The **ip-router** commands let you configure and monitor features and functions that work across the various routing protocols.

31.1 COMMAND SUMMARY

The following table lists the **ip-router** commands. The sections following the table describe the command syntax for each command.

ip-router authentication add key-chain <num> <string> <option-list>
ip-router authentication create key-chain <num> <string> <option-list>
ip-router clear dropped-route-stats
ip-router find route <ip-addr> [ignore-state]
ip-router global add interface <name-or-IPaddr>
ip-router global add martian <ipAddr/mask> default[host][allow]
ip-router global set autonomous-system <num1> loops <num2>
ip-router global set confederation-id <identifier>
ip-router global set install-lsp-routes on off
ip-router global set interface <interface-name> all preference <num1> down-preference <num2> passive autonomous system <num3>
ip-router global set max-bgjob-interval <seconds>
ip-router global set memory-threshold level-1 <percent1> level-2 <percent2> level-3 <percent3> level-4 <percent4> [disable]
ip-router global set router-id <hostname-or-IPaddr>
ip-router global set trace-level <level>
ip-router global set trace-options <option-list>
ip-router global set trace-state on off
ip-router global use provided_config
ip-router kernel set flash-inst-cnt <number-of-routes>
ip-router kernel set inst-cnt <number-of-routes>

ip-router kernel trace <option-list> detail send receive
ip-router policy add aspath-regular-expression <identifier> <regex>
ip-router policy add community-list <number-or-string> <community-string>
ip-router policy add filter <option-list>
ip-router policy add optional-attributes-list <number-or-string> <option-list>
ip-router policy aggr-gen destination <name> <option-list>
ip-router policy create aggr-export-source <option-list>
ip-router policy create aggr-gen-dest <option-list>
ip-router policy create aggr-gen-source <option-list>
ip-router policy create aspath-export-source <number-or-string> <option-list>
ip-router policy create aspath-regular-expression <identifier> <regex>
ip-router policy create bgp-export-destination <number-or-string> <option-list>
ip-router policy create bgp-export-source <number-or-string> <option-list>
ip-router policy create bgp-import-source <number-or-string> <option-list>
ip-router policy create community-list <number-or-string> <community-string>
ip-router policy create direct-export-source <option-list>
ip-router policy create filter <option-list>
ip-router policy create isis-export-destination <number-or-string> <option-list>
ip-router policy create isis-export-source <number-or-string> <option-list>
ip-router policy create optional-attributes-list <option-list>
ip-router policy create ospf-export-destination <number-or-string> <option-list>
ip-router policy create ospf-export-source <number-or-string> <option-list>
ip-router policy create ospf-import-source <number-or-string> <option-list>
ip-router policy create rip-export-destination <number-or-string> <option-list>
ip-router policy create rip-export-source <number-or-string> <option-list>
ip-router policy create rip-import-source <number-or-string> <option-list>
ip-router policy create static-export-source <option-list>
ip-router policy create tag-export-source <number-or-string> <option-list>
ip-router policy export destination <option-list>
ip-router policy import source <option-list>
ip-router policy redistribute from-proto <protocol> <option-list> to-proto <option-list>
ip-router policy summarize route <ipAddr/mask> default <option-list>
ip-router show configuration-file active permanent
ip-router show rib [detail [show-all-info]]
ip-router show route [ip-addr-mask default] [detail] longer-prefixes

<code>ip-router show route-preferences</code>
<code>ip-router show state [all] [memory] [timers] [task <string> all gii icmp inet interface krt route]</code>
<code>ip-router show summary [drops]</code>

ip-router authentication add key-chain

Mode
Configure

Format

ip-router authentication add key-chain <num>|<string>|<option-list>

Description

This command adds a key to an existing key-chain.

Parameter	Value	Meaning
key-chain	<num>	Identifies the key-chain with a numerical value.
	<string>	Identifies the key-chain with a character string.
	<option-list>	Specifies the options you are adding. Specify one of the following:
key	<string>	Adds a new key to an existing key-chain. The key can be up to 16 characters long.
type	primary secondary	Specifies whether the key is a primary key or a secondary key within the key chain. Default is primary.
id	<num>	Specifies an integer between 1 and 255. This option is only necessary for MD5 authentication method.

Restrictions

None.

ip-router authentication create key-chain

Mode

Configure

Format

```
ip-router authentication create key-chain <num>|<string>|<option-list>
```

Description

This command creates a key-chain and associate an identifier with it.

Parameter	Value	Meaning
key-chain	<num>	Identifies the key-chain with a numerical value.
	<string>	Identifies the key-chain with a character string.
	<option-list>	Specifies the options you are adding. Specify one of the following:
key	<string>	Specifies a key to be included in this key chain. The key can be up to 16 characters long.
type	primary secondary	Specifies whether the key is a primary key or a secondary key within the key chain. Default is primary.
id	<num>	Specifies an integer between 1 and 255. This option is only necessary for MD5 authentication method.

Restrictions

None.

ip-router clear dropped-route-stats

Mode

Enable

Format

```
ip-router clear dropped-route-stats
```

Description

This command clears the counter for routes that were dropped because of low memory.

Restrictions

None.

ip-router find route

Mode

Enable

Format

```
ip-router find route <ip-addr> [ignore-state]
```

Description

This command finds the active route in the RIB which the packet will use.

Parameter	Value	Meaning
route	<ip-addr>	Specifies the destination of the packet.
ignore-state		This optional parameter allows inactive routes to be considered in route determination.

Restrictions

None.

ip-router global add interface

Mode

Configure

Format

```
ip-router global add interface <name-or-IPaddr>
```

Description

This command adds an interface.

Parameter	Value	Meaning
interface	<name-or-IPaddr>	Makes an interface known to the IP router.

Restrictions

None.

ip-router global add martian

Mode

Configure

Format

```
ip-router global add martian <ipAddr/mask>|default [host] [allow]
```

Description

This command adds a martian. Martians are invalid addresses that are rejected by the routing software.

Parameter	Value	Meaning
martian	<ipAddr/mask>	The IP address and netmask for the martian.
	default	Adds default martian.
host		Specifies that this martian is a host address.
allow		Allows a subset of a range that was disallowed.

Restrictions

None.

ip-router global set autonomous-system

Mode

Configure

Format

```
ip-router global set autonomous-system <num1> loops <num2>
```

Description

This command sets the autonomous system number. This is required for BGP.

Parameter	Value	Meaning
autonomous-system	<num1>	Sets the AS number for the router. It is only required if the router is going to run BGP. Specify a number from 1 to 65535.
loops	<num2>	Controls the number of times the AS may appear in the as-path. Default is 1. It is only required if the router is going to run protocols that support as-path, such as BGP.

Restrictions

None.

ip-router global set confederation-id

Mode

Configure

Format

```
ip-router global set confederation-id <identifier>
```

Description

This command sets the BGP confederation identifier.

Parameter	Value	Meaning
confederation-id	<identifier>	Sets the autonomous system number that is the identifier to the outside world for the BGP confederation. Specify a number from 1 to 65535.

Restrictions

None.

ip-router global set install-lsp-routes

Mode

Configure

Format

```
ip-router global set install-lsp-routes on|off
```

Description

This command installs LSP routes in the FIB. By default, the LSP routes are not installed in the FIB.

Parameter	Value	Meaning
on		Install LSP routes in the FIB
off		Do not install LSP routes in the FIB

Restrictions

None.

ip-router global set interface

Mode

Configure

Format

```
ip-router global set interface <interface-name>|all preference <num1> down-preference  
<num2> passive autonomous system <num3>
```

Description

This command sets interface parameters.

Parameter	Value	Meaning
interface	<interface-name> all	Specify an interface that was added using the ip-router global add interface command, or all for all interfaces.
preference	<num1>	Sets the preference for routes to this interface when it is up and functioning. Specify a number from 0 – 255. Default value is 0.
down-preference	<num2>	Sets the preference for routes to this interface when it is down. Specify a number from 0 – 255. Default value is 255.
passive		Prevents changing of route preference to this interface if it is down.
autonomous-system	<num3>	The AS that will be used to create as-path associated with the route created from the definition of this interface. Value has range of from 1 to 65535

Restrictions

None.

ip-router global set max-bgjob-interval

Mode

Configure

Format

```
ip-router global set max-bgjob-interval <seconds>
```

Description

This command sets the maximum time interval (in seconds) that a background job waits.

Parameter	Value	Meaning
max-bgjob-interval	<seconds>	The maximum number of seconds that a background job waits. Specify a value between 4-600.

Restrictions

None.

ip-router global set memory-threshold

Mode

Configure

Format

```
ip-router global set memory-threshold level-1 <percent1> level-2 <percent2> level-3  
<percent3> level-4 <percent4> [disable]
```

Description

This command sets any of four thresholds for the percentage of memory used in the routing information base (RIB). When a level-1, level-2, or level-3 threshold is reached, a warning message appears and routes *may* be deleted from the RIB. When the level-4 threshold is reached, a warning message appears and *no* routing updates to the RIB are processed.

The **ip-router show summary drops** command shows information about routes that are deleted or not added due to low memory, as well as the current threshold settings and percentage of memory used. The protocol of the route determines whether existing routes are deleted or new routes added in the RIB when a threshold is reached. See the *Riverstone Networks RS Switch Router User Guide* for more information on memory thresholds.

Parameter	Value	Meaning
level-1	<percent1>	First threshold for memory consumption. This is a percentage of the memory used for the RIB. Specify a value between 1-99. The default is 60.
level-2	<percent2>	Second threshold for memory consumption. This is a percentage of the memory used for the RIB. Specify a value between 1-99. The default is 65.
level-3	<percent3>	Third threshold for memory consumption. This is a percentage of the memory used for the RIB. Specify a value between 1-99. The default is 70.
level-4	<percent4>	Fourth threshold for memory consumption. This is a percentage of the memory used for the RIB. Specify a value between 1-99. The default is 75.
disable		If this parameter is specified, the RS does not check to see if any threshold is reached.

Restrictions

None.

ip-router global set router-id

Mode
Configure

Format

ip-router global set router-id <hostname-or-IPaddr>

Description

This command sets the router ID for use by BGP and OSPF.

Parameter	Value	Meaning
router-id	<hostname-or-IPaddr>	The most preferred address is any address other than 127.0.0.1 on the loopback interface. If there are no secondary addresses on the loopback interface, then the default router ID is set to the address of the first interface which is in the up state that the RS encounters (except the interface en0, which is the Control Module’s interface). The address of a non point-to-point interface is preferred over the local address of a point-to-point interface.

Restrictions

None.

ip-router global set trace-level

Mode

Configure

Format

```
ip-router global set trace-level <level>
```

Description

This command sets the trace level.

Parameter	Value	Meaning
trace-level	<level>	Specifies the level of tracing. Specify a value between 0-255.

Restrictions

None.

ip-router global set trace-options

Mode

Configure

Format

```
ip-router global set trace-options <option-list>
```

Description

This command sets various trace options.

Parameter	Value	Meaning
trace-options	<option-list>	Specifies the trace options you are setting. Specify one or more of the following:
	startup	Trace startup events.
	parse	Trace lexical analyzer and parser of gate-d config files.
	ydebug	Trace lexical analyzer and parser in detail.
	adv	Trace allocation and freeing of policy blocks.
	all	Turn on all tracing.
	general	Turn on normal and route tracing.
	state	Trace state machine transitions in protocols.
	normal	Trace normal protocol occurrences. Abnormal occurrences are always traced.
	policy	Traces the application of policy to routes being exported and imported.
	task	Traces system interfaces and task processing associated with this protocol or peer.
	timer	Traces timer usage by this protocol or peer.
	route	Traces routing table changes for routes installed by this protocol or peer.

Restrictions

None.

ip-router global set trace-state

Mode

Configure

Format

```
ip-router global set trace-state on|off
```

Description

This command enables or disables tracing.

Parameter	Value	Meaning
trace-state	on off	Specifies whether you are enabling or disabling tracing. Specify on to enable tracing or specify off to disable tracing. The default is off .

Restrictions

None.

ip-router global use provided_config

Mode

Configure

Format

```
ip-router global use provided_config
```

Description

This command causes the RS to use the configuration file stored in the Control Module's NVRAM.

**Note**

This command requires that you first copy the ROSRD configuration into the Control Module's NVRAM.

To do this, enter the following command in Enable mode:

```
rs# copy tftp-server to rosrd.conf
TFTP server [10.50.89.88]? 10.50.89.88
Source filename [tmp/rosrd.conf]?
#####
%TFTP-I-XFERRATE, Received 5910 bytes in 0.1 seconds
```

Restrictions

None.

ip-router kernel set flash-inst-cnt

Mode

Configure

Format

```
ip-router kernel set flash-inst-cnt <number-of-routes>
```

Description

This command sets the number of routes flashed to protocol in one iteration.

Parameter	Value	Meaning
flash-inst-cnt	<number-of-routes>	Number of routes that are flashed to protocol in one iteration. Specify a number greater than or equal to 100. Default is unlimited.

Restrictions

None.

ip-router kernel set inst-cnt

Mode

Configure

Format

```
ip-router kernel set inst-cnt <number-of-routes>
```

Description

This command sets the number of routes installed in the forwarding information base in one iteration.

Parameter	Value	Meaning
inst-cnt	<number-of-routes>	Number of routes that are installed in the forwarding information base in one iteration. Specify a number greater than or equal to 100. Default is unlimited.

Restrictions

None.

ip-router kernel trace

Mode

Configure

Format

```
ip-router kernel trace <option-list> [detail][send][receive]
```

Description

This command provides trace capabilities between the Routing Information Base and the Forwarding Information Base.

Parameter	Value	Meaning
kernel trace	<option-list>	Specifies the kernel trace options. Specify one or more of the following:
	symbols	Trace symbols read from kernel.
	if-list	Trace the reading of the kernel interface list.
	packets	Packets exchanged with the kernel.
	routes	Routes exchanged with the kernel.
	redirect	Redirect messages received from the kernel.
	interface	Interface messages received from the kernel.
	other	All other messages received from the kernel.
	remnants	Routes read from the kernel when the RS routing process starts.
	request	The RS routing process requests to Add/Delete/Change routes in the kernel forwarding table.
	info	Informational messages received from the routing socket, such as TCP loss, routing lookup failure, and route resolution request.
detail		Show details about messages.
send		Show information about messages sent by ROSRD.
receive		Show information about messages received by ROSRD.

Restrictions

None.

ip-router policy add aspath-regular-expression Mode

Configure

Format

```
ip-router policy add aspath-regular-expression <identifier> <regexp>
```

Description

The **ip-router policy add aspath-regular-expression** command allows you to add an AS path regular expression to an existing AS path regular expression list. An AS path regular expression list and its associated identifier are created with the **ip-router policy create aspath-regular-expression** command.

Parameter	Value	Meaning
aspath-regular-expression	<identifier>	Specifies the identifier of the AS path regular expression list that was previously created with the ip-router policy create aspath-regular-expression command.
	<regexp>	Specifies the AS path regular expression to be used to match the AS path. Enclose the regular expression in quotes.

Restrictions

None.

Example

The following command *creates* an AS path regular expression list named ‘scRoutes’ that specifies AS paths that start with AS numbers 62000 or 63000.

```
rs(config)# ip-router policy create aspath-regular-expression scRoutes  
"((62000.*)|(63000.*))"
```

The following command *adds* to the newly-created list ‘scRoutes’ the specification for AS paths that start with AS number 64000:

```
rs(config)# ip-router policy add aspath-regular-expression scRoutes "(64000.*)"
```

Note that the two commands shown above are equivalent to the following single command line:

```
rs(config)# ip-router policy create aspath-regular-expression scRoutes  
"((62000.*)|(63000.*)|(64000))"
```

ip-router policy add community-list

Mode

Configure

Format

```
ip-router policy add community-list <number-or-string> <community-string>
```

Description

The **ip-router policy add community-list** command allows you to add communities to an existing community list. These community lists can be used in the **route-map** command to match a set of communities.

Parameter	Value	Meaning
community-list	<number-or-string>	Specifies the identifier of the community list.
	<community-string>	Quoted string of communities like "a:b c:d" where a,c are the AS portion of a community split and b,d are the community identifier portion of a community split. You can also specify the following keywords for well-known communities:
	no-export	Is a special community that indicates the routes associated with this attribute must not be advertised outside a BGP confederation boundary. Since the RS's implementation does not support confederations, this boundary is an AS boundary.
	no-advertise	Is a special community indicating that the routes associated with this attribute must not be advertised to other BGP peers.
	no-export-subconfed	Is a special community indicating the routes associated with this attribute must not be advertised to external BGP peers. (This includes peers in other members' autonomous systems inside a BGP confederation.)

Restrictions

None.

Example

In the following example, the first command creates a community list named 'comm'. The second command adds communities to the newly-created list 'comm':

```
rs(config)# ip-router policy create community-list comm "4:56 no-export"  
rs(config)# ip-router policy add community-list comm "6:78 no-advertise"
```

ip-router policy add filter

Mode

Configure

Format

```
ip-router policy add filter <number-or-string> network <ipAddr/mask> [exact|refines|between  
<low-high>][host-net] [restrict]
```

Description

This command adds a route filter. Routes are specified by a set of filters that will match a certain set of routes by destination, or by destination and mask.

Parameter	Value	Meaning
filter	<number-or-string>	Specifies the identifier of the route filter.
network	<IP-address>	Specifies networks that are to be filtered. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be filtered are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact , refines , or between parameters, the mask of the destination is also considered.
exact		Specifies that the mask of the routes to be filtered must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		Specifies that the mask of the routes to be filtered must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
host-net		This option qualifies that the specified network is a host. To match, the address must exactly match the specified and the network mask must be a host mask (i.e. all ones). This is equivalent to a network specification of host/255.255.255.255 along with the exact option.
restrict		Specifies that routes that match the filter are not exported.

Restrictions

None.

ip-router policy add optional-attributes-list

Mode

Configure

Format

```
ip-router policy add optional-attributes-list <number-or-string> <option-list>
```

Description

This command expands a previously created optional-attributes-list.

Parameter	Value	Meaning
optional-attributes-list	<number-or-string>	Specifies the identifier for the optional attributes list you are expanding.
<option-list>		Specifies the options you are setting. Specify the following:
community-id	<number>	Specifies a community identifier portion of a community split. This is combined with the autonomous system value entered to create a value for the community attribute.
autonomous-system	<number>	Specifies the autonomous system portion of a community split. This would be combined with the community id value entered to create a value for the community attribute. Specify a number from 1 to 65535.
well-known-community		Specifies one of the well-known communities.
reserved-community	<number>	Specifies one of the reserved communities which is not well-known. A reserved community is one which is in one of the following ranges (0x00000000 - 0x0000FFFF) or (0xFFFF0000 - 0xFFFFFFFF).

Restrictions

None.

ip-router policy aggr-gen destination

Mode

Configure

Format

```
ip-router policy aggr-gen destination <number-or-string> [source <number-or-string> [filter
<number-or-string>| [network <ipAddr/mask> [exact|refines|between <low-high>] [preference
<number>|restrict]]]]
```

Description

This command creates an aggregate or generate route.

Parameter	Value	Meaning
destination	<number-or-string>	Is the identifier of the aggregate-destination that specifies the aggregate/summarized route.
source	<number-or-string>	Is the identifier of the aggregate-source that contributes to an aggregate route.
filter	<number-or-string>	Specifies the filter for an aggregate/generate.
network	<ipAddr/mask>	This option specifies networks which are to be aggregated. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be aggregated are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact , refines , or between parameters, the mask of the destination is also considered.
exact		This option specifies that the mask of the routes to be aggregated must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		This option specifies that the mask of the routes to be aggregated must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
preference	<number>	This option specifies the preference to be assigned to the resulting aggregate route.

Restrictions

None.

ip-router policy create aggr-export-source

Mode

Configure

Format

```
ip-router policy create aggr-export-source <number-or-string> [metric <number>|restrict]  
[sequence-number <number>]
```

Description

This command creates a source for exporting aggregate routes into other protocols.

Parameter	Value	Meaning
aggregate-export -source	<number-or-string>	Specifies the identifier of the aggregate export source.
metric	<number>	Specifies the metric to be associated with the exported routes.
restrict		Specifies that nothing is exported from the specified source.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy create aggr-gen-dest

Mode

Configure

Format

```
ip-router policy create aggr-gen-dest <number-or-string> network <ipAddr/mask> [default [type  
aggregate|generation] [preference <number>]][brief]
```

Description

This command creates an aggregate-generation destination. An aggregate-generation destination is one of the building blocks needed to create an aggregate/generate route.

Parameter	Value	Meaning
aggr-gen-dest	<number-or-string>	Specifies the identifier of an aggregate-generation destination.
network	<ipAddr/mask> default	Specifies the aggregate or generated route.
type aggregate		Specifies that the destination is an aggregate.
type generation		Specifies that the destination is a generate.
preference	<num>	Specifies the preference to be assigned to the resulting aggregate route. The default preference is 130.
brief		Used to specify that the AS path should be truncated to the longest common AS path. The default is to build an AS patch consisting of SETs and SEQUENCES of all contributing AS paths.

Restrictions

None.

ip-router policy create aggr-gen-source

Mode

Configure

Format

```
ip-router policy create aggr-gen-source <number-or-string> protocol <protocol>
[autonomous-system <number>][aspath-regular-expression <identifier>][origin <origin>][tag
<number>][preference <number>|restrict]
```

Description

This command creates a source for the routes contributing to a aggregate/generate route.

Parameter	Value	Meaning
aggr-gen-source	<number-or-string>	Specifies the identifier of an aggregate-generation source.
protocol	<protocol>	Specifies the protocol of the contributing aggregate source. Specify one of the following:
	aggregate	Aggregate route sources.
	all	All protocols.
	bgp	BGP route sources.
	direct	Direct route sources
	isis-level-1	IS-IS level 1 route sources.
	isis-level-2	IS-IS level 2 route sources.
	ospf	OSPF route sources.
	rip	RIP route sources.
	static	Static route sources.
autonomous-system	<number>	Restricts selection of routes to those learned from the specified autonomous system. This selection may also be carried out by using route filters to explicitly list the set of routes to be accepted. Specify a number from 1 to 65535.
aspath-regular-expression	<identifier>	Specifies either a regular expression or the identifier of the AS path regular expression list that must be satisfied for the route to be selected. The AS path regular expression list and its identifier must have previously been created with the ip-router policy create aspath-regular-expression command.

Parameter	Value	Meaning
	<i><expression></i>	Specifies a regular expression. Enclose the regular expression in quotes.
origin	<i><origin></i>	Specifies the origin that matches the origin attribute of exported routes. Specify one of the following:
	any	Origin attribute can be EGP, EGP, or INCOMPLETE.
	egp	Origin attribute is EGP.
	igp	Origin attribute is IGP.
	incomplete	Origin attribute is INCOMPLETE.
tag	<i><number></i>	Restricts selection of routes to those identified by a tag.
preference	<i><number></i>	Specifies the preference to assign to the contributing routes.
restrict		Indicates that these routes cannot contribute to the aggregate.

Restrictions

None.

ip-router policy create aspath-export-source

Mode

Configure

Format

```
ip-router policy create aspath-export-source <number-or-string> <option-list>
```

Description

This command creates an export source where routes to be exported are identified by the autonomous system path associated with them. This command applies only if you are using BGP.

Parameter	Value	Meaning
aspath-export-source	<number-or-string>	Specifies a name or number for the Autonomous System path export source.
<option-list>		Specifies the Autonomous System path source options you are setting. Specify one of the following:
protocol	<name>	Specifies the protocol by which the routes to be exported were learned. Specify one of the following:
	all	All protocols.
	static	Static routes.
	direct	Direct routes.
	aggregate	Aggregate routes.
	rip	RIP routes.
	ospf	OSPF routes.
	bgp	BGP routes.
	isis	IS-IS routes.
aspath-regular-expression	<identifier>	Specifies either a regular expression or the identifier of the AS path regular expression list that must be satisfied for the route to be exported. The AS path regular expression list and its identifier must have previously been created with the ip-router policy create aspath-regular-expression command.
	<expression>	Specifies a regular expression. Enclose the regular expression in quotes.

Parameter	Value	Meaning
origin	<string>	Specifies whether the origin of the routes to be exported was an interior gateway protocol or an exterior gateway protocol. Specify one of the following:
	any	Any protocol.
	igp	Interior gateway protocol.
	egp	Exterior gateway protocol.
	incomplete	Incomplete route origin.
metric	<num>	Specifies metric associated with the exported routes.
restrict		Specifies that nothing is exported from the specified source.
 Note You can specify metric or restrict even if you specified protocol, aspath-regular-expression, or origin.		
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy create aspath-regular-expression

Mode
Configure

Format

ip-router policy create aspath-regular-expression <identifier> <regexp>

Description

This command creates an AS path regular expression list and associates an identifier (tag) with it. You can specify an AS path regular expression list for matching routes that are to be exported. The **ip-router policy create aspath-regular-expression** command allows you to create the list and assign an identifier to it. Once the list is created, you can add additional AS path regular expressions to the list with the **ip-router policy add aspath-regular-expression** command. You can then specify the list identifier for matching routes with the **ip-router policy** and **route-map** commands.

Parameter	Value	Meaning
aspath-regular-expression	<identifier>	Specifies the identifier of the AS path regular expression list. The identifier can be a number or a string.
	<regexp>	Specifies the AS path regular expression to be used to match the AS path. Enclose the regular expression in quotes.

Restrictions

None.

Example

The following example creates an AS path regular expression list named 'ncRoutes' that specifies AS paths that start with AS numbers 61000 or 62000:

```
rs(config)# ip-router policy create aspath-regular-expression ncRoutes
"((61000.*)|(62000.*))"
```

ip-router policy create bgp-export-destination Mode

Configure

Format

```
ip-router policy create bgp-export-destination <number-or-string> <option-list>
```

Description

This command creates an export destination for BGP routes.

Parameter	Value	Meaning
bgp-export-destination	<number-or-string>	Creates a BGP export destination and associates an identifier (tag) with it.
<option-list>		Specifies the BGP export destination options you are setting. Specify the following:
autonomous-system	<num>	Specifies the autonomous system of the peer-group to which we would be exporting. Specify a number from 1 to 65535.
optional-attribute-list	<num-or-string>	Specifies the identifier of the optional-attribute-list which contains the optional attributes which are to be sent along with these exported routes. This option may be used to send the BGP community attribute. Any communities specified in the optional-attributes-list are sent in addition to any received with the route or those specified with the 'set peer-group' or 'set peer-host' commands.
metric	<num>	Specifies the metric to be associated with the BGP exported routes.
peer-host	<ipaddr>	Specifies the IP address of the BGP peer host to which we would be exporting.
peer-group	<number-or-string>	Specifies the name of the BGP peer group to which we would be exporting.
restrict		Restricts the export of BGP routes to the specified destination.
sequence-number	<num>	Specifies the relative position of this export-destination in a list of bgp export-destinations.
community-add	<number-or-string>	Specifies the community to be added.
community-delete	<number-or-string>	Specifies the community to be deleted.

Restrictions

The following options will not have any effect if you are using this **bgp-export-destination** command in an export policy along with route-map: **optional-attribute-list**, **metric**, **restrict**.

ip-router policy create bgp-export-source

Mode

Configure

Format

```
ip-router policy create bgp-export-source <number-or-string> <option-list>
```

Description

This command creates a source for exporting BGP routes into other protocols.

Parameter	Value	Meaning
bgp-export-source	<number-or-string>	Creates a BGP export source and associates an identifier (tag) with it.
<option-list>		Specifies the BGP export source options you are setting. Specify the following:
autonomous-system	<num>	Specifies the autonomous system of the peer-group from which we would be exporting. A route filter could alternatively be used to explicitly list a set of routes to be accepted. Specify a number from 1 to 65535.
metric	<num>	Specifies the metric to be associated with the BGP exported routes.
peer-group	<number-or-string>	Specifies the identifier (tag) of the BGP peer group from which we would be exporting. You can also specify a route filter (created with the ip-router policy create filter command).
peer-host	<ipaddr>	Specifies the IP address of the BGP peer host from which we would be exporting. You can also specify a route filter (created with the ip-router policy create filter command).
restrict		Restricts the export of BGP routes from the specified source.
protocol	<protocol>	Specifies the protocol attribute of the routes to be exported. Specify one of the following:
	all	Specifies that the protocol attribute can be any one of static, direct, aggregate, rip, ospf, and bgp.
	static	Specifies that the protocol attribute is static.
	direct	Specifies that the protocol attribute is direct.

Parameter	Value	Meaning
	aggregate	Specifies that the protocol attribute is aggregate.
	rip	Specifies that the protocol attribute is RIP.
	ospf	Specifies that the protocol attribute is OSPF.
	bgp	Specifies that the protocol attribute is BGP.
aspath-regular-expression	<identifier>	Specifies either an expression or the identifier of the AS path regular expression list that must be satisfied for the route to be exported. (The AS path regular expression list and its identifier must have previously been created with the ip-router policy create aspath-regular-expression command.)
	<expression>	Specifies a regular expression. Enclose the regular expression in quotes.
origin	<value>	Specifies the origin attribute. Specify one of the following:
	any	Specifies that the origin attribute can be any one of igp, egp and incomplete.
	igp	Specifies that the origin attribute of the imported routes is IGP.
	egp	Specifies that the origin attribute of the imported routes is EGP.
	incomplete	Specifies that the origin attribute of the imported routes is incomplete.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

The following options will not have any effect if you are using this **bgp-export-destination** command in an export policy along with route-map: **metric, restrict**.

ip-router policy create bgp-import-source

Mode

Configure

Format

```
ip-router policy create bgp-import-source <number-or-string> <option-list>
```

Description

This command creates a source for importing BGP routes.

Parameter	Value	Meaning
bgp-import-source	<number-or-string>	Creates a BGP import source and associates an identifier (tag) with it.
<option-list>		Specifies the BGP import source options you are setting. Specify the following:
peer-group	<number-or-string>	Specifies the identifier (tag) of the BGP peer group from which we would be importing. You can also specify a route filter (created with the ip-router policy create filter command)
peer-host	<ipaddr>	Specifies the IP address of the BGP peer host from which we would be importing. You can also specify a route filter (created with the ip-router policy create filter command)
autonomous-system	<num>	Specifies the autonomous system of the peer-group from which we would be exporting. A route filter could alternatively be used to explicitly list a set of routes to be accepted. Specify a number from 1 to 65535.
aspath-regular-expression	<identifier>	Specifies either a regular expression or the identifier of the AS path regular expression list that must be satisfied for the route to be exported. The AS path regular expression list and its identifier must have previously been created with the ip-router policy create aspath-regular-expression command.
	<expression>	Specifies a regular expression. Enclose the regular expression in quotes.
origin	<value>	Specifies the origin attribute. Specify one of the following:

Parameter	Value	Meaning
	any	Specifies that the origin attribute can be any one of igp, egp and incomplete.
	igp	Specifies that the origin attribute of the imported routes is IGP.
	egp	Specifies that the origin attribute of the imported routes is EGP.
	incomplete	Specifies that the origin attribute of the imported routes is incomplete.
optional-attribute-list	<num-or-string>	Specifies the identifier of the optional-attribute-list. This option allows the specification of import policy based on the path attributes found in the BGP update. If multiple communities are specified in the aspath-opt option, only updates carrying all of the specified communities will be matched. If none is specified, only updates lacking the community attribute will be matched.
preference	<num>	Specifies the preference to be associated with the BGP imported routes.
restrict		Specifies that nothing is exported from the specified source.
sequence number	<num>	Indicates the position this import source will have in a list of BGP import sources.

Restrictions

The following options do not have any effect if you use this command in an import policy along with the **route-map** command: **origin**, **optional-attribute-list**, **preference**, **restrict**.

ip-router policy create community-list

Mode

Configure

Format

```
ip-router policy create community-list <number-or-string> <community-string>
```

Description

This command creates a community list. These community lists can be used in the **route-map** command to match a set of communities.

Parameter	Value	Meaning
community-list	<number-or-string>	Specifies the identifier of the community list.
<community-string>		Quoted string of communities like "a:b c:d" where a,c are the AS portion of a community split and b,d are the community identifier portion of a community split. You can also specify the following keywords for well-known communities:
	no-export	A special community that indicates the routes associated with this attribute must not be advertised outside a BGP confederation boundary. Since the RS's implementation does not support confederations, this boundary is an AS boundary.
	no-advertise	A special community indicating that the routes associated with this attribute must not be advertised to other BGP peers.
	no-export-subconfed	A special community indicating the routes associated with this attribute must not be advertised to external BGP peers. (This includes peers in other members' autonomous systems inside a BGP confederation.)

Restrictions

None.

Example

The following example creates a community list named 'comm':

```
rs(config)# ip-router policy create community-list comm "4:56 no-export"
```

ip-router policy create direct-export-source

Mode

Configure

Format

```
ip-router policy create direct-export-source <number-or-string> [interface  
<name-or-IPaddr>][metric <num>|restrict] [sequence-number <number>]
```

Description

This command creates an export source for interface routes.

Parameter	Value	Meaning
direct-export-source	<number-or-string>	Creates a source for exporting direct routes and associates an identifier with it.
interface	<name-or-IPaddr>	This option qualifies that the direct routes should be associated with the specific interface.
metric	<num>	Specifies the metric to be associated with the exported routes.
restrict		Restricts the export of routes from the specified source.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy create filter

Mode

Configure

Format

```
ip-router policy create filter <number-or-string> network <ipAddr/mask>  
[exact|refines|between <low-high>][host-net] [restrict]
```

Description

This command creates a route filter. Routes are filtered by specifying a set of filters that will match a certain set of routes by destination, or by destination and mask.

Parameter	Value	Meaning
filter	<number-or-string>	Specifies the identifier of the route filter.
network	<IP-address>	This option specifies networks which are to be filtered. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be filtered are specified, then any destination that falls in the range implied by this network specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact , refines , or between parameters, the mask of the destination is also considered.
exact		This option specifies that the mask of the routes to be filtered must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		This option specifies that the mask of the routes to be filtered must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
host-net		This option qualifies that the specified network is a host. To match, the address must exactly match the specified and the network mask must be a host mask (i.e. all ones). This is equivalent to a network specification of host/255.255.255.255 along with the exact option.
restrict		Specifies that routes that match the filter are not exported.

Restrictions

None.

ip-router policy create isis-export-destination Mode

Configure

Format

```
ip-router policy create isis-export-destination <number-or-string> level 1|2  
sequence-number <num> metric <num>|restrict
```

Description

This command creates an IS-IS export destination and associates an identifier to it.

Parameter	Value	Meaning
isis-export-destination	<number-or-string>	Specifies the identifier (either a number or a character string) for the IS-IS export destination. Specify any number or character string.
level	1 2	Specifies the level of the IS-IS export destination. Default value is level 1.
sequence-number	<num>	Specifies where this export destination will be positioned in the IS-IS export destinations list. Specify any number.
metric	<num>	Specifies the metric to be associated with the exported IS-IS routes. Specify any number between 1 and 16777214.
restrict		Restricts any exporting to the specified destination.

Restrictions

None.

ip-router policy create isis-export-source

Mode

Configure

Format

```
ip-router policy create isis-export-source <number-or-string> metric <num>|restrict  
[sequence-number <num>]
```

Description

This command creates an IS-IS export source and associates an identifier to it.

Parameter	Value	Meaning
isis-export-source	<number-or-string>	Specifies the identifier (either a number or a character string) for the IS-IS export destination. Specify any number or character string.
metric	<num>	Specifies the metric to be associated with the exported IS-IS routes. Specify any number equal to or greater than 0.
restrict		Restricts any exporting from the specified source.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations. Specify any number.

Restrictions

None.

ip-router policy create optional-attributes-list Mode

Configure

Format

```
ip-router policy create optional-attributes-list <number-or-string> <option-list>
```

Description

This command creates an optional-attributes-list for BGP.

Parameter	Value	Meaning
optional-attributes-list	<number-or-string>	Specifies the identifier for the attributes list.
<option-list>		Specifies the options you are setting. Specify the following:
community-id	<number>	Specifies a community identifier portion of a community split. This is combined with the autonomous system value entered to create a value for the community attribute.
autonomous-system	<number>	Specifies the autonomous system portion of a community split. This would be combined with the community id value entered to create a value for the community attribute. Specify a number from 1 to 65535.
well-known-community		Specifies one of the well-known communities. Specify one of the following keywords:
	no-export	Specifies that all routes received with this attribute value will not be advertised outside a BGP confederation boundary.
	no-advertise	Specifies that all routes received with this attribute value will not be advertised to other BGP peers.
	no-export-subconfed	Specifies that all routes received with this attribute value will not be advertised to external BGP peers (this includes peers in other members autonomous systems inside a BGP confederation)

Parameter	Value	Meaning
none		Specifies that routes received are only matched if no communities are present.
reserved-community	<number>	Specifies one of the reserved communities which is not well-known. A reserved community is one which is in one of the following ranges (0x00000000 - 0x0000FFFF) or (0xFFFF0000 - 0xFFFFFFFF).

Restrictions

None.

ip-router policy create ospf-export-destination

Mode

Configure

Format

```
ip-router policy create ospf-export-destination <number-or-string> [tag <num>][type  
1|2][metric <num>|restrict]
```

Description

This command creates a destination for exporting routes into OSPF.

Parameter	Value	Meaning
ospf-export-destination	<number-or-string>	Creates an OSPF export destination and associates an identifier with it.
tag	<num>	Tag to be associated with exported OSPF routes.
type	1 2	Specifies that OSPF routes to be exported are type 1 or type 2 ASE routes. Specify 1 or 2.
metric	<num>	Specifies the metric to be associated with the exported routes.
restrict		Restricts the export of the specified routes.

Restrictions

It is not possible to create OSPF intra- or inter-area routes by exporting routes from the routing table into OSPF. You can only export from the routing table into OSPF ASE routes.

ip-router policy create ospf-export-source

Mode

Configure

Format

```
ip-router policy create ospf-export-source <number-or-string> [type ospf|ospf-ase][metric <num>|restrict][sequence-number <number>]
```

Description

This command creates a source for exporting OSPF routes into other protocols.

Parameter	Value	Meaning
ospf-export-source	<number-or-string>	Creates an OSPF export source and associates an identifier with it.
type	ospf	Exported routes are OSPF routes.
type	ospf-ase	Exported routes are OSPF ASE routes.
metric	<num>	Specifies the metric to be associated with the exported routes.
restrict		Specifies that nothing is to be exported from this source.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy create ospf-import-source

Mode

Configure

Format

```
ip-router policy create ospf-import-source <number-or-string> [tag <num>][preference <num>|restrict]
```

Description

This command creates a source for importing OSPF routes.

Parameter	Value	Meaning
ospf-import-source	<number-or-string>	Creates an OSPF import source and associates an identifier with it.
tag	<num>	Tag to be associated with the imported routes.
preference	<num>	Preference associated with the imported OSPF routes.
restrict		Specifies that matching ospf-ase routes are not imported.

Restrictions

None.

ip-router policy create rip-export-destination **Mode**

Configure

Format

```
ip-router policy create rip-export-destination <number-or-string>  
[interface <name-or-IPaddr>|gateway <name-or-IPaddr>] [metric <num>|restrict]
```

Description

This command creates a destination for exporting routes into RIP.

Parameter	Value	Meaning
rip-export-destination	<number-or-string>	Specifies an identifier for the RIP export destination.
interface	<name-or-IPaddr> all	Specifies router interfaces over which to export routes. Specify all to export routes to all interfaces.
gateway	<name-or-IPaddr>	Specifies the gateway that will receive the exported routes.
metric	<num>	Specifies the metric to be associated with the exported routes. Specify a number from 1 – 16.
restrict		Restricts the export of routes to the specified destination.

Restrictions

None.

ip-router policy create rip-export-source

Mode

Configure

Format

```
ip-router policy create rip-export-source <number-or-string> [interface  
<name-or-IPaddr>|gateway <name-or-IPaddr>][metric <num>|restrict][sequence-number  
<number>]
```

Description

This command creates a source for exporting RIP routes into other protocols.

Parameter	Value	Meaning
rip-export-source	<number-or-string>	Specifies an identifier for the RIP export source.
interface	<name-or-IPaddr>	Indicates that only routes learned over specified interfaces are exported.
gateway	<name-or-IPaddr>	Indicates that only routes learned over specified gateways are exported.
metric	<num>	Specifies the metric to be associated with the exported routes.
restrict		Indicates that nothing is exported from the specified source.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy create rip-import-source

Mode

Configure

Format

```
ip-router policy create rip-import-source <number-or-string>  
[interface <name-or-IPaddr>|gateway <name-or-IPaddr>][preference <num>|restrict]
```

Description

This command creates a source for importing RIP routes.

Parameter	Value	Meaning
rip-import-source	<number-or-string>	Specifies an identifier for the RIP import source.
interface	<name-or-IPaddr>	Indicates that only routes learned over specified interfaces are imported.
gateway	<name-or-IPaddr>	Indicates that only routes learned over specified gateways are imported.
preference	<num>	Specifies the preference to be associated with the imported routes.
restrict		Indicates that nothing is imported from the specified source.

Restrictions

None.

ip-router policy create static-export-source

Mode

Configure

Format

```
ip-router policy create static-export-source <number-or-string>  
[interface <name-or-IPaddr>][metric <num>|restrict][sequence-number <number>]
```

Description

This command creates a source for exporting static routes into other protocols.

Parameter	Value	Meaning
static-export-source	<number-or-string>	Creates a source for exporting <i>static</i> routes and associates an identifier with it.
interface	<name-or-IPaddr>	This option qualifies that the <i>static</i> routes should be associated with the specific interface.
metric	<num>	Specifies the metric to be associated with the exported routes.
restrict		Restricts the export of routes from the specified source.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy create tag-export-source

Mode

Configure

Format

```
ip-router policy create tag-export-source <number-or-string>  
protocol all|static|direct|aggregate|rip|ospf|bgp [tag <number>][metric  
<number>|restrict][sequence-number <number>]
```

Description

This command creates an export source where routes to be exported are identified by the tag associated with them.

Parameter	Value	Meaning
tag-export-source	<number-or-string>	Specifies the identifier of an tag-export source.
protocol	<string>	Specifies the protocol of the contributing source. Specify one of the following:
	all	All protocols.
	static	Static routes.
	direct	Direct routes.
	aggregate	Aggregate routes.
	rip	RIP routes.
	ospf	OSPF routes.
	bgp	BGP routes.
tag	<number>	Restricts selection of routes to those identified by a tag.
metric	<number>	Specifies the metric to assign to the exported routes.
restrict		Indicates that the matching routes are not exported.
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

None.

ip-router policy export destination

Mode

Configure

Format

```
ip-router policy export destination <exp-dest-id> [source <exp-src-id> [route-map
<route-map-id>][sequence <seq-num>][filter <filter-id>|[network <ipAddr/mask>
[exact|refines|between <low-high>] [metric <number>|restrict]]]]
```

Description

This command creates an export policy from the various building blocks.

Parameter	Value	Meaning
destination	<exp-dest-id>	Is the identifier of the export-destination which determines where the routes are to be exported. If no routes to a particular destination are to be exported, then no additional parameters are required.
source	<exp-src-id>	If specified, is the identifier of the export-source which determines the source of the exported routes. If a export-policy for a given export-destination has more than one export-source, then the <i>ip-router policy export destination</i> <exp-dest-id> command should be repeated for each <exp-src-id>.
route-map	<route-map-id>	If specified, is the identifier of the route-map associated with this export policy. Only one route-map can be specified for an export source and export-destination combination. The route-map parameter is only supported if one or more of the export destinations or sources is BGP. All conditions can be specified in this route-map.
sequence	<seq-num>	Is the sequence in which the route map is applied.
filter	<filter-id>	If specified, is the identifier of the route-filter associated with this export-policy. If there is more than one route-filter for any export-destination and export-source combination, then the <i>ip-router policy export destination</i> <exp-dest-id> <i>source</i> <exp-src-id> command should be repeated for each <filter-id>.

Parameter	Value	Meaning
network	<ipAddr/mask>	Specifies networks which are to be exported. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be exported are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact , refines , or between parameters, the mask of the destination is also considered.
exact		This option specifies that the mask of the routes to be exported must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		This option specifies that the mask of the routes to be exported must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
metric	<number>	Specifies the metric to be associated with the routes that match the specified filter.
restrict		Specifies that routes matching the filter are not to be exported.

Restrictions

None.

ip-router policy import source

Mode

Configure

Format

```
ip-router policy import source <imp-src-id> [route-map <route-map-id>] [sequence
<seq-num>][filter <filter-id>][network <ipAddr/mask> [exact|refines|between <low-high>]
[preference <number>|restrict]]]
```

Description

This command creates an import policy.

Parameter	Value	Meaning
source	<imp-src-id>	Is the identifier of the import-source that determines the source of the imported routes. If no routes from a particular source are to be imported, then no additional parameters are required.
route-map	<route-map-id>	If specified, is the identifier of the route-map associated with this import policy. Only one route-map can be specified for an import source. The route-map parameter is only supported if the import source is BGP. All conditions can be specified in this route-map.
sequence	<seq-num>	Is the sequence in which the route map is applied.
filter	<filter-id>	If specified, is the identifier of the route-filter associated with this import-policy. If there is more than one route-filter for any import-source, then the ip-router policy import source <imp-src-id> command should be repeated for each <filter-id>.
network	<ipAddr/mask>	Specifies networks which are to be imported. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be imported are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact , refines , or between parameters, the mask of the destination is also considered.
exact		This option specifies that the mask of the routes to be imported must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.

Parameter	Value	Meaning
refines		This option specifies that the mask of the routes to be imported must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
restrict		Specifies that routes matching the filter are not to be imported.
preference	<number>	Specifies the preference with which the imported routes that match the specified filter should be installed.

Restrictions

None.

ip-router policy redistribute

Mode

Configure

Format

```
ip-router policy redistribute from-proto <protocol> [preference
<number>|internal|external] to-proto <protocol> [route-map <route-map-id>]
[route-map-sequence <seq-num>] [network <ipAddr/mask> [exact|refines|between <low-high>]]
[metric <number>|restrict] [source-as <number>] [target-as <number>] [tag]
[ase-type][sequence-number <number>]
```

Description

This command creates a simple route redistribution policy.

Parameter	Value	Meaning
from-proto	<protocol>	Specifies the protocol of the source routes. The values for the from-proto parameter are aggregate , any bgp , direct , isis-level-1 , isis-level-2 , ospf , ospf-ase , rip , or static .
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.
preference	<number> internal external	If specified, is the metric to be associated with routes that match the filter. Specify internal or external to have the route inherit the metric from the IGP route of the next hop.
to-proto	<protocol>	Specifies the destination protocol where the routes are to be exported. The values for the to-proto parameter are rip , ospf , bgp , isis-level-1 , isis-level-2 , or ospf-nssa .
route-map	<route-map-id>	If specified, is the identifier of the route-map associated with this policy. Only one route-map can be specified for a distribution policy. The route-map parameter is only supported if BGP is the protocol for at least one from-proto or to-proto parameter. All conditions can be specified in this route-map.
route-map-sequence	<seq-num>	Is the sequence in which the route map is applied.

Parameter	Value	Meaning
network	<ipAddr/mask>	Provides a means to define a filter for the routes to be distributed. The network parameter defines a filter that is made up of an IP address and a mask. Routes that match the filter are considered as eligible for redistribution. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be redistributed are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact, refines, or between parameters, the mask of the destination is also considered.
exact		This option specifies that the mask of the routes to be redistributed must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		This option specifies that the mask of the routes to be redistributed must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
restrict		Specifies that routes matching the filter are not to be redistributed.
source-as	<number>	Specifies the AS of the peer group from which BGP routes are exported. This value has a range of from 1 to 65535.
target-as	<number> all	Specifies the AS of the peer group to which BGP routes are exported. If you specify all , BGP routes are exported to all autonomous systems. This value has a range of from 1 to 65535.
metric	<number> internal	Indicates the metric to be associated with the redistributed routes. Specify internal for BGP to advertise a MED that corresponds to the IGP metric associated with the NEXT HOP of the route. If you specify internal , multiple BGP speakers in the same AS can advertise different MEDs for a particular prefix. Note that if the IGP metric changes, BGP does not readvertise the route.
tag		Tag to be associated with the exported OSPF routes.

Parameter	Value	Meaning
ase-type		Routes exported from the ROSRD routing table into OSPF default to becoming type 1 ASEs. This default may be explicitly overridden here. Thus, this option should be used to specify if the routes are to be exported as OSPF Type 1 or Type 2 ASE routes.
 Note Each protocol (RIP, OSPF, and BGP) has a configurable parameter that specifies the default-metric associated with routes exported to that protocol. If a metric is not explicitly specified with the redistribute command, then it is inherited from the default-metric associated with the protocol to which the routes are being exported.		
sequence-number	<number>	Specifies the position of this export source in the list of configured export destinations.

Restrictions

The following options do not have any effect if you use the **route-map** option in this redistribution policy: **network, tag, ase-type, metric, restrict**.

ip-router policy summarize route

Mode

Configure

Format

```
ip-router policy summarize route <ipAddr/mask> | default [from-network  
<ipAddr/mask>][exact | refines | between <low-high>][preference  
<number>|restrict][source-proto <protocol>] [type aggregate|generation] [brief]
```

Description

This command creates a simple aggregate or generation.

Parameter	Value	Meaning
route	<ipAddr/mask> default	The summarized network. Specify default for default networks.
from-network	<ipAddr/mask>	Specifies the network to be summarized. If no additional options that qualify the networks to be filtered are specified, then any destination that falls in the range implied by this network specification is matched; the mask of the destination is ignored. If a natural network is specified, the network and any subnets and any hosts will be matched.
exact		Specifies that the mask of the routes to be summarized must match the supplied mask exactly. This is used to match a network, but no subnets or hosts of that network.
refines		Specifies that the mask of the routes to be summarized must be more specific (i.e., longer) than the supplied mask. This is used to match subnets and/or hosts of a network, but not the network.
between	<low-high>	Specifies that the mask of the routes to be summarized must be as or more specific (i.e., as long as or longer) than the lower limit (the first number value) and no more specific (i.e., as long as or shorter) than the upper limit (the second number value).
preference	<number>	If specified, is the metric to be associated with the routes that match the filter.
restrict		If specified, routes that match the filter are not to be summarized.
source-proto	<protocol>	Specifies the protocol of the source routes. Specify one of the following:
	all	All protocols.

Parameter	Value	Meaning
	bgp	BGP routes.
	direct	Direct routes.
	isis-level-1	IS-IS level 1 routes.
	isis-level-2	IS-IS level 2 routes.
	ospf	OSPF routes.
	rip	RIP routes.
	static	Static routes.
type	aggregate generation	Specifies whether the object being created is an aggregate or a generation.
brief		Specifies that the AS path is to be truncated to the longest common AS path. The default is to build an AS path that consists of SETs and SEQUENCES of all contributing AS paths.

Restrictions

None.

ip-router show configuration file

Mode

Enable

Format

```
ip-router show configuration-file active|permanent
```

Description

This command displays the active or startup configuration file in GateD format.

Parameter	Value	Meaning
active		Shows the active configuration file in RAM; this is the default.
permanent		Shows the permanent configuration file in NVRAM, if available.

Restrictions

None.

ip-router show rib

Mode

Enable

Format

```
ip-router show rib [detail [show-all-info]]
```

Description

The **ip-router show rib** command shows the route-manager's routing information base (RIB). For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) sign next to it. If a route has been the last active route and is also the current active route, then it is shown with an asterisk (*) sign next to it. The legend is as follows:

- “+” Active Route
- “-” Last Active
- “*” Both

If the **detail** option is used, then additional information is displayed about these routes. The announcements bits for the active route are shown which shows the protocol into which this route is advertised.

Parameter	Value	Meaning
detail		Allows you to view additional information about the routes in the RIB.
show-all-info		Shows information about transmitting subscriber information (TSI) blocks for the RIB route.

Restrictions

None.

Examples:

A sample output of the **ip-router show rib** command is shown below:

```

rs# ip-router show rib
Routing Tables:
Generate Default: no
Destinations: 63776      Routes: 63776
Holddown: 0      Delete: 53811      Hidden: 1
Codes: Network - Destination Network Address
      S - Status + = Best Route, - = Last Active, * = Both
      Src - Source of the route :
      Ag - Aggregate, B - BGP derived, C - Connected
      R - RIP derived, St - Static, O - OSPF derived
      OE - OSPF ASE derived, D - Default
      Next hop - Gateway for the route ; Next hops in use: 4
      Netif - Next hop interface
      Prf1 - Preference of the route, Prf2 - Second Preference of the route
      Metrc1 - Metric1 of the route, Metrc2 - Metric2 of the route
      Age - Age of the route
Network/Mask      S Src Next hop      Netif Prf1 Metrc1 Metrc2      Age
-----
3/8               *   B 134.141.178.33      mls0  170              70:34:28
4/8               *   B 134.141.178.33      mls0  170              70:34:28
4.17.106/24       *   B 134.141.178.33      mls0  170              70:34:28
4.17.115/24       *   B 134.141.178.33      mls0  170              70:34:28
4.24.148.128/25   *   B 134.141.178.33      mls0  170              70:34:28
6/8               *   B 134.141.178.33      mls0  170              70:34:28
6.80.137/24       *   B 134.141.178.33      mls0  170              70:34:28
9.2/16            *   B 134.141.178.33      mls0  170              70:34:28
9.20/17           *   B 134.141.178.33      mls0  170              70:34:28
10.50/16          *   C 10.50.90.1           en     0      0      0 113:31:09
10.60.90/24       *   C 10.60.90.1           mls2   0      0      0 113:31:09
12/8              *   B 134.141.178.33      mls0  170              70:34:28
12.1.248/24       *   B 134.141.178.33      mls0  170              70:34:28

```

Table 31-1 Display field descriptions for the ip-router show rib command

FIELD	DESCRIPTION
Metric 1	A computation of cost. In OSPF, this is the cost of the link. In RIP, this is the hop count of the route.
Metric 2	In BGP, this is the multi-exit discriminator (MED). The MED specifies the preferred path into autonomous systems that have more than one entry point. Metric 2 carries from one protocol to the next when redistributing routes.

To see a specific route, use the **ip-router show route** command.

ip-router show route

Mode

Enable

Format

```
ip-router show route <ipaddr/mask>|default [detail] longer-prefixes
```

Description

This command shows a specific route in the route-manager's routing information base (RIB). For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) next to it. If a route has been the last active route and is also the current active route, then it is shown with an asterisk (*) sign next to it. The legend is as follows:

- “+” Active Route
- “-” Last Active
- “*” Both

If the detail option is used, then additional information is displayed about this routes. The announcements bits for the active route are shown which shows the protocol into which this route is advertised.

Parameter	Value	Meaning
route	<ipAddr/mask> default	Allows you to specify a particular IP address mask for the RIB route in question, or refer to the default address mask.
detail		Allows you to view additional information about the routes in the RIB.
	longer-prefixes	Displays all routes with subnet mask of that specified in <ip-addr/mask> and longer.

Restrictions

None.

Examples

A sample output of the **ip-router show route detail** command is shown below.

```
rs# ip-router show route 10.12.1.0/255.255.255.252 detail
10.12.1          mask 255.255.255.252
entries 2      announce 1
TSI:
RIP 150.1.255.255mc <> metric 1
RIP 222.1.1.255mc <> metric 1
BGP_Sync_64805 dest 10.12.1/2 metric 0
BGP group type Routing AS 64805 no metrics
Instability Histories:

*Direct      Preference: 0
*NextHop: 10.12.1.2      Interface: 10.12.1.2(to-c4500)
State: <Int Active Retain>
Age: 5:12:10      Metric: 0      Metric2: 0      Tag: 0
Task: IF
Announcement bits(5):
2-KRT 4-RIP.0.0.0.0+520 5-RIP.0.0.0.0+520
6-BGP_Sync_64805
7-BGP_Group_64805
AS Path: IGP (Id 1)

OSPF      Preference: -10
*NextHop: 10.12.1.1      Interface: 10.12.1.2(to-c4500)
State: <NotInstall NoAdvise Int Hidden Gateway>
Local AS: 64805
Age: 1:20:05      Metric: 1      Metric2: -1      Tag: 0
Task: OSPF
AS Path: (64805) IGP (Id 9551)
Cost: 1      Area: 0.0.0.0      Type: Net      AdvRouter:
172.23.1.14
```

In this case there two routes to network 10.12.1.0/255.255.255.252 One of them is a direct route and other route is learned through OSPF. The direct route has a better preference (lower preference is considered better preference), and is thus the active route. The direct route has been installed since 5 hours, 12 minutes and 10 seconds. This direct route is being announced to the Forwarding Information Base (FIB) which is indicated by KRT, over two RIP interfaces (which is indicated by 4-RIP.0.0.0.0+520, 5-RIP.0.0.0.0+520) and also to the BGP internal peer-group for autonomous system 64805.

To see all the routes in the RIB, use the **ip-router show rib** command.

ip-router show route-preferences

Mode

Enable

Format

```
ip-router show route-preferences
```

Description

The **ip-router show route-preferences** command displays the types of routes configured on the RS and the preference value associated with each route type. For example, direct, static, OSPF, OSPF ASE, ISIS level 1 and 2, RIP, and BGP external routes are displayed with their preference values.

Restrictions

None.

Example

A sample output of the **ip-router show route-preferences** command is shown below:

Route	Preferences:
-----	-----
Direct	0
Static	5
OSPF	10
ISIS L1	11
ISIS L2	151
Default	20
Router Discovery	55
RIP	100
DIRECT AGGREGATE	110
AGGREGATE	130
OSPF ASE	150
BGP EXT	99

ip-router show state

Mode
Enable

Format

```
ip-router show state [all] [memory] [timers] [task <string>|all|gii  
|icmp|inet|interface|krt |route]
```

Description

This command displays the state of ROSRD.

Parameter	Value	Meaning
all		Shows all ouput.
memory		Shows memory allocations.
timers		Shows various ROSRD timers.
task		Shows task-specific information. The default is to show information for all tasks. You can specify a task using the following options:
	<string>	Displays information for the task specified.
	all	Shows information for all tasks.
	gii	Shows GII information.
	icmp	Shows information for the ICMP task.
	inet	Shows information for the INET task.
	interface	Shows information for the interface task.
	krt	Shows information for the KRT task.
	route	Shows information for the route task.

Restrictions

None.

ip-router show summary

Mode

Enable

Format

ip-router show summary [drops]

Description

This command displays a summary of the routing information base. The **ip-router show summary** command shows a summary of the route-manager's routing information base (RIB). The **drops** parameter shows information about dropped RIB routes. To see the contents of the RIB, use the **ip-router show rib** command.

Parameter	Value	Meaning
summary	drops	Displays information about dropped RIB routes.

Restrictions

None.

Example

A sample output of the **ip-router show summary** command is shown below:

```
Summary of routes in RIB
-----
Number of Unique routes : 7
Number of routes       : 7
Kernel routes          : 0
Direct routes          : 2
Static routes          : 5
RIP routes              : 0
OSPF routes            : 0
OSPF ASE routes        : 0
ISIS level 1 routes    : 0
ISIS level 2 routes    : 0
BGP routes             : 0
Other Protocol routes  : 0
Hidden routes          : 0
```


32 IPX COMMANDS

The **ipx** commands let you add entries to the IPX SAP table for SAP servers and display the IPX forwarding database, RIP table, and SAP table.

32.1 COMMAND SUMMARY

The following table lists the **ipx** commands. The sections following the table describe the command syntax for each command.

<code>ipx add route <networkaddr> <nexttroutnextnode> <metric> <ticks></code>
<code>ipx add sap <type> <SvcName> <node> <socket> <metric> <interface-network></code>
<code>ipx find rip <address></code>
<code>ipx find sap <type> all <SvcName> all <network> all <entrytype></code>
<code>ipx l3-hash module <num> all variant <num></code>
<code>ipx set interface ifname <string> ipg <num> ripintvl <num> sapintvl <num></code>
<code>ipx set port forwarding-mode destination-based</code>
<code>ipx set rip buffers</code>
<code>ipx set ripreq buffers</code>
<code>ipx set sap buffers</code>
<code>ipx set sapgns buffers round-robin</code>
<code>ipx set type20 propagation</code>
<code>ipx show buffers</code>
<code>ipx show hash-variant <num> all</code>
<code>ipx show interfaces <interface> [brief]</code>
<code>ipx show rib <destination></code>
<code>ipx show servers hops net name type</code>
<code>ipx show tables routing rip sap summary</code>

ipx add route

Mode

Configure

Format

```
ipx add route <networkaddr> <nextroutnetnode> <metric> <ticks>
```

Description

The **ipx add route** command adds a route into the IPX RIP routing table.

Parameter	Value	Meaning
route	<networkaddr>	Destination network address in hexadecimal format.
	<nextroutnetnode>	Next router's address in <IPX-network-address>.<MAC-address> format.
	<metric>	The number of hops associated with this route. You can specify a number from 1-14.
	<ticks>	Ticks associated with this route. You can specify a number from 1-65535.

Restrictions

Route entries that you add using the **ipx add route** command override dynamically learned entries, regardless of hop count.

Example

To add an IPX route to IPX network A1B2C3F5 via router A1B2C3D4.00:E0:63:11:11:11 with a metric of 1 and a tick of 100:

```
rs(config)# ipx add route A1B2C3F5 A1B2C3D4.00:E0:63:11:11:11 1 100
```

ipx add sap

Mode

Configure

Format

```
ipx add sap <type> <SvcName> <node> <socket> <metric> <interface-network>
```

Description

The **ipx add sap** command adds an entry for an IPX server to the IPX SAP table.

Parameter	Value	Meaning
sap	<type>	The type of service. Specify the service type using its hexadecimal value.
	<SvcName>	Name of the IPX server. You can use any characters in the name except the following: " * . / : ; < = > ? [] \]
 Note Lowercase characters are changed to uppercase characters.		
	<node>	The IPX network and node address. Specify the address in the following format: <netaddr> . <macaddr>. Example: a1b2c3d4.aa:bb:cc:dd:ee:ff.
	<socket>	The socket number for this SAP entry. You can specify a Hexadecimal number from 0x0 – 0xFFFF.
	<metric>	The number of hops to the server. You can specify a number from 1 – 14.
	<interface-network>	The interface network associated with this SAP entry.

Restrictions

SAP entries that you add using the **ipx add sap** command override dynamically learned entries, regardless of hop count. Moreover, if a dynamic route entry that is associated with the static SAP entry ages out or deleted, the RS does not advertise the corresponding static SAP entries for the service until it relearns the route.

ipx find rip

Mode

Enable

Format

```
ipx find rip <address>
```

Description

The **ipx find rip** command searches for an IPX address in the routing table.

Parameter	Value	Meaning
rip	<address>	The IPX network address of this interface. Specify the IPX address using its hexadecimal value.

Restrictions

None.

Example

To find an IPX network in the route table:

```
rs(config)# ipx find rip A1B2C3F5
```

ipx find sap

Mode

Enable

Format

```
ipx find sap <type>|all <SvcName>|all <network>|all <entrytype>
```

Description

The **ipx find sap** command searches for a SAP entry in the routing table.

Parameter	Value	Meaning
sap	<type> all	The types of service. Specify the service type using its hexadecimal value. Specify all for all types of service.
	<SvcName> all	Name of the IPX service. You can use any characters in the name except the following: <code>"* . / : ; < = ? [] \ </code> . Specify all for all IPX services.
 Note Lowercase characters are changed to uppercase characters.		
	<netaddr> all	Network on which the service resides. Specify an IPX network address in a format like the following example: a1b2c3d4. Specify all for all networks.
	<entrytype>	The types of entry you want to find. Specify one of the following:
	all	Finds static and dynamic SAP entries.
	dynamic	Finds only the dynamic SAP entries.
	static	Finds only the static SAP entries.

Restrictions

None.

Example

To find a SAP entry in the route table:

```
rs(config)# ipx find sap 4 FILESERVER a2b2c3d4 dynamic
```

ipx l3-hash

Mode

Configure

Format

```
ipx l3-hash module <num>|all variant <num>
```

Description

The RS's L3 Lookup table is organized as a hash table. The hash function reduces the destination and source MAC addresses to 16-bit quantities each. The hashing algorithm generates a uniform distribution within the MAC address space. However, given a particular set of addresses, the distribution may cause addresses to clump together in the table. To minimize the risk of thrashing in the tables, three variations to the basic hashing algorithm are defined. Only one variation is in effect on a line card at any given time. You can use the **ipx l3-hash** command to set which variation is in effect for a line card.

Swizzling shifts the hash value by a certain amount of bits, producing more random distribution across the L3 lookup table.

Auto-hashing periodically queries the L2 or L3 tables for hash bucket overflow on a port. If there are more overflows than a certain threshold level, auto-hashing will automatically change the hash mode for that port. Eventually a 'best' hash mode for the particular traffic will be found, which will provide a more even distribution across the L2 or L3 lookup table.

Parameter	Value	Meaning
module	<num> all	Is a slot number on the RS. Specify any number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot. The all option causes the hashing algorithm to change on all ports on all slots.
variant	<num>	Causes a variation to the basic hashing algorithm to be made. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). If you specify 0, the default hashing algorithm is used.

Restrictions

None.

Example

To change the default hashing algorithm used for the L3 lookup table on all ports on slot 7:

```
rs(config)# ipx l3-hash module 7 variant 1
```


ipx set interface

Mode

Configure

Format

```
ipx set interface ifname <string> | ipg <num> | ripintvl <num> | sapintvl <num>
```

Description

The **ipx set interface** command sets the IPX interface parameters such as interface name, inter-packet gap, broadcast interval for RIP, and broadcast interval for SAP.

Parameter	Value	Meaning
ifname	<string>	Specify the interface name.
ipg	<num>	Specify the Inter Packet Gap (in milliseconds). Specify any number between 30 and 180.
ripintvl	<num>	Specify the broadcast interval for RIP (in seconds). Specify any number between 60 and 300.
sapintvl	<num>	Specify the broadcast interval for SAP (in seconds). Specify any number between 60 and 300.

Restrictions

None.

ipx set port

Mode

Configure

Format

```
ipx set port forwarding-mode destination-based
```

Description

The **ipx set port forwarding-mode destination-based** command sets up an IPX port to forward traffic based on the packet destination network, node, and socket.

Restrictions

None.

ipx set rip buffers

Mode

Configure

Format

```
ipx set rip buffers <buffer-size>
```

Description

The **ipx set rip buffers** command sets the RIP socket buffer size.

Parameter	Value	Meaning
buffers	<buffer-size>	Specify the socket buffer size in bytes.

Restrictions

None.

ipx set ripreq buffers

Mode

Configure

Format

```
ipx set ripreq buffers <buffer-size>
```

Description

The **ipx set ripreq buffers** command sets the buffers for RIP request packets.

Parameter	Value	Meaning
buffers	<buffer-size>	Size of the buffer in bytes.

Restrictions

None.

ipx set sap buffers

Mode

Configure

Format

ipx set sap buffers <*buffer-size*>

Description

The **ipx set sap buffers** comand sets the SAP socket buffer size.

Parameter	Value	Meaning
buffers	< <i>buffer-size</i> >	Specify the buffer size in bytes.

Restrictions

None.

ipx set sapgns

Mode

Configure

Format

```
ipx set sapgns [buffers <buffer-size>] [packets-per-iteration <num>] [round-robin]
```

Description

The **ipx set sapgns** command sets the following parameters for SAP get nearest server (GNS) packets:

Parameter	Value	Meaning
buffers	<buffer-size>	Specify the buffer size in bytes. Default is 64K.
packets-per-iteration	<num>	Number of SAP GNS packets processed per iteration. Default is 100.
round-robin		Sets a round-robin scheme for finding the nearest server.

Restrictions

None.

ipx set type20 propagation

Mode

Configure

Format

```
ipx set type20 propagation
```

Description

The **ipx set type20 propagation** command controls the propagation of type 20 packets.

Restrictions

None.

ipx show buffers

Mode

Enable

Purpose

Display the RIP and SAP socket buffer sizes.

Format

```
ipx show buffers
```

Description

The `ipx show buffers` command displays the RIP and SAP socket buffer sizes.

Restrictions

None.

ipx show hash-variant

Mode

Enable

Format

```
ipx show hash-variant <num>|all
```

Description

The **ipx show hash-variant** command displays hash variant information. There are a total of 16 modules using the hash variant feature (1-16).

Enabling hash variant causes a variation to the basic hashing algorithm. This variation will prevent clustering of hash values and will provide a more even distribution across the L3 lookup table. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). The default hashing algorithm is 0.

Swizzling shifts the hash value by a certain amount of bits, causing a more random distribution across the L3 lookup table. Auto-hashing allows the RS to auto-select a hashing algorithm optimized for 'best case' L3 table distribution.

Parameter	Value	Meaning
hash-variant	<num> all	Specifies the module. Specify any number between 1-16. Specify all to display hash variant information for all modules.

Restrictions

None.

Example

To display IPX hash variant information on all 16 modules:

```
rs# ipx show hash-variant all
```

IPX Module	Hash Variant
Module 2	variant-3
Module 3	variant-0
Module 4	variant-0
Module 5	variant-0
Module 6	variant-5
Module 7	variant-0
Module 8	variant-0
Module 9	variant-0
Module 10	variant-0
Module 11	variant-2
Module 12	variant-2
Module 13	variant-0
Module 14	variant-0
Module 15	variant-1

ipx show interfaces

Mode

Enable

Format

```
ipx show interfaces <interface> [brief]
```

Description

The **ipx show interfaces** command displays the configuration of an IPX interface. If you issue the command without specifying an interface name, then the configuration of all IPX interfaces is displayed.

Parameter	Value	Meaning
interfaces	<interface>	Name of the IPX interface; for example, i14.
brief		Shows a brief summary of the interface in tabular form.

Restrictions

If you specify an interface name, the name must belong to an existing IPX interface.

Example

To display the configuration of all IPX interfaces:

```
rs# ipx show interfaces
i12: flags=9863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,LINK0,MULTICAST>
      VLAN: _VLAN-1
      Ports: et.1.7
      IPX: A1B2C3D4.00:E0:63:11:11:11
i14: flags=9863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,LINK0,MULTICAST>
      VLAN: _VLAN-2
      Ports: et.1.2
      IPX: ABCD1234.00:E0:63:11:11:11
```

ipx show rib

Mode

User

Format

```
ipx show rib <destination>
```

Description

The **ipx show rib** command displays IPX RIP table output sorted by destination.

Parameter	Value	Meaning
rib	<destination>	Specifies the destination.

Restrictions

None.

ipx show servers

Mode

User

Format

```
ipx show servers hops|net|name|type
```

Description

The **ipx show servers** command displays IPX server information sorted by any or all of the optional arguments. Sorting is done based on the order of optional arguments given.

Parameter	Value	Meaning
servers	hops	Shows output sorted by hop count.
	name	Shows output sorted by SAP service name.
	net	Shows output sorted by network number.
	type	Shows output sorted by SAP service type.

Restrictions

None.

ipx show summary

Mode

User

Format

ipx show summary

Description

The **ipx show summary** command displays a summary of the IPX RIP/SAP table.

Restrictions

None.

33 ISIS COMMANDS

The **isis** commands let you display and set parameters for the Intermediate System-Intermediate System (IS-IS) routing protocol.

33.1 COMMAND SUMMARY

The following table lists the isis commands. The sections following the table describe the command syntax.

<code>isis add area <string></code>
<code>isis add interface <string> all</code>
<code>isis add label-switched-path <interface-name> <ipaddr></code>
<code>isis add summary-filt <ipAddr-mask></code>
<code>isis add summary-orig <ipAddr-mask> metric <number></code>
<code>isis set area-key-chain <string> authentication-method md5 none simple</code>
<code>isis set domain-key-chain <string> authentication-method md5 none simple</code>
<code>isis set domain-wide</code>
<code>isis set external-preference level-1 <number> level-2 <number></code>
<code>isis set igp-shortcuts enable</code>
<code>isis set interface <interface-name-or IPaddr> all <options></code>
<code>isis set level 1 2 1-and-2</code>
<code>isis set overload bit</code>
<code>isis set preference level-1 <number> level-2 <number></code>
<code>isis set psn-interval <number></code>
<code>isis set reference-bandwidth</code>
<code>isis set require-snp-auth</code>
<code>isis set spf-interval <number></code>
<code>isis set system-id <string></code>
<code>isis set traffic-engineering enable</code>

isis show adjacencies [detail]
isis show all
isis show circuits
isis show export-policies
isis show globals
isis show lsp-database level 1 2 [detail][id <string>]
isis show timers
isis start
isis stop
isis trace <options>

isis add area

Mode

Configure

Format

isis add area *<string>*

Description

The **isis add area** command allows you to define the IS-IS area to which the router will belong. A router can belong to only one area.

Parameter	Value	Meaning
area	<i><string></i>	Specifies the address for the IS-IS area. Specify an ISO address in a hexadecimal string that is from 3 through 13 bytes.

Restrictions

None.

Example

To add the area 49.0001.49.da02.0001.0002.0003:

```
rs(config)# isis add area 49.0001.49.da02.0001.0002.0003
```

isis add interface

Mode

Configure

Format

```
isis add interface <string>|all
```

Description

The **isis add interface** command allows you to enable the IS-IS routing protocol on an IP interface. When you enable IS-IS on an interface, the interface becomes part of the area in which the router is a member. All interfaces on a router belong to the same area.

Parameters

Parameter	Value	Meaning
interface	<string>	Specifies the name of the IP interface on which IS-IS will be enabled.
	all	Specify all to enable IS-IS on all interfaces.

Restrictions

None.

Example

To add the interface "int10:"

```
rs(config)# isis add int10
```

isis add label-switched-path

Mode

Configure

Format

isis add label-switched-path <interface-name> | <ipaddr>

Description

Associates a label switched path (LSP) with an IS-IS area.

Parameter	Value	Meaning
label-switched-path	<interface-name> <ipaddr>	Interface name or IP address.

Restrictions

None.

isis add summary-filt

Mode

Configure

Format

```
isis add summary-filt <ipAddr-mask>
```

Description

The **isis add summary-filt** command applies filters for the specified Level 2 routes.

The **isis set domain** wide command allows the propagation of Level 2 routes into the Level 1 domain. If you want to block certain Level 2 routes from being propagated throughout the Level 1 domain, you can do so using the **isis add summary-filt** command. You can add as many filters as needed.

Parameter	Value	Meaning
summary-filt	<ipAddr-mask>	Specify an IP address and mask.

Restrictions

None.

Example

To add the summary filter 25.1.1.1/16:

```
rs(config)# isis add summary-filt 25.1.1.1/16
```

isis add summary-orig

Mode

Configure

Format

```
isis add summary-orig <ipAddr-mask> metric <number>
```

Description

The **isis add summary-orig** command allows you to summarize Level 1 routes as a single IP address. This summarized address is used during communication with other Level 1-and-2 routers.

Parameter	Value	Meaning
summary-orig	<ipAddr-mask>	Specifies the IP address. Specify an IP address and mask.
metric	<number>	Specifies the metric or cost that corresponds to the IS-IS interface.

Restrictions

None.

isis set area-key-chain

Mode

Configure

Format

```
isis set area-key-chain <string> authentication-method md5|none|simple
```

Description

The **isis set area-key-chain** command specifies the authentication method. It applies to all interfaces in the area.

Parameter	Value	Meaning
area-key-chain	<string>	Identifies a key-chain which must have been previously created with the ip-router authentication create key-chain command.
authentication-method		Specify the authentication method to be used.
	md5	Use MD5 to create a crypto-checksum of a OSPF packet and an authentication key of up to 16 characters.
	none	No authentication method.
	simple	Specifies that the authentication-method is a simple password in which an authentication key of up to 16 characters is included in the packet.

Restrictions

None.

isis set domain-key-chain

Mode

Configure

Format

```
isis set domain-key-chain <string> authentication-method md5|none|simple
```

Description

The **isis set domain-key-chain** allows you to set an authentication method.

Parameter	Value	Meaning
domain-key-chain	<string>	Identifies a key-chain which must have been previously created with the ip-router authentication create key-chain command.
authentication-method		Specify the authentication method to be used.
	md5	Use MD5 to create a crypto-checksum of an IS-IS packet and an authentication key of up to 16 characters.
	none	No authentication method.
	simple	Specifies that the authentication-method is a simple password in which an authentication key of up to 16 characters is included in the packet.

Restrictions

None.

isis set domain-wide

Mode

Configure

Format

```
isis set domain-wide
```

Description

The **isis set domain-wide** command allows you to propagate the Level 2 routes to Level 1 routers.

Restrictions

None.

isis set external-preference

Mode

Configure

Format

isis set external-preference level-1 <number>|level-2 <number>

Description

The **isis set external-preference** command sets the preference of routes exported into IS-IS with external metrics.

Parameter	Value	Meaning
level-1	<number>	Specifies the external route preference for Level 1.
level-2	<number>	Specifies the external route preference for Level 2.

Restrictions

None.

Example

To specify an external route preference of "10" for Level 1:

```
rs(config)# isis set external-preference level-1 10
```

isis set igp-shortcuts

Mode

Configure

Format

```
isis set igp-shortcuts enable
```

Description

The **isis set igp-shortcuts** command allows you to use label switched paths (LSPs) as IGP shortcuts.

Parameter	Value	Meaning
enable		Enables use of LSPs as IGP shortcuts.

Restrictions

None.

Example

To use LSPs as IGP shortcuts:

```
rs(config)# isis set igp-shortcuts enable
```

isis set interface

Mode

Configure

Format

```
isis set interface <interface-name-or IPaddr> |all <options>
```

Description

The **isis set interface** command allows you to define operating parameters for an IS-IS interface.

metric <number>

Parameter	Value	Meaning
interface	<interface-name-or IPaddr> all	Identifies the interface. Specify either the name of the interface or its IP address or specify all for all interfaces.
level		Sets the IS-IS level at which the interface will operate. The operating level of the interfaces should be synchronized with the operating level of the router. (This is set through the isis set level command.) For example, if the router's IS-IS level is 1, then its interfaces should be set to level 1. (If you set an interface to level 2, that interface will be unable to pass IS-IS traffic.) But if some of the interfaces will be set at level 1 and some will be set at level 2, then the RS level should be set to level 1-and-2.
	1	Sets the IS-IS operating level to level 1.
	2	Sets the IS-IS operating level to level 2.
	1-and-2	Sets the IS-IS operating level to level 1 and 2.
metric	<number>	Sets the cost for the interface. Enter a value between 1 and 63, inclusive. (Default: 10)
priority	<number>	Sets the priority of the interface during the election of the Designated Intermediate System (DIS). Enter a value between 1 and 127, inclusive. (Default: 64)
hello-interval	<number>	Sets the interval at which hello packets are sent on the circuit. Enter a value between 1 and 300, inclusive. (Default: 10)
dis-hello-interval	<number>	Sets the hello-interval used if the router becomes the DIS. Enter a value between 1 and 100, inclusive. (Default: 3)

Parameter	Value	Meaning
hello-multiplier	<number>	Sets the number of hello-intervals a router must wait to receive the next Hello packet before the router determines the neighboring IS is down. Enter a value between 1 and 100, inclusive. (Default: 3)
csn-interval	<number>	Sets the interval (in seconds) at which the router will multicast Complete Sequence Number PDUs (CSNPs), if the router becomes the DIS. Enter a value between 1 and 100, inclusive. (Default: 10)
lsp-interval	<number>	Sets the interval between the generation of Link State PDUs (LSPs). LSPs contain information about the identity and routing metric values of the adjacencies of this IS. Enter a value between 3 and 3000, inclusive. (Default: 33)
max-burst	<number>	Sets the maximum number of packets to be transmitted during a particular time interval. This pertains to LSPs and CSNPs. Enter a value between 1 and 10, inclusive. (Default: 10)
passive		When you set this parameter, the adjacency goes down and the interface stops transmitting IS-IS packets. The interface, though, may still be used to view IS-IS information.
retransmit-interval	<number>	Sets the interval, in seconds, between the retransmission of LSPs. Enter a number between 1 and 100 inclusive. (Default: 5)
authentication-method		Specifies the authentication method for all interfaces in the area.
	md5	Uses the MD5 algorithm to create a crypto-checksum of an IS-IS packet and an authentication key of up to 16 characters.
	simple	Uses a simple string (password) of up to 8 characters in length for authentication. If you choose this authentication method, then you should also specify a key-chain identifier using the key-chain option.
key-chain	<string>	Identify the key-chain containing the authentication keys. Note that the key-chain must have been previously created with the ip-router authentication create key-chain command.
l1-csn-interval	<number>	Sets the CSN interval for Level 1 routers. Enter a value between 1 and 100, inclusive. (Default: 10)
l1-dis-hello-interval	<number>	Sets the hello-interval used if the router becomes the DIS for Level 1. Enter a value between 1 and 100, inclusive. (Default: 3)

Parameter	Value	Meaning
l1-hello-interval	<number>	Sets the hello-interval for Level 1 routers. Enter a value between 1 and 300, inclusive. (Default: 10)
l1-hello-multiplier	<number>	For Level 1 routers, sets the number of hello-intervals a router must wait to receive the next Hello packet before the router determines the neighboring IS is down. Enter a value between 1 and 100, inclusive. (Default: 3)
l1-priority	<number>	Sets the priority of the interface during the election of the Designated Intermediate System (DIS) for Level 1 routers. Enter a value between 0 and 127, inclusive. (Default: 1)
l2-csn-interval	<number>	Sets the CSNP interval for Level 2 routers. Enter a value between 1 and 100, inclusive. (Default: 10)
l2-dis-hello-interval	<number>	Sets the hello-interval used if the router becomes the DIS for Level 2. Enter a value between 1 and 300, inclusive. (Default: 3)
l2-hello-interval	<number>	Sets the hello-interval for Level 2 routers. Enter a value between 1 and 300, inclusive. (Default: 10)
l2-hello-multiplier	<number>	For Level 2 routers, sets the number of hello-intervals a router must wait to receive the next Hello packet before the router determines the neighboring IS is down. Enter a value between 1 and 100, inclusive. (Default: 3)
l2-priority	<number>	Sets the priority of the interface during the election of the Designated Intermediate System (DIS) for Level 2 routers. Enter a value between 0 and 127, inclusive. (Default: 1)
mesh-group	<number>	Assigns the interface to a mesh group as specified in RFC 2973. If an LSP is received on an interface belonging to a particular mesh group, all other ports within that mesh group will not send out the LSP. Mesh groups are intended for use in point-to-point, full-mesh topologies. Mesh group membership is assigned by numbers from 0 to 2147483647. The mesh group 0 has special significance in that an interface belonging to mesh group 0 will not send out LSPs for any reason.

Restrictions

None.

Example

To set IS-IS parameters for interface "int10:"

```
rs(config)# isis set interface int10 level 1 metric 2 priority 1
hello-interval 10 dis-hello-interval 10 hello-multiplier 4 csn interval
8 lsp-interval 20 max-burst 12 retransmit-interval 8
```

isis set level

Mode

Configure

Format

```
isis set level 1|2|1-and-2
```

Description

The **isis set level** command allows you to select the routing level for the RS. Level 1 routers route intra-area traffic only. Level 2 routers route inter-area traffic only. A Level 1-and-2 router routes on both levels.

If a router's operating level is set to Level 1 or Level 2, its interfaces should be set to the same level, if they are to route IS-IS traffic. If a router's operating level is set to Level 1-and-2, then its interfaces can be set to both Level 1 and Level 2.

Parameter	Value	Meaning
level		Specifies the level at which the RS will route.
	1	Select 1 to configure the RS to route at Level 1 (intra-area).
	2	Select 2 to configure the RS to route at Level 2 (inter-area).
	1-and-2	Select 1-and-2 to configure the RS to be able to route on both levels. The default level is 1-and-2.

Restrictions

None.

isis set overload-bit

Mode

Configure

Format

```
isis set overload-bit
```

Description

There may be times when the router may not have sufficient memory to store a received Link State PDU (LSP). When this happens, the router ignores the LSP and enters into a waiting state. A timer is started and the router floods its LSPs with a zero LSP number and the overload bit set. This prevents other routers from using it for transit traffic.

The **isis set overload-bit** command allows you to manually set the overload bit so the router functions as an end node only.

Restrictions

None.

isis set preference

Mode

Configure

Format

```
isis set preference level-1 <number>|level-2 <number>
```

Description

The **isis set preference** command allows you to set the preference of IS-IS routes over routes from other protocols. The preference value you set applies to all interfaces on which IS-IS is enabled. You can set the preference for Level-1 routes and for Level-2 routes.

Parameter	Value	Meaning
level-1	<number>	Specifies the preference value for IS-IS Level-1 routes. Enter a number between 0 and 255 inclusive.
level-2	<number>	Specifies the preference value for IS-IS Level-2 routes. Enter a number between 0 and 255 inclusive.

Restrictions

None.

Example

To set the preference for Level-1 routes:

```
rs(config)# isis set preference level-1 10
```

isis set psn-interval

Mode

Configure

Format

```
isis set psn-interval <number>
```

Description

The **isis set psn-interval** command allows you define the time interval between the retransmission of Partial Sequence Number PDUs (PSNPs).

Parameter	Value	Meaning
psn-interval	<number>	Specifies the time interval, in seconds. Specify any number between 1 and 100.

Restrictions

None.

Example

To set the interval between PSNP transmissions:

```
rs(config)# isis set psn-interval 8
```

isis set reference-bandwidth

Mode

Configure

Format

```
isis set reference-bandwidth <number>
```

Description

The **isis set reference-bandwidth** command allows you to specify a reference bandwidth. The reference bandwidth is used in calculating the default interface metric. The default metric is calculated using the following formula:

$$\text{metric} = \text{reference-bandwidth} / \text{bandwidth}$$

Parameter	Value	Meaning
reference-bandwidth	<number>	Specify a value in bits-per-second (bps). The value should be between 1 and 2147483647.

Restrictions

None.

Example

To set the the reference bandwidth to 100:

```
rs(config)# isis set reference-bandwidth 100
```

isis set require-snp-auth

Mode

Configure

Format

```
isis set require-snp-auth
```

Description

The **isis set require-snp-auth** command allows you to require the authentication of Sequence Number PDUs (SNPs). When this command is set, the RS uses the interface password to authenticate SNPs.

Restrictions

None.

isis set spf-interval

Mode

Configure

Format

isis set spf-interval <number>

Description

The **isis set spf-interval** command sets the interval, in seconds, between the recalculation of the routing table.

Parameter	Value	Meaning
spf-interval	<number>	Specifies the time interval, in seconds. Enter a value between 1 and 30 inclusive

Restrictions

None.

Example

To set the router's spf-interval:

```
rs(config)# isis set spf-interval 3
```

isis set system-id

Mode

Configure

Format

```
isis set system-id <string>
```

Description

A system identifier for the intermediate system is automatically configured by default. The **isis set system-id** command allows you overwrite the default system identifier. The system identifier uniquely identifies the router in its routing domain. It is part of the Network Entity Title (NET) for the intermediate system. Once the system identifier is set, it cannot be changed without disabling and re enabling IS-IS.

Parameter	Value	Meaning
system-id	<string>	Specifies the system identifier, in octets. Specify a 12 hexadecimal digit string for the system identifier.

Restrictions

None.

Example

To set the router's System ID:

```
rs(config)# isis set 0000.2080.2A89
```

isis set traffic-engineering

Mode

Configure

Format

isis set traffic-engineering enable

Description

The **isis set traffic-engineering** command allows you to enable traffic engineering metrics.

Parameter	Value	Meaning
enable		Enables traffic engineering metrics.

Restrictions

None.

Example

To enable traffic engineering metrics:

```
rs(config)# isis set traffic-engineering enable
```

isis show adjacencies

Mode
Enable

Format

isis show adjacencies [detail]

Description

The **isis show adjacencies** command allows you to display the router’s adjacencies.

Parameter	Value	Meaning
detail		Displays detailed information about adjacencies in each circuit.

Restrictions

None.

Example

Following is an example of the **isis show adjacencies** command:

rs# isis show adjacencies							
Adjacencies							
Interface	SystemID	State	Level	Hold(s)	SNPA	Priority	
rt6-rt10	0000.0a0a.0a0a	up	L1	9	802.2 0:e0:63:6:5:c0	64	
rt6-rt10	0000.0a0a.0a0a	up	L2	9	802.2 0:e0:63:6:5:c0	64	
rt6-rt3.1	0000.0303.0303	up	L2	8	802.2 0:e0:63:b:44:40	64	
rt6-rt3.2	0000.0303.0303	up	L2	8	802.2 0:e0:63:b:44:40	64	
rt6-rt3.4	0000.0303.0303	up	L2	8	802.2 0:e0:63:b:44:40	64	
rt6-rt3.3	0000.0303.0303	up	L2	8	802.2 0:e0:63:b:44:40	64	
rt6-rt5.so1	0000.0505.0505	up	L1/L2	28			
rt6-rt5.so2	0000.0505.0505	up	L1/L2	28			
rt6-rt5.so3	0000.0505.0505	up	L1/L2	28			
rt6-rt5.so4	0000.0505.0505	up	L1/L2	22			
rt4-rt3.st	0000.0303.0303	up	L2	8	802.2 0:e0:63:b:44:40	64	

Following is an example of the **isis show adjacencies detail** command:

```
rs# isis show adjacencies detail
Adjacencies

Circuit name: rt6-rt5
  No level-1 Adjacencies

  No level-2 Adjacencies

Circuit name: rt6-rt3
  No level-2 Adjacencies

Circuit name: rt6-rt10
  Number of level-1 Adjacencies: 1
  SystemID: 0000.0a0a.0a0a      Snpa: 802.2 0:e0:63:6:5:c0
  State: up      Type: l1-is      Pri: 64      Hold: 8
  Time created: 2001-02-20 10:19:40
  Uptime: 3 days 1 hrs 55 mins 18 secs
  Areas: 33.3333
  Supported protocols: inet4
  Neighbor Ifaddr: 200.135.89.140

  Number of level-2 Adjacencies: 1
  SystemID: 0000.0a0a.0a0a      Snpa: 802.2 0:e0:63:6:5:c0
  State: up      Type: l2-is      Pri: 64      Hold: 8
  Time created: 2001-02-20 10:19:40
  Uptime: 3 days 1 hrs 55 mins 18 secs
  Areas: 33.3333
  Supported protocols: inet4
  Neighbor Ifaddr: 200.135.89.140

Circuit name: rt6-rt3.1
  No level-1 Adjacencies

  Number of level-2 Adjacencies: 1
  SystemID: 0000.0303.0303      Snpa: 802.2 0:e0:63:b:44:40
  State: up      Type: l2-is      Pri: 64      Hold: 7
  Time created: 2001-02-20 10:19:40
  Uptime: 3 days 1 hrs 55 mins 18 secs
  Areas: 22.2222
  Supported protocols: inet4
  Neighbor Ifaddr: 200.135.90.73
.
.
.
```

isis show all

Mode

Enable

Format

isis show all

Description

The **isis show all** command allows you to display all the IS-IS tables which can be displayed using the individual **isis show** commands. These include the following:

- IS-IS timers
- circuits
- adjacencies
- global parameters
- link state database(s)

For additional information about each table, refer to the appropriate **isis show** command.

Restrictions

None.

isis show circuits

Mode

Enable

Format

isis show circuits [detail]

Description

The **isis show circuits** command allows you display information about the routers on the circuits. An IS-IS circuit is a point-to-point connection between two intermediate systems.

Parameter	Value	Meaning
detail		Displays detailed information about the circuit.

Restrictions

None.

Example

The following is an example of the **isis show circuits** command:

rs#						
Interface	Level	Nos of		Nos of		DR
		CirID	L1-adj	DR	L2-adj	
lo	na	na	na	na	na	na
rt6-rt5	1&2	0x003	na	N	na	N
rt6-rt3	2	0x004	na	na	na	N
rt6-rt10	1&2	0x005	1	N	1	N
rt6-rt3.1	1&2	0x006	na	N	1	N
rt6-rt3.2	1&2	0x007	na	N	1	N
rt6-rt3.4	1&2	0x008	na	N	1	N
rt6-rt3.3	1&2	0x009	na	N	1	N
rt6-rt5.so1	1&2	0x00A	1	na	1	na
rt6-rt5.so2	1&2	0x00B	1	na	1	na
rt6-rt5.so3	1&2	0x00C	1	na	1	na
rt6-rt5.so4	1&2	0x00D	1	na	1	na
rt4-rt3.st	1&2	0x00E	na	N	1	N

isis show export-policies

Mode

Enable

Format

```
isis show export-policies
```

Description

The **isis show export-policies** command allows you to display IS-IS export policies.

Restrictions

None.

isis show globals

Mode

Enable

Format

isis show globals

Description

The **isis show globals** command allows you to display the IS-IS parameters that were set for the router.

Restrictions

None.

Example

The following is an example of the **isis show globals** command:

```
DUT# isis show globals

Task ISIS: Globals

ISIS enabled : True
Number of areas : 1
Area[s] : 21.2223.2425.2627.2829.3031.3233
System ID   : aaaa.aaaa.aaaa
IS mode     : IS
ISIS level  : 1
SPF interval : 2
Partial SNP interval : 2
```

The output displays the following:

- whether IS-IS is enabled on the router
- the number of areas configured
- the address of the IS-IS area
- the router's System ID
- the IS-IS level at which the router is operating
- the SPF interval configured for the router
- the PSNP interval configured for the RS

isis show lsp-database

Mode

Enable

Format

```
isis show lsp-database level 1|2 [detail][id <string>]
```

Description

The **isis show lsp-database** command allows you display Link State PDU (LSP) database information.

An LSP database contains information from the latest LSPs gathered from all other intermediate systems in the area. The information contained in the database is used to compute the shortest paths to all other intermediate systems in the area.

Parameter	Value	Meaning
level		Selects which LSP database to display.
	1	Specify 1 to display level 1 LSP database information.
	2	Specify 2 to display level 2 LSP database information.
detail		Specify detail to display detailed information about the LSP database.
id	<string>	Selects which LSP to show.

Restrictions

None.

Example

The following is an example of the **isis show lsp-database** command:

```
rs# isis show lsp-database

Task ISIS: Link State Database

IS-IS Level-1 Link State Database (* - originated local)
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.6401.0102.0000* 0X0000000E  0X2B9D        293           0/0/0

IS-IS Level-2 Link State Database (* - originated local)
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0a32.0701.0000  0X0000000F  0XD602        867           0/0/0
0000.6401.0102.0000* 0X00000011  0X258C        442           0/0/0
0000.6401.0102.0300* 0X00000012  0X8EF8        991           0/0/0
```

The **isis show lsp database** command displays the following information for each LSP:

- LSP ID which is the system ID of the originating router concatenated with 2 more octets (pseudonode ID and LSP number)
- the sequence number of the LSP
- the LSP checksum computed by the source IS
- the Holdtime is the LSP's Remaining Lifetime in seconds
- the status of the Attached (ATT) bit, Partition (P) bit, and Overload (O) bit of each LSP; a 1 in the Attached bit indicates a Level 2 or Level 1-and-2 router has a route to another area; a 1 in the Partition bit indicates the router has partition repair capability; and a 1 in the Overload bit indicates the router's memory is overloaded or it has an link state incomplete database

The following is an example of the **isis show lsp-database detail** command:

```
DUT# isis show lsp-database detail

Task ISIS: Link State Database

IS-IS Level-1 Link State Database (* - originated local)
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
aaaa.aaaa.aaaa.0000*  0X000000B2  0XD6CE       501           0/0/0
Area Addresses:21.2223.2425.2627.2829.3031.3233
NLPID: 0Xg
System Name: Router-1
IP Address: 10.3.1.1
IP Address: 10.2.1.1
IP Address: 10.1.1.1
Metric: 10 IP 10.3/16
Metric: 10 IP 10.2/16
Metric: 10 IP 10.1/16
DUT#
```

In addition to the information displayed by the **isis show lsp-database** command, the **isis show lsp-database detail** command displays the area addresses in the LSPs, the System Name (set with the **system set name** command), the protocol ID, and reachability information.

isis show timers

Mode

Enable

Format

```
isis show timers
```

Description

The **isis show timers** command allows you display the IS-IS timers.

Restrictions

None.

Example

The following is an example of the **isis show timers** command:

```
rs# isis show timers
Timers:
-----

Timer                               State   Last      Next      Intvl Jitter Flags
-----
ISIS_CSN burst timer (10, 33, 10) Inactive -      -      -      -      OneShot
Inactive
ISIS_level 2 lsp SystemID 0000.6401.0102.0300 hold-down timer Inactive -
-      -      -      OneShot Inactive
ISIS_level 2 lsp SystemID 0000.6401.0102.0300 refresh timer Active   14:58:01
15:13:30.909 15:00 90000000
ISIS_CSN interval timer (10, 33, 10) Active   15:10:20 15:10:29.699 10      1000000
ISIS_isis adjacency hold timer Active   15:10:55 15:10:55 -      -      OneShot
ISIS_election timer      Inactive -      -      -      -      OneShot Inactive
ISIS_hello timer        Active   15:10:27 15:10:30 3      -      HiPrio SubJitter
ISIS_election timer      Inactive -      -      -      -      OneShot Inactive
ISIS_hello timer        Active   15:10:20 15:10:29.609 10      1000000 HiPrio SubJitter
ISIS_LSP broadcast burst timer Inactive -      -      -      -      OneShot Inactive
ISIS_level 2 lsp SystemID 0000.6401.0102.0300 hold-down timer Inactive -
-      -      -      OneShot Inactive
ISIS_level 2 lsp SystemID 0000.6401.0102.0300 refresh timer Active   15:06:01
15:21:20.568 15:00 90000000
ISIS_level 2 spf         Inactive -      -      -      -      OneShot Inactive
ISIS_level 1 spf         Inactive -      -      -      -      OneShot Inactive
ISIS_level 2 lsp SystemID 0000.6401.0102.0000 hold-down timer Inactive --      -
-      OneShot Inactive
ISIS_level 2 lsp SystemID 0000.6401.0102.0000 refresh timer Active   14:56:52
15:11:32.977 15:00 90000000
ISIS_level 1 lsp SystemID 0000.6401.0102.0000 hold-down timer Inactive --      -
-      OneShot Inactive
ISIS_level 1 lsp SystemID 0000.6401.0102.0000 refresh timer Active   15:09:31
15:23:57.641 15:00 90000000
ISIS_lr_daemon_t        Active   15:10:23 15:10:33 10      -

SystemID 0000.6401.0102

rs#
```

ISIS_LSP broadcast burst timer	The maximum number of LSP packets that can be transmitted during an interval.
ISIS_election timer	The time period during which a Designated Intermediate System (DIS) is elected.
ISIS_hello timer	The interval in seconds between the generation of IS-IS Hello PDUs. It displays the time of the last and next Hello transmission, the interval, and the amount of jitter applied.

isis start

Mode

Configure

Format

```
isis start
```

Description

The IS-IS protocol is disabled by default. The **isis start** command enables the IS-IS protocol on the router.

Restrictions

None.

isis stop

Mode
Configure

Format

```
isis stop
```

Description

The **isis stop** command disables the IS-IS protocol on the router.

Restrictions

None

isis trace

Mode

Enable

Format

```
isis trace system|adjacency|dis-election|db|flooding|spf|debug|packets
[detail|send|receive]|iih [detail|send|receive]|lsp [detail|send|receive]|csnp
[detail|send|receive]|psnp [detail|send|receive]|local options
[all|general|state|normal|policy|task|timer|route|none] [cspf]
```

Description

The **isis trace** command lets you set IS-IS trace options for the RS.

Parameter	Value	Meaning
system		Traces isis-system tracepoints.
adjacency		Traces isis-adjacency tracepoints.
dis-election		Traces IS-IS Designated Intermediate System election.
db		Traces IS-IS LSP database.
flooding		Traces the flooding of all LSPs.
spf		Traces the running of the SPF algorithm.
debug		Traces IS-IS debugging.
packets		Traces the transmission and receipt of packets.
	detail	Provides detailed information about all IS-IS packets.
	send	Traces IS-IS packets sent by the router.
	receive	Traces IS-IS packets received by the router.
iih		Traces the transmission and receipt of IIH packets.
	detail	Provides detailed information about IIH packets.
	send	Traces IIH packets sent by the router.
	receive	Traces IIH packets received by the router.
lsp		Traces the transmission and receipt of LSPs.
	detail	Provides detailed information about LSPs.
	send	Traces LSPs sent by the router.
	receive	Traces LSPs received by the router.
csnp		Traces the processing and construction of CSNPs.

Parameter	Value	Meaning
	detail	Provides detailed information about CSNPs.
	send	Traces CSNPs sent by the router.
	receive	Traces CSNPs received by the router.
psnp		Traces the processing and construction of PSNPs.
	detail	Provides detailed information about PSNPs.
	send	Traces PSNPs sent by the router.
	receive	Traces PSNPs received by the router.
local options		Sets various trace options for the IS-IS protocol only. (By default, these options are inherited from the ip-router global set trace-options command.)
	all	Turns on all tracing options.
	general	Turns on normal and route tracing.
	state	Traces state machine transmissions in the protocols.
	normal	Traces normal protocol occurrences.
	policy	Traces the application of protocol and user-specified policy to routes being imported and exported.
	task	Trace system interface and processing associated with this protocol or peer.
	timer	Traces timer usage by this router with this protocol or peer.
	route	Traces routing table changes for routes installed by this protocol or per.
	none	Specifies that all tracing should be turned off for this protocol or peer.
cspf		Traces the running of the constrained shortest path first (CSPF) algorithm.

Restrictions

None.

34 L2-TABLES COMMANDS

The **l2-tables** commands let you display various L2 tables related to MAC addresses.

34.1 COMMAND SUMMARY

The following table lists the **l2-tables** commands. The sections following the table describe the command syntax for each command.

l2-tables show all-flows [vlan <VLAN-num> [source-mac <MACaddr>]] [undecoded]
l2-tables show all-macs [verbose [undecoded]] [vlan <VLAN-num>] [source] [destination] [multicast]
l2-tables show bridge-management
l2-tables show igmp-mcast-registrations [vlan <VLAN-num>]
l2-tables show mac <MACaddr> vlan <VLAN-num>
l2-tables show mac-table-stats
l2-tables show port-macs <port-list> all-ports [[vlan <VLAN-num>] [source] [destination] [multicast] [undecoded] [no-stats] verbose]
l2-tables show vlan-igmp-status vlan <VLAN-num>

l2-tables show all-flows

Mode

User or Enable

Format

```
l2-tables show all-flows [vlan <VLAN-num> [source-mac <MACaddr>]] [undecoded]
```

Description

The **l2-tables show all-flows** command shows all the L2 flows learned by the RS. The RS learns flows on ports that are operating in flow-bridging mode.

Parameter	Value	Meaning
vlan	<VLAN-num>	The VLAN number associated with the flows. The VLAN number can be from 1 – 4095.
source-mac	<MACaddr>	The source MAC address of the flows. Specify the MAC address in either of the following formats: xx:xx:xx:xx:xx:xx xxxxxxxx:xxxxxxxx
undecoded		Prevents the RS from displaying the vendor names with the MAC addresses. Instead, the organizationally unique identifier (OUI) of each MAC address is displayed “as is,” in hexadecimal format. If you do not use this option, the RS decodes the OUI and displays the vendor name.

Restrictions

None.

Example

To show all flows for VLAN 2:

```
rs# l2-tables show all-flows vlan 2
  Id           Flows           VLAN  Source Port
-----
000001  src:  00:00:01:B0:33:BC  0002  et.1.3
      1  dst:  02:01:A0:00:00:00
```

For each flow, the following is displayed:

- the source and destination MAC addresses
- the VLAN ID
- the port which is the source of the flow information

l2-tables show all-macs

Mode

User or Enable

Format

```
l2-tables show all-macs [verbose [undecoded]] [vlan <VLAN-num>] [source] [destination] [multicast]
```

Description

The **l2-tables show all-macs** command shows the MAC addresses currently in the RS's L2 tables. You can format the displayed information based on VLAN, source MAC address, destination MAC address or multicast. If you enter the verbose option, the command also shows the individual MAC addresses.

Parameter	Value	Meaning
vlan	<VLAN-num>	Displays only MAC addresses in the specified VLAN.
source		Displays only source addresses.
destination		Displays only destination addresses.
multicast		Displays only multicast and broadcast addresses.
verbose		Shows detailed information for each MAC address entry.
undecoded		Prevents the RS from displaying the vendor names with the MAC addresses. Instead, the organizationally unique identifier (OUI) of each MAC address is displayed “as is,” in hexadecimal format. If you do not use this option, the RS decodes the OUI and displays the vendor name.

Restrictions

None.

Example

To display both detailed and summary information about the MAC addresses in the RS's L2 tables:

```
rs# l2-tables show all-macs verbose
```

Id ^❶				

000001	01:80:C2:00:00:00	4095	mcast	et.2.(1-2),et.3.(1-3)
000002	01:80:C2:00:00:00	0003	mcast	et.2.3
000003	01:80:C2:00:00:00	0001	mcast	et.2.(4-8),et.3.(4-8),et.4.(1-8)


```
Statistics Summary ❷
```

Total number of unique MACs found	3			
MACs that reside on a port as a source	0			
MACs that reside on port(s) as a dest	3			
Multicasts (subset of dest MACs)	3			

Legend:

- The detailed information lists the following for each MAC address:
 - the VLAN ID
 - the source port (For multicast , the address is added as a destination into the L2 table of the port in which the packet was received.)
 - the ports on which the MAC address is listed as a destination in the port's L2 table
- The summary information displays the following statistics:
 - total number of MAC addresses in the RS's L2 tables
 - the number of MAC addresses that are in a port's L2 table as source addresses
 - the number of MAC addresses that are in the RS's ports' L2 tables as destination addresses

l2-tables show bridge-management

Mode

User or Enable

Purpose

Show information about all MAC addresses registered by the system.

Format

```
l2-tables show bridge-management
```

Description

The **l2-tables show bridge-management** command shows MAC addresses that have been inserted into the L2 tables for management purposes. Generally, these entries are configured so that a port forwards a frame to the Control Module if the management MAC matches the frame's destination MAC.

An example of a bridge-management MAC is Spanning Tree's bridge group address (0180C2:000000), which is registered in the L2 tables of RS ports on which the Spanning Tree Protocol (STP) is enabled.

Restrictions

None.

Example

To display MAC addresses registered by the system:

```
rs# l2-tables show bridge-management

Name:          Mgmt Entry 1
----
VLAN:          Default Bridging VLAN
Dest MAC:      0180C2:000000
In-List ports: et.2.(1-8),et.3.(1-8),et.4.(1-8)
```

The output displays the following:

- the name of the VLAN
- the MAC address(es) inserted into the L2 tables for management purposes
- the ports in which the MAC address is listed

l2-tables show igmp-mcast-registrations

Mode

User or Enable

Format

```
l2-tables show igmp-mcast-registrations [vlan <VLAN-num>]
```

Description

The **l2-tables show igmp-mcast-registrations** command shows the multicast MAC addresses that IGMP has registered with the L2 tables. The RS forwards the multicast MAC addresses only to the ports that IGMP specifies.

Parameter	Value	Meaning
vlan	<VLAN-num>	Displays only the multicast MAC addresses registered for the specified VLAN.

Restrictions

None.

Example

To display the multicast MAC addresses registered for VLAN 3:

```
rs# l2-tables show igmp-mcast-registrations vlan 3

Name:          Igmp Entry 6
----
VLAN:          3
Dest MAC:      01015E:000004
In-List ports: et.2.(1-8)
Out-List ports: et.1.(1-8),et.2.(1-8),gi.3.(1-2)

Name:          Igmp Entry 7
----
VLAN:          3
Dest MAC:      01015E:000007
In-List ports: et.2.(1-8)
Out-List ports: et.1.(1-8),et.2.(1-8),gi.3.(1-2)
```

l2-tables show mac

Mode

User or Enable

Format

l2-tables show mac <MACaddr> vlan <VLAN-num>

Description

The **l2-tables show mac** command shows the VLAN and the port number on which the specified MAC address resides.

Parameter	Value	Meaning
mac	<MACaddr>	Is a MAC address. You can specify the address in either of the following formats: xx:xx:xx:xx:xx:xx xxxxxx:xxxxxx
vlan	<VLAN-num>	Displays the MAC address for this VLAN.

Restrictions

None.

Example

To display information about the MAC address 01:80:c2:00:00:00:

rs# l2-tables show mac 01:80:c2:00:00:00				
Id	MAC	VLAN	SourcePort	Ports where MAC resides as a dest.
-----	-----	----	-----	-----
000001	01:80:C2:00:00:00	0001	mcast	et.2.(4-8),et.3.(4-8),et.4.(1-8)
000002	01:80:C2:00:00:00	0003	mcast	et.2.3
000003	01:80:C2:00:00:00	4095	mcast	et.2.(1-2),et.3.(1-3)

l2-tables show mac-table-stats

Mode

User or Enable

Format

```
l2-tables show mac-table-stats
```

Description

The **l2-tables show mac-table-stats** command shows statistics for the master MAC address table in the Control Module and the MAC address tables on the individual ports.

Restrictions

None.

Example

To display information on the MAC addresses in the MAC address tables:

```
rs# l2-tables show mac-table-stats

MAC Address Table - Statistics Summary
-----
Status: learning and bridging.
Current number of learned MAC addresses: 3
Number of requests to learn a new MAC address: 3
Number of requests to remove a MAC address (from all ports): 0
Current number of learned L2 flows: 0
Number of requests to learn a new L2 flow: 0
Number of requests to remove an L2 flow: 0
Number of times stations have moved between ports: 0
Learning on an invalid port: 0
```

l2-tables show port-macs

Mode

User or Enable

Format

```
l2-tables show port-macs port <port-list> | all-ports [[vlan <VLAN-num>] [source]
[destination] [multicast] [undecoded] [no-stats] verbose]
```

Description

The **l2-tables show port-macs** command shows the information about the learned MAC addresses in individual L2 MAC address tables. Each port has its own MAC address table. The information includes the number of source MAC addresses and the number of destination MAC addresses in the table. If you enter the **verbose** option, the MAC addresses also are displayed.

Parameter	Value	Meaning
port	<port-list> all-ports	Specifies the port(s) for which you want to display MAC address information. You can specify a single port or a comma-separated list of ports. If you use the all-ports keyword, MAC address information is displayed for all ports.
vlan	<VLAN-num>	Specifies the type of MAC address for which you want to show statistics.
source		Displays statistics for only source addresses.
destination		Displays statistics for only destination addresses.
multicast		Displays statistics for only multicast and broadcast addresses.
undecoded		Prevents the RS from displaying the vendor names with the MAC addresses. Instead, the organizationally unique identifier (OUI) of each MAC address is displayed “as is,” in hexadecimal format. If you do not use this option, the RS decodes the OUI and displays the vendor name.
no-stats		Lists the MAC addresses without displaying any statistics.
verbose		Shows detailed statistics for each MAC address entry.

Restrictions

None.

Example

To display information about the MAC addresses in port et.2.1's L2 table:

```
rs# l2-tables show port-macs port et.2.1

L2 table information for port et.2.1
-----
Number of source MAC addresses: 0
Number of destination MAC addresses: 0
Number of management-configured MAC addresses: 1
Port table capacity: 5888
Port table demand deletion upper & lower thresholds: 95% - 85%
Number of times table usage has reached upper threshold: 0
Number of times buckets have become full: 0
Number of duplicate learning frames: 0
Number of times LG port got out-of-sync: 0
Number of requests to learn a frame on an invalid VLAN: 0
Number of frames received from this switch (possible loop): 0
Aging is enabled
Addresses will be aged-out after 300 seconds
```

l2-tables show vlan-igmp-status

Mode

Enable

Format

```
l2-tables show vlan-igmp-status vlan <VLAN-num>
```

Description

The **l2-tables show vlan-igmp-status** command shows the multicast MAC addresses that IGMP has registered with the L2 tables. This command also shows the ports to which the multicast MAC addresses are forwarded.



Note

For IGMP forwarding to occur for a multicast MAC address, IGMP must be enabled on the VLAN with which the MAC address is associated.

Parameter	Value	Meaning
vlan	<VLAN-num>	The VLAN number. The VLAN number can be from 1 – 4095.

Restrictions

None.

Example

To show whether IGMP is enabled on VLAN 1:

```
rs# l2-tables show vlan-igmp-status vlan 1
```

```
IGMP status on VLAN 1: disabled
```

35 LACP COMMANDS

The LACP commands configure and control the ports and parameters required for the 802.3ad Link Aggregation Control Protocol (LACP).

35.1 COMMAND SUMMARY

The following table lists the lacp commands. The sections following the table describe the command syntax.

lacp set aggregator <smarttrunk> [port-type 10-100-Ethernet Gigabit-Ethernet] [actor-key <number>] [partner-key <number>] [partner-system-priority <number>] [partner-system-id <MacAddr>] [individual]
lacp set port <port-list> [enable] [port-key <number>] [aggregation aggregatable individual] [port-priority <number>] [activity active passive] [timeout long short]
lacp set system actor-system-priority <number>
lacp show aggregator <smarttrunk> all-smarttrunks
lacp show keygroup key <number> all-keys
lacp show lag index <number> all-unique
lacp show port <port-list> [parameters] [statistics] [protocol-state]

lACP set aggregator

Mode

Configure

Format

```
lACP set aggregator <smarttrunk>|<singleport> [port-type 10-100-Ethernet|Gigabit-Ethernet]
[actor-key <number>] [partner-key <number>] [partner-system-priority <number>]
[partner-system-id <MacAddr>] [individual]
```

Description

The **lACP set aggregator** command lets you define the SmartTRUNK that will be the aggregator and specify its operating parameters.

Parameter	Value	Meaning
aggregator	<smarttrunk> or <singleport>	The SmartTRUNK or single port that is the aggregator.
port-type		Specify the type of ports for which the SmartTRUNK or single port is an aggregator.
	10-100-Ethernet	Aggregator of only 10/100 Mbit Ethernet ports.
	Gigabit-Ethernet	Aggregator of only Gigabit-Ethernet ports.
actor-key	<number>	Specifies the actor aggregator's administrative key.
partner-key	<number>	Specifies the partner system's administrative key.
partner-system-priority	<number>	Sets the partner system's system priority.
partner-system-id	<MacAddr>	Sets the partner system's MAC address.
individual		Sets the aggregator to individual, preventing it from joining a Link Aggregation Group (LAG).

Restrictions

None.

lACP set port

Mode

Configure

Format

```
lACP set port <port-list> [enable] [port-key <number>] [aggregation  
aggregatable|individual] [port-priority <number>] [activity active|passive] [timeout  
long|short]
```

Description

The **lACP set port** command enables the Link Aggregation Control Protocol (LACP) on the specified ports and sets their LACP parameters.

Parameter	Value	Meaning
port	<port-list>	The port(s) on which LACP will be enabled.
enable		Enables LACP on the specified ports.
port-key	<number>	Sets the administrative key for the port.
aggregation		Sets the type of aggregation.
	aggregatable	Specifies that the port can join a Link Aggregation Group (LAG).
	individual	Specifies that the port cannot join a LAG.
port-priority	<number>	Sets the administrative priority for the port(s).
activity		Sets the administrative LACP activity for the port(s)
	active	Specifies that the port will transmit LACP PDUs regardless of its partner's control value.
	passive	Specifies that the port will transmit LACP PDUs only if its partner's control value is <i>active</i> .
timeout		Sets the administrative LACP timeout value for the port (s).
	long	Specifies a long timeout value.
	short	Specifies a short timeout value.

Restrictions

None.

lacp set system

Mode

Configure

Format

```
lacp set system actor-system-priority <number>
```

Description

The `lacp set system` command sets the actor system priority.

Parameter	Value	Meaning
actor-system-priority	<number>	Enter a value between 1 and 65535, inclusive.

Restrictions

None.

lACP show aggregator

Mode

Enable

Format

lACP show aggregator <smarttrunk>|all-smarttrunks

Description

The **lACP show aggregator** command displays information about the aggregator.

Parameter	Value	Meaning
aggregator	<smarttrunk>	Displays information about the specified SmartTRUNK.
	all-smarttrunks	Displays information about all SmartTRUNKs.

Restrictions

None.

Example

Following is an example of the **lACP show aggregator** command which displays the aggregator's port type, whether the aggregator was set to "individual," the ID of the LAG to which it is attached, and information about the actor and its partner system.

```
rs# lACP show aggregator st.1
Aggregator st.1
  Identifier 1
  Port Type  Gigabit Ethernet
  Individual FALSE
  Attached Lag Id:
  Actor
    System Priority:1
    MAC Address:    00001D:123456
    Admin Key:      25
    Oper Key:       25
  Partner
    System Priority:0
    MAC Address:    00002E:342156
    Oper Key:       52
rs#
```

lACP show keygroup

Mode

Enable

Format

lACP show keygroup key <number>|all-keys

Description

The **lACP show keygroup** command displays information about the key group that corresponds to the actor operational key.

Parameter	Value	Meaning
key	<number>	Show information about the key group that corresponds to the specified actor operational key.
	all-keys	Show information about all key groups.

Restrictions

None.

Example

Following is an example of the **lACP show keygroup** command.

```
rs# lACP show keygroup all-keys
Ports with Actor Operational Key: 2
    gi.3.1
    gi.3.2
    gi.3.3
```


lacp show lag

Mode

Enable

Format

lacp show lag index <number>|all-unique

Description

The **lacp show lag** command displays the Link Aggregations Group's (LAG) properties.

Parameter	Value	Meaning
index	<number>	Show information for the specified LAG index.
	all-unique	Show information for all unique LAGs.

Restrictions

None.

Example

Following is an example of the **lacp show lag** command.

```
rs# lacp show lag all-unique

LAG index 65
  Id: [(1, 00001D:123456, 2, 0, 0), (0, 000000:000000, 0, 0, 0)]

  Ports in the LAG:
    gi.3.1
    gi.3.2
    gi.3.3
```

lACP show port

Mode

Enable

Format

```
lACP show port <port-list> [parameters] [statistics] [protocol-state]
```

Description

The **lACP show port** command displays LACP information for the specified port.

Parameter	Value	Meaning
port	<port-list>	The port for which information will be displayed.
parameters		Shows the LACP parameters of the port.
statistics		Shows the LACP statistics of the port.
protocol-state		Shows the LACP protocol state of the port.

Restrictions

None.

Example

Following is an example of the **lACP show port statistics** command. The output displays the number and type of PDUs that were sent and received.

```
rs# lACP show port gi.3.1 statistics
gi.3.1 LACP statistics:
      LACP Pdus sent:           0
      Marker Response Pdus sent: 0
      LACP pdus received:       0
      Marker pdus received:     0
rs#
```

36 LDP COMMANDS

The **ldp** commands allow you to configure the label distribution protocol that is used to distribute label binding information.

36.1 COMMAND SUMMARY

The following table lists the **ldp** commands. The sections following the table describe each command in greater detail.

<code>ldp add export-filter request mapping nexthop <ip address> neighbor <ip address> interface <name> prefix-filter <prefix-filter-name> network <ipaddr/mask> all [exact refines between <range>] [host-net] [restrict] [sequence <seq-num>]</code>
<code>ldp add import-filter request mapping nexthop <ip address> neighbor <ip address> interface <name> prefix-filter <prefix-filter-name> network <ipaddr/mask> all [exact refines between <range>] [host-net] [restrict] [sequence <seq-num>]</code>
<code>ldp add interface <name> <ip-address> all></code>
<code>ldp add l2-fec {[vlan <vlanid>]}[customer-id <cust-id>]} to-peer <ipaddr></code>
<code>ldp add prefix-filter <name> network <ipaddr/mask> all [exact refines between <range>] [host-net]</code>
<code>ldp add remote-peer <ipaddr></code>
<code>ldp clear all {interface <name> <ip-address>} peer <ip-address> statistics</code>
<code>ldp map ports <port-list> customer-id <cust-id></code>
<code>ldp set egress-policy [peer-address <ipaddr> <ipaddr-list>] route-map <route-map> sequence <sequence></code>
<code>ldp set global loop-detection-enable path-vector-limit <number></code>
<code>ldp set interface <name> <ip-address> all link-hello-hold-time <seconds> remote-hello-hold-time <seconds> keepalive-timeout <seconds></code>
<code>ldp set l2-fec transport-lsp <lsp-name> {[vlan <vlanid> any]} [customer-id <cust-id> any]} to-peer <ipaddr> [alternate-acceptable] [no-switchback]</code>
<code>ldp set md5-password <password> [interface <name> <ipaddr>] [peer <ipaddr>]</code>
<code>ldp set remote-peer <ipaddr> hello-hold-time <seconds> keepalive-timeout <seconds></code>
<code>ldp set trace-level <level></code>

ldp set trace-options <i><option></i>
ldp show all
ldp show database
ldp show global
ldp show interface <i><name></i> <i><ip-address></i> all [verbose]
ldp show l2-fec [neighbor <i><ip-address></i>]
ldp show neighbor <i><ip-address></i> all [verbose]
ldp show session <i><name></i> <i><ip-address></i> all [verbose]
ldp show statistics
ldp start

ldp add export-filter

Mode

Configure

Format

```
ldp add export-filter request|mapping nexthop <ip address> neighbor <ip address> interface
<name> prefix-filter <prefix-filter-name> network <ipaddr/mask> |all [exact|refines|between
<range>] [host-net] [restrict] [sequence <seq-num>]
```

Description

The **ldp add export-filter** command allows you to filter label requests or label bindings sent to other LDP routers. If you add more than one filter with the same **nexthop**, **neighbor** or **interface** value, the filters are appended (and executed) in order of ascending sequence number.

Parameter	Value	Meaning
export-filter	request	Specifies an outgoing label request.
	mapping	Specifies an outgoing label mapping.
nexthop	<ip address>	Matches label requests or mappings to the neighbor advertising the specified nexthop IP address. Specify an IP address in the form a . b . c . d.
neighbor	<ip address>	Matches label requests or mappings to this LDP router ID. Specify an IP address in the form a . b . c . d
interface	<name>	Matches label requests or mappings to a neighbor that is adjacent over the specified interface. Specify an interface name.
prefix-filter	<prefix-filter-name>	Specifies the LDP prefix filter for export. Specify the name of a prefix filter that was created with the ldp add prefix-filter command.
network	<ipaddr/mask> all	Specifies the networks that are to be filtered. Specify an IP address/netmask in either the 1.2.3.4/255.255.0.0 or 1.2.3.4/16 form. Specify all to match any network. You can also specify the parameters exact , refines , and between to further define the routes to be exported.
exact		Specifies that the netmask of the routes to be exported must exactly match the specified netmask. This is used to match a network, but not the subnets or hosts of that network.
refines		Specifies that the netmask of the routes to be exported must be more specific (longer) than the specified netmask. This is used to match subnets or hosts of a network, but not the network.

Parameter	Value	Meaning
between	< <i>range</i> >	Specifies that the netmask of the routes to be exported must be as or more specific (as long as or longer) than the first number in the range and no more specific (as long as or shorter) than the second number in the range.
host-net		Specifies that the network is a host. This is equivalent to specifying network with a netmask of 255.255.255.255, along with the exact parameter.
restrict		Specifies that LDP label requests and LDP label mappings are <i>not</i> sent.
sequence	< <i>seq-num</i> >	Number that indicates the position a new LDP export filter is to have in the list of export filters already configured with the same nexthop , neighbor or interface value. Export filters with the same identifier are executed in the order of increasing sequence numbers.

Restrictions

None

Example

The following command prevents the label bindings for 10.10.10.10/32 from being advertised to the neighbor router 1.1.1.1:

```
rs(config)# ldp add export-filter mapping network 10.10.10.10/32 restrict neighbor  
1.1.1.1 sequence 1
```

ldp add import-filter

Mode

Configure

Format

```
ldp add import-filter request|mapping nexthop <ip address> neighbor <ip address> interface
<name> prefix-filter <prefix-filter-name> network <ipaddr/mask> |all [exact|refines|between
<range>] [host-net] [restrict] [sequence <seq-num>]
```

Description

The **ldp add import-filter** command allows you to filter label requests or label bindings sent from other LDP routers. If you add more than one filter with the same **nexthop**, **neighbor** or **interface** value, the filters are appended (and executed) in order of ascending sequence number.

Parameter	Value	Meaning
import-filter	request	Specifies an incoming label request.
	mapping	Specifies an incoming label mapping.
nexthop	<ip address>	Matches label requests or mappings from the neighbor advertising the specified nexthop IP address. Specify an IP address in the form a.b.c.d.
neighbor	<ip address>	Matches label requests or mappings from this LDP router ID. Specify an IP address in the form a.b.c.d
interface	<name>	Matches label requests or mappings from a neighbor that is adjacent over the specified interface. Specify an interface name.
prefix-filter	<prefix-filter-name>	Specifies the LDP prefix filter for import. Specify the name of a prefix filter that was created with the ldp add prefix-filter command.
network	<ipaddr/mask> all	Specifies the networks that are to be filtered. Specify an IP address/netmask in either the 1.2.3.4/255.255.0.0 or 1.2.3.4/16 form. Specify all to match any network. You can also specify the parameters exact , refines , and between to further define the routes to be exported.
exact		Specifies that the netmask of the routes to be exported must exactly match the specified netmask. This is used to match a network, but not the subnets or hosts of that network.
refines		Specifies that the netmask of the routes to be exported must be more specific (longer) than the specified netmask. This is used to match subnets or hosts of a network, but not the network.

Parameter	Value	Meaning
between	<range>	Specifies that the netmask of the routes to be exported must be as or more specific (as long as or longer) than the first number in the range and no more specific (as long as or shorter) than the second number in the range.
host-net		Specifies that the network is a host. This is equivalent to specifying network with a netmask of 255.255.255.255, along with the exact parameter.
restrict		Specifies that LDP label requests are <i>not</i> answered and LDP label mappings are <i>not</i> installed.
sequence	<seq-num>	Number that indicates the position a new LDP import filter is to have in the list of import filters already configured with the same nexthop , neighbor or interface value. Import filters with the same identifier are executed in the order of increasing sequence numbers.

Restrictions

None

Example

The following commands deny bindings for 10.10.10.10/32 from neighbor router 1.1.1.1 while allowing all other bindings from the same neighbor router. Note that the more restrictive filter command has the lower sequence number and will be executed first.

```
rs(config)# ldp add import-filter mapping network 10.10.10.10/32 restrict neighbor  
1.1.1.1 sequence 1  
rs(config)# ldp add import-filter mapping network all neighbor 1.1.1.1 sequence 2
```


ldp add interface

Mode

Configure

Format

```
ldp add interface <name> | <ip-address> | all
```

Description

The **ldp add interface** command enables LDP on an interface.

Parameter	Value	Meaning
interface	<name> <ip-address>	Specifies an interface. LDP is enabled on this interface. Specify an interface name or an IP address.
	all	Specify all to enable LDP on all interfaces.

Restrictions

None

Example

The following command enables LDP on the interface 'group1':

```
rs(config)# ldp add interface group1
```

ldp add l2-fec

Mode

Configure

Format

```
ldp add l2-fec {[vlan <vlanid>][customer-id <cust-id>]} to-peer <ipaddr>
```

Description

The **ldp add l2-fec** command allows you to specify an L2 forwarding equivalence class (FEC) for which a label mapping will be sent to the specified remote LDP peer. You can specify either a VLAN ID or a customer ID (created with the **ldp map ports** command) or both a VLAN ID and customer ID.

If only the VLAN ID is specified, the label mapping is for a specific VLAN ID provided by the ISP. If only the customer ID is specified, the label mapping is for a specific port associated with a particular customer. If both VLAN ID and customer ID are specified, the label mapping is for a specific port associated with a specific customer for a customer-specified VLAN.

Parameter	Value	Meaning
vlan	<vlanid>	Specifies the ID of the VLAN for which label mapping will be sent. Specify a value between 1-4094.
customer-id	<cust-id>	Specifies a customer ID value between 1-4294967295 that represents a customer ID to port mapping. The customer ID is created using the ldp map ports command.
to-peer	<ipaddr>	Specifies the remote LDP peer. Specify an IP address in the form a.b.c.d.

Restrictions

None

Example

The following command specifies that label mapping for VLAN 1000 be sent to the LDP peer 10.10.10.101:

```
rs(config)# ldp add l2-fec vlan 1000 to-peer 10.10.10.101
```

ldp add prefix-filter

Mode

Configure

Format

```
ldp add prefix-filter <name> network <ipaddr/mask> [all [exact|refines|between <range>]
[host-net]
```

Description

The **ldp add prefix-filter** command allows you to define an LDP prefix filter. You can then use the LDP prefix filter with the **ldp add export-filter** or **ldp add import-filter** commands to filter label requests or bindings. If you add more than one filter with the same name, the new filter is appended to the existing filter.

Parameter	Value	Meaning
prefix-filter	<name>	Name of the LDP prefix filter.
network	<ipaddr/mask> all	Specifies the networks that are to be filtered. Specify an IP address/netmask in either the 1.2.3.4/255.255.0.0 or 1.2.3.4/16 form. Specify all to match any network. You can also specify the parameters exact , refines , and between to further define the destination.
exact		Specifies that the netmask of the destination must exactly match the specified netmask. This is used to match a network, but not the subnets or hosts of that network.
refines		Specifies that the netmask of the destination must be more specific (longer) than the specified netmask. This is used to match subnets or hosts of a network, but not the network.
between	<range>	Specifies that the netmask of the destination must be as or more specific (as long as or longer) than the first number in the range and no more specific (as long as or shorter) than the second number in the range.
host-net		Specifies that the network is a host. This is equivalent to specifying network with a netmask of 255.255.255.255, along with the exact parameter.

Restrictions

None

Example

In the following example, the **ldp add prefix-filter** command defines a prefix filter for the host node 10.10.10.101. The subsequent commands use the prefix filter to prevent requests or bindings for 10.10.10.101 from being sent to other LDP routers.

```
rs(config)# ldp add prefix-filter 101serv network 10.10.10.101/32 host-net
rs(config)# ldp add export-filter request restrict prefix-filter 101serv neighbor
1.1.1.1 sequence 1
rs(config)# ldp add export-filter mapping restrict prefix-filter 101serv neighbor
1.1.1.1 sequence 1
```

Ldp add remote-peer

Mode

Configure

Format

```
ldp add remote-peer <ipaddr>
```

Description

When LDP is started on the RS, the router automatically finds and establishes communications with LDP peers that are directly connected. The **ldp add remote-peer** command allows you to specify an LSR that is *not* directly connected that the router should communicate with via LDP.

Parameter	Value	Meaning
remote-peer	<ipaddr>	The router ID, in the form a.b.c.d., of the LDP peer that is not directly connected to the local router.
 Note The router ID of the remote peer must be the loopback address of the remote router.		

Restrictions

None

Example

The following command specifies the IP address 100.127.139.145 as an LDP peer:

```
rs(config)# ldp add remote-peer 100.127.139.145
```

ldp clear

Mode

Enable

Format

```
ldp clear all | {interface <name> | <ip-address>} | peer <ip-address> | statistics
```

Description

The **ldp clear** command allows you to clear LDP sessions.

Parameter	Value	Meaning
all		Clears all LDP sessions on the router, including remote sessions.
interface	<name> <ip-address>	Clears LDP session that have been established on this interface, including remote sessions. Specify an interface name or an IP address.
peer	<ip-address>	Clears the LDP session with the peer specified by the IP address.
statistics		Clears LDP statistics that are displayed with the ldp show statistics command.

Restrictions

None.

Example

The following command clears LDP sessions on the interface 'int1':

```
rs(config)# ldp clear interface int1
```

ldp map ports

Mode

Configure

Format

```
ldp map ports <port-list> customer-id <cust-id>
```

Description

The **ldp map ports** command allows you to map one or more ports to a customer identification number. You can then specify the customer ID when defining an L2 FEC for label mapping with the **ldp add l2-fec** command.

Parameter	Value	Meaning
ports	<port-list>	Specifies the port(s) to which the customer ID applies. If you specify more than one port, use commas to separate port names.
customer-id	<cust-id>	Specifies a customer ID that represents a customer ID to port mapping. Specify a value between 1-4294967295.

Restrictions

None

Example

The following command maps Ethernet ports et.3.1 and et.3.2 to the customer ID 2000:

```
rs(config)# ldp map ports et.3.1, et.3.2 customer-id 2000
```

The following command maps ATM port at.4.1 (note that no virtual channel or port number is used) to the customer ID 4002:

```
rs(config)# ldp map ports at.4.1 customer-id 4002
```

ldp set egress-policy

Mode

Configure

Format

```
ldp set egress-policy [peer-address <ipaddr>|<ipaddr-list>] route-map <route-map> sequence <sequence>
```

Description

The **ldp set egress-policy** command allows you to apply an egress policy to LDP peers. The egress policy defines one or more route-maps that allow routes to be imported or exported to the LDP peers.

Parameter	Value	Meaning
peer-address	<ipaddr> <ipaddr-list>	Specifies the router ID of the LDP peer(s) to which this policy applies. To specify multiple peers, separate the router IDs with spaces and enclose the list in quotation marks.
route-map	<route-map>	Name of the route-map. Define route-maps with the route-map permit/deny command. If peer-address is not defined, this route-map is applied to all LDP peers.
sequence	<sequence>	Specifies the sequence in which this route-map defined with route-map is applied. Specify a number between 1-65535.

Restrictions

None

Example

The following command applies the route-map '10-net-routes' to the LDP peer 1.1.1.1:

```
rs(config)# ldp set egress-policy peer-address 1.1.1.1 route-map 10-net-routes  
sequence 1
```


ldp set global

Mode

Configure

Format

```
ldp set global hop-count-loop-detection-enable|path-vector-loop-detection-enable  
path-vector-limit <number>
```

Description

The **ldp set global** command allows you to configure LDP parameters for the entire router. Loop detection is disabled by default on the RS. The **ldp set global** command allows you to enable loop detection based on either hop count or path vector and specify the path vector limit that applies to either type of loop detection.

Parameter	Value	Meaning
hop-count-loop-detection-enable		Enables loop detection based on hop count.
path-vector-loop-detection-enable		Enables loop detection based on path vector.
path-vector-limit	<number>	Specifies the path vector limit. This limit also applies for loop detection based on hop count. Specify a number between 1-255.

Restrictions

None

Example

The following command enables loop detection based on hop count with a path vector limit of 100:

```
rs(config)# ldp set global hop-count-loop-detection-enable path-vector-limit 100
```

ldp set interface

Mode

Configure

Format

```
ldp set interface <name> | <ip-address> | all link-hello-hold-time <seconds>  
remote-hello-hold-time <seconds> keepalive-timeout <seconds>
```

Description

The **ldp set interface** command allows you to configure various parameters on an LDP interface. LDP uses hello and keepalive messages to validate that the LSR peer and link are still active, maintaining connectivity with adjacent nodes.

Parameter	Value	Meaning
interface	<name > <ip-address>	Specifies the LDP interface. Specify an interface name or IP address.
	all	Specify all to configure all LDP interfaces.
link-hello-hold-time	<seconds>	Sets the hold timer, in seconds, for LDP link hello messages. If a hello message is not received by an LDP neighbor before this timer expires, the local LDP router is considered to be down. Specify a value between 1-65535. The default value is 15 seconds.
remote-hello-hold-time	<seconds>	Sets the hold time for LDP remote hello messages. If a hello message is not received by a remote LDP peer before this timer expires, the local LDP router is considered to be down. Specify a value between 1-65535. The default value is 15 seconds.
keepalive-timeout	<seconds>	Sets the keepalive timeout for an LDP session with a remote peer. A keepalive message is sent if there is no other LDP traffic on the session. If a keepalive or other LDP message is not received before the keepalive timeout, the LDP session is considered failed. Specify a value between 1-65535. The default value is 30 seconds.

Restrictions

None

Example

The following command sets various parameters on the LDP interface 'R1OUT':

```
rs(config)# ldp set interface R1OUT link-hello-hold-time 20 remote-hello-hold-time  
45 keepalive-timeout 35
```

ldp set l2-fec

Mode

Configure

Format

```
ldp set l2-fec transport-lsp <lsp-name> {[vlan <vlanid>|any]}[customer-id <cust-id>|any]}
to-peer <ipaddr> [alternate-acceptable] [no-switchback]
```

Description

The **ldp set l2-fec** command allows you to specify an LSP that is to be used as a transport LSP when a label is received for an L2 FEC from a remote LDP peer. The transport LSP, also referred to as a “tunnel LSP,” transports L2 frames from an ingress LSR to the egress LSR across an MPLS network. The specified transport LSP must be an RSVP-signaled LSP, although you can specify either an RSVP- or LDP-signaled LSP as an alternate transport LSP.

You can specify either a VLAN ID or a customer ID (created with the **ldp map ports** command) or both a VLAN ID and customer ID to specify the transport LSP. If only the VLAN ID is specified, the transport LSP is for a specific VLAN. If only the customer ID is specified, the transport LSP is for a specific port associated with a particular customer. If both VLAN ID and customer ID are specified, the transport LSP is for a specified port associated with a specific customer for the specified VLAN.

Parameter	Value	Meaning
transport-lsp	<lsp-name>	The name of an RSVP-signaled LSP that is to be used as the transport LSP.
vlan	<vlanid>	Specifies the ID of the VLAN for which label mapping will be sent. Specify a value between 1-4094.
	any	Specifies any VLAN.
customer-id	<cust-id>	Specifies a customer ID value between 1-4294967295 that represents a customer ID to port mapping. The customer ID is created using the ldp map ports command.
	any	Specifies any customer ID.
to-peer	<ipaddr>	Specifies the remote LDP peer. Specify an IP address in the form a.b.c.d.
alternate-acceptable		Specifies that an RSVP or LDP-signaled LSP can be used as an alternate transport LSP if the LSP specified with the transport-lsp parameter is not active. If the transport LSP later becomes active, it will override the alternate LSP unless the no-switchback option is specified.
no-switchback		Specifies not to switch back from the alternate LSP to the configured transport LSP when the transport LSP becomes available.

Restrictions

None

Example

The following command specifies that LSP1 is to be used as the transport LSP to the specified peer when a label mapping for VLAN 1000 is received from the peer:

```
rs(config)# ldp set l2-fec transport-lsp LSP1 vlan 1000 to-peer 10.10.10.101
```

ldp set md5-password

Mode

Configure

Format

```
ldp set md5-password <password> [interface <name>|<ipaddr>] [peer <ipaddr>]
```

Description

The **ldp set md5-password** command allows you to configure the TCP MD5 password for LDP sessions. You can optionally specify the interface and/or the peer for which the MD5 password applies. Otherwise, the MD5 password applies to all LDP sessions on the router.

Parameter	Value	Meaning
md5-password	<password>	Specify a string of up to 80 characters for the password. The password is case-sensitive.
interface	<name> <ipaddr>	Specifies the interface on which the MD5 password applies. All LDP sessions on this interface will use this password.
peer	<ipaddr>	Specifies the transport address of the peer for which the MD5 password applies. The transport address is the address of the interface used by the peer for the LDP session.
 Note For RS routers, the transport address is the address of the interface specified with the ldp add interface command and <i>not</i> the address of the loopback interface. Use the ldp show neighbor command with the verbose option to see the transport address for the peer.		

Restrictions

None

Example

The following command sets the MD5 password 'rsadmin' for all LDP sessions on the router:

```
rs(config)# ldp set md5-password rsadmin
```

ldp set remote-peer

Mode

Configure

Format

```
ldp set remote-peer <ipaddr> hello-hold-time <seconds> keepalive-timeout <seconds>
```

Description

The **ldp set remote-peer** command allows you to set LDP parameters for a remote peer specified with the **ldp add remote-peer** command. The session with the remote peer is restarted if there is any change.

Parameter	Value	Meaning
remote-peer	<ipaddr>	Specifies the IP address of the remote peer.
hello-hold-time	<seconds>	Sets the hold time for LDP remote hello messages. If a hello message is not received by the remote LDP peer before this timer expires, the local router is considered to be down. Specify a value between 1-65535. The default value is 15 seconds.
keepalive-timeout	<seconds>	Sets the keepalive timeout for an LDP session with a remote peer. A keepalive message is sent if there is no other traffic on the LDP session. If a keepalive or other LDP message is not received before the keepalive timeout, the LDP session is considered failed. Specify a value between 1-65535. The default value is 30 seconds.

Restrictions

None

Example

The following command sets the keepalive timeout with peer 100.100.101.125 to 40 seconds:

```
rs(config)# ldp set remote-peer 100.100.101.125 keepalive-timeout 40
```

ldp set trace-level

Mode

Enable

Format

```
ldp set trace-level <level>
```

Description

The **ldp set trace-level** command allows you to configure the level of LDP tracing.

Parameter	Value	Meaning
trace-level	<level>	Specifies the LDP tracing level. Specify 0 to disable tracing. Otherwise, specify a value between 1-4, where 4 provides the most detailed level of tracing.

Restrictions

None.

Example

The following command configures detailed tracing:

```
rs# ldp set trace-level 4
```


ldp set trace-options

Mode

Enable/
Configure

Format

```
ldp set trace-options <option>
```

Description

The **ldp set trace-options** command allows you to enable the type of tracing that is performed on LDP traffic.

Parameter	Value	Meaning
trace-options	<option>	Specifies the type of tracing to be performed. Specify one or more of the following:
	address	Trace address and address withdrawal messages.
	hello	Trace hello messages.
	initialization	Trace initialization messages.
	interface	Trace packets only on this interface.
	keepalive	Trace keepalive messages.
	label	Trace label request, label map, label withdrawal, label release and label abort messages.
	notification	Trace notification messages.
	packet	Trace all packets.
	peer	Trace packets from/to all peers with this address LSR ID portion of LDP ID.
	receive	Trace only received packets.
	send	Trace only packets being sent.

Restrictions

None

Example

The following command enables all packets to be traced:

```
rs# ldp set trace-options packet
```

ldp show all

Mode

Enable

Format

ldp show all

Description

The **ldp show all** command allows you to display various LDP information and statistics.

Restrictions

None.

Example

The following is an example of the **ldp show all** command:

```
RS# ldp show all
Global parameters
-----

Ordered control mode
Loop detection disabled

Interface parameters
-----

Interface          Label space          Nbr count  Next
hello(seconds)
rt1-rt3.mp         113.2.2.1:0          1           2
rt1-rt6.mp2        116.3.3.1:0          1           2

Neighbor parameters
-----

Address            Interface            Label space ID      Hold
Time(seconds)
116.3.3.6          rt1-rt6.mp2          6.6.6.6:0           14
113.2.2.3          rt1-rt3.mp           3.3.3.3:0           12

Session parameters
-----

Address            State                Connection          Hold Time(seconds)
116.3.3.6          Operational          Open                14
113.2.2.3          Operational          Open                12

Label Database
-----

Input label database, 1.1.1.1:0-6.6.6.6:0
Label Prefix
2058 3.3.3.3/32
2059 1.1.1.1/32
16 6.6.6.6/32

Output label database, 1.1.1.1:0-6.6.6.6:0
```

Label	Prefix
2050	3.3.3.3/32
2051	6.6.6.6/32
16	1.1.1.1/32
Input label database, 1.1.1.1:0-3.3.3.3:0	
Label	Prefix
2052	1.1.1.1/32
2053	6.6.6.6/32
16	3.3.3.3/32
Output label database, 1.1.1.1:0-3.3.3.3:0	
Label	Prefix
2050	3.3.3.3/32
2051	6.6.6.6/32
16	1.1.1.1/32

Table 36-1 Display field descriptions for the ldp show all command

Field	Description
Global parameters	Displays the values of LDP global parameters. See the ldp show global command for specific information.
Interface parameters	Displays LDP interface information. See the ldp show interface command for specific information.
Neighbor parameters	Displays information about LDP neighbors. See the ldp show neighbor command for specific information.
Session parameters	Displays LDP session information. See the ldp show session command for specific information.
Label Database	Displays the LDP database. See the ldp show database command for specific information.

ldp show database

Mode

Enable

Format

```
ldp show database
```

Description

The **ldp show database** command allows you to display the LDP label database. The database consists of input and output labels exchanged for each LDP session.

Restrictions

None.

Examples

The following is an example of the **ldp show database** command:

```
RS# ldp show database

Input label database, 1.1.1.1:0-6.6.6.6:0
Label      Prefix
 2058      3.3.3.3/32
 2059      1.1.1.1/32
   16      6.6.6.6/32

Output label database, 1.1.1.1:0-6.6.6.6:0
Label      Prefix
 2050      3.3.3.3/32
 2051      6.6.6.6/32
   16      1.1.1.1/32

Input label database, 1.1.1.1:0-3.3.3.3:0
Label      Prefix
 2052      1.1.1.1/32
 2053      6.6.6.6/32
   16      3.3.3.3/32

Output label database, 1.1.1.1:0-3.3.3.3:0
Label      Prefix
 2050      3.3.3.3/32
 2051      6.6.6.6/32
   16      1.1.1.1/32
```

Table 36-2 Display field descriptions for the ldp show database command

Field	Description
Input label database	Labels received from another LSR on the indicated LDP session.
Output label database	Labels advertised to another LSR on the indicated LDP session.
Label	Received or advertised labels on the LDP session.
Prefix	Route prefix.

The following is an example of the **ldp show database** command with the **verbose** option:

```

RS# ldp show database verbose

Input label database, 1.1.1.1:0-6.6.6.6:0
  Label    Prefix
  2058     3.3.3.3/32
           State:Active
  2059     1.1.1.1/32
           State:Active
  16       6.6.6.6/32
           State:Active

Output label database, 1.1.1.1:0-6.6.6.6:0
  Label    Prefix
  2050     3.3.3.3/32
           State:Active
  2051     6.6.6.6/32
           State:Active
  16       1.1.1.1/32
           State:Active

Input label database, 1.1.1.1:0-3.3.3.3:0
  Label    Prefix
  2052     1.1.1.1/32
           State:Active
  2053     6.6.6.6/32
           State:Active
  16       3.3.3.3/32
           State:Active

Output label database, 1.1.1.1:0-3.3.3.3:0
  Label    Prefix
  2050     3.3.3.3/32
           State:Active
  2051     6.6.6.6/32
           State:Active
  16       1.1.1.1/32
           State:Active

```

The **verbose** option shows the state of the label binding. State values and their descriptions are shown in [Table 36-3](#):

Table 36-3 LDP label binding state values

State	Description
Active	Label is installed and distributed. This is the typical state.
Filtered	Label binding is filtered, either with the ldp add export-filter or ldp add import-filter command. Input label bindings that are marked “Filtered” are not considered for LSP establishment and are not advertised to other LDP peers. Output label bindings that are marked “Filtered” can be considered for LSP establishment on the local router but are not advertised to other LDP peers.
New	New label is not yet distributed.
MapRcv	Waiting to receive label binding.
MapSend	Waiting to send label binding.
ReIRcv	Waiting to receive label release.
ReIRsnd	Waiting to receive label release before sending label binding.
ReISend	Waiting to send label release.
ReqSend	Waiting to send label request.
W/dSend	Waiting to send label withdrawal.

ldp show global

Mode

Enable

Format

```
ldp show global
```

Description

The **ldp show global** command allows you to display the values of LDP global parameters. Default parameter values can be changed using the **ldp set global** command.

Restrictions

None.

Example

The following is an example of the **ldp show global** command that shows the default LDP global parameter settings:

```
RS# ldp show global
Ordered control mode
Loop detection disabled
```

ldp show interface

Mode
Enable

Format

ldp show interface <name>|<ip-address>|all [verbose]

Description

The **ldp show interface** command allows you to display LDP interface information.

Parameter	Value	Meaning
interface	<name> <ip-address>	Displays LDP interface information. Specify an interface name or an IP address.
	all	Specify all to display information on all interfaces.
verbose		Displays detailed information.

Restrictions

None.

Examples

The following is an example of the **ldp show interface** command:

RS# ldp show interface all				
Interface	Label space	Nbr count	Next hello(seconds)	
rt1-rt3.mp	113.2.2.1:0	1	0	
rt1-rt6.mp2	116.3.3.1:0	1	0	

Table 36-4 Display field descriptions for the ldp show interface command

Field	Description
Interface	Name of the interface.
Label space	Label space identifier that the router is advertising on this interface.
Nbr count	Number of LDP neighbors on this interface.
Next hello	Number of seconds until the next hello packet is sent on this interface.

The following is an example of the **ldp show interface** command with the **verbose** option:

```
RS# ldp show interface all verbose
Interface          Label space          Nbr count  Next hello(seconds)
rt1-rt3.mp         113.2.2.1:0          1           2
  Hold time: 15, Liberal label retention, Downstream unsolicited
rt1-rt6.mp2        116.3.3.1:0          1           2
  Hold time: 15, Liberal label retention, Downstream unsolicited
```

Table 36-5 Display field descriptions for the ldp show interface verbose command

Field	Description
Interface	Name of the interface.
Label space	Label space identifier that the router is advertising on this interface.
Nbr count	Number of LDP neighbors on this interface.
Next hello	Number of seconds until the next hello packet is sent on this interface.
Hold time	Number of seconds for hello hold time.
Liberal label retention	Label retention mode for this interface. Liberal is the default mode.
Downstream unsolicited	Label advertisement method for this interface. Downstream unsolicited is the default method.

ldp show l2-fec

Mode

Enable

Format

ldp show l2-fec [neighbor <ip-address>]

Description

The **ldp show l2-fec** command allows you to display the labels that have been sent or received for L2 FECs and the transport LSPs selected for the FEC.

Parameter	Value	Meaning
neighbor	<ip-address>	Displays the labels that have been sent to or received from the specified LDP peer. Specify the router ID of the LDP peer. If you do not specify the neighbor parameter, then information is displayed for all L2 FECs configured on the RS.

Restrictions

None.

Example

The following is an example of the **ldp show l2-fec** command:

```
RS# ldp show l2-fec

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 2.2.2.2:0
FEC                               in-lbl  out-lbl  Transport LSP name/label
VLAN ID 55                        2136    2136    LDP 0.0.0.0/17
Customer ID 33                    2137    2137    LDP 0.0.0.0/17

Remote neighbor 6.6.6.6:0
FEC                               in-lbl  out-lbl  Transport LSP name/label
VLAN ID 60                        2138    2138    LDP 0.0.0.0/18
Customer ID 66                    2139    2139    LDP 0.0.0.0/18
```

The following is an example of the **ldp show l2-fec** command with the **neighbor** option:

```
RS# ldp show l2-fec neighbor 2.2.2.2
FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent
Remote neighbor 2.2.2.2:0
FEC                               in-lbl  out-lbl  Transport LSP name/label
VLAN ID 55                       2136    2136    LDP 0.0.0.0/17
Customer ID 33                   2137    2137    LDP 0.0.0.0/17
```

ldp show neighbor

Mode
Enable

Format

ldp show neighbor <ip-address>|all [verbose]

Description

The **ldp show neighbor** command allows you to display information about LDP neighbors.

Parameter	Value	Meaning
neighbor	<ip-address>	Displays information about LDP neighbors. Specify the router ID of the LDP peer.
	all	Specify all to display information on all neighbors.
verbose		Displays detailed information.

Restrictions

None.

Example

The following is an example of the **ldp show neighbor** command:

RS# ldp show neighbor all			
Address	Interface	Label space ID	Hold Time(seconds)
116.3.3.6	rt1-rt6.mp2	6.6.6.6:0	14
113.2.2.3	rt1-rt3.mp	3.3.3.3:0	12

Table 36-6 Display field descriptions for the ldp show neighbor command

Field	Description
Address	Neighbor’s IP address.
Interface	Interface on which neighbor was discovered.
Label space ID	Label space identifier advertised by neighbor.
Hold Time	Seconds before the neighbor expires.

The following is an example of the **ldp show neighbor** command with the **verbose** option:

RS# ldp show neighbor all verbose			
Address	Interface	Label space ID	Hold Time(seconds)
116.3.3.6	rt1-rt6.mp2	6.6.6.6:0	12
Transport address: 116.3.3.6			
113.2.2.3	rt1-rt3.mp	3.3.3.3:0	7
Transport address: 113.2.2.3			

Table 36-7 Display field descriptions for the ldp show neighbor verbose command

Field	Description
Address	Neighbor's IP address.
Interface	Interface on which neighbor was discovered.
Label space ID	Label space identifier advertised by neighbor.
Hold Time	Seconds before the neighbor expires.
Transport address	Address to which the LDP session with the neighbor is to be established.

ldp show session

Mode

Enable

Format

```
ldp show session <name>|<ip-address>|all [verbose]
```

Description

The **ldp show session** command allows you to display LDP session information.

Parameter	Value	Meaning
session	<name>	Displays LDP session information. Specify an interface name to show all sessions over that interface.
	<ip-address>	Specify the router ID of the LDP peer to show all sessions to that router.
	all	Specify all to display information on all neighbors.
verbose		Displays detailed information.

Restrictions

None.

Examples

The following is an example of the **ldp show session** command:

RS# ldp show session all					
Codes: Tx - Sent, Rx tot - Received Total, Rx fltd - Received Filtered					
Address	State	Connection	Hold Time(sec)	Tx/Rx tot/Rx fltd	
5.20.10.2	Operational	Open	12	975/1/0	

Table 36-8 Display field descriptions for the ldp show session command

Field	Description
Address	Session transport address.
State	Session state. It can be one of the following states: • Nonexistent: session does not exist. • Connecting: TCP session connection is being established. • Initialized: TCP session connection is established. • OpenSent: Initialization or keepalive messages being transmitted. • OpenRec: Keepalive messages being transmitted. • Operational: Receiving or transmitting shutdown message. • Closing: Closing session connection.
Connection	TCP connection state. It can be one of the following states: • Closed • Opening • Open
Hold Time	Seconds before the session will be closed.
Tx	Number of labels sent.
Rx tot	Total number of labels received.
Rx fltd	Number of labels received and filtered.

The following is an example of the **ldp show session** command with the **verbose** option:

```
RT1# ldp show session all verbose
Address: 5.20.10.2, State: Operational, Connection: Open, Hold time: 12
Labels Sent 1125, Received total 1, Received filtered 0
Session ID: 159.1.1.2:0--159.1.1.15:0
Next keepalive in 0 seconds
Passive, Maximum PDU: 4096, Hold time: 15 seconds
Keepalive interval: 10 seconds, Connect retry interval: 14 seconds
Local address: 5.20.10.1, Remote address: 5.20.10.2
Next-hop addresses received:
  40.1.1.2
  40.2.1.2
  40.3.1.2
  40.4.1.2
  5.20.10.2
```

Table 36-9 Display field descriptions for the ldp show session verbose command

Field	Description
Address	Session transport address.
State	Session state. It can be one of the following states: • Nonexistent: session does not exist. • Connecting: TCP session connection is being established. • Initialized: TCP session connection is established. • OpenSent: Initialization or keepalive messages being transmitted. • OpenRec: Keepalive messages being transmitted. • Operational: Receiving or transmitting shutdown message. • Closing: Closing session connection.
Connection	TCP connection state. It can be one of the following states: • Closed • Opening • Open
Hold Time	Seconds before the session will be closed.
Labels Sent	Number of labels transmitted.
Received total	Number of labels received.
Received filtered	Number of labels received and filtered.
Session ID	Session identifier.
Next keeaplive	Seconds until next keepalive is sent.
Maximum PDU	Maximum PDU size for session.
Hold time	Seconds for session hold time.
Keepalive interval	Keepalive interval (in seconds).
Connect retry interval	TCP connection retry interval (in seconds).
Local address	Local transport address.
Remote address	Remote transport address.
Next-hop addresses received	Next-hop addresses that were received on the LDP session.

ldp show statistics

Mode

Enable

Format

```
ldp show statistics
```

Description

The **ldp show statistics** command allows you to display LDP statistics. Use the **ldp clear statistics** command to reset the statistics counters.

Restrictions

None.

Example

The following is an example of the **ldp show statistics** command:

rs# ldp show statistics					
Message type		Total		Last 5 seconds	
=====		=====		=====	
Sent	Received	Sent	Received		
----	-----	----	-----		
Hello		1438	1438	0	2
Initialization		29	29	0	0
Keepalive		697	696	0	0
Notification		27	1	0	0
Address		87	117	0	0
Address withdraw		0	0	0	0
Label mapping		80	213	0	0
Label request		0	0	0	0
Label withdraw		7	2	0	0
Label release		1	2	0	0
Label abort		0	0	0	0
All UDP		1438	1438	0	2
All TCP		928	816	0	0
Event type		Total		Last 5 seconds	
=====		=====		=====	
Sessions opened		36		0	
Sessions closed		34		0	
Shutdown received		1		0	
Shutdown sent		34		0	
Keep alive expired		0		0	
Malformed TLV		0		0	
Bad TLV length		0		0	
Bad message length		0		0	
Bad PDU length		0		0	
Bad LDP identifiers		0		0	
Hello errors		0		0	
Advertisement errors		0		0	
Max PDU errors		0		0	
Label range errors		0		0	

Table 36-10 Display field descriptions for the ldp show statistics command

Field	Description
Message type	Type of LDP message.
Total Sent	Number of each LDP message type that was sent.
Total Received	Number of each LDP message type that was received.
Last 5 seconds Sent	Number of each LDP message type that was sent in the last 5 seconds.
Last 5 seconds Received	Number of each LDP message type that was received in the last 5 seconds.

Table 36-10 Display field descriptions for the ldp show statistics command

Field	Description
Event type	Type of LDP event or error.
Total	Number of each type of LDP event or error.
Last 5 seconds	Number of each type of LDP event or error that occurred in the last 5 seconds.

ldp start

Mode

Configure

Format

ldp start

Description

The **ldp start** command allows you to start LDP on the RS. You must first enable LDP on the appropriate interfaces with the **ldp add interface** command.

Parameter	Value	Meaning
start		Enables LDP functionality.

Restrictions

None

Example

The following commands enable LDP on the interface 'group1' and then start LDP on the RS:

```
rs(config)# ldp add interface group1
rs(config)# ldp start
```

37 LFAP COMMANDS

The `lfap` commands let you configure the LFAP agent on the RS and manage the Layer-3 IP accounting information that is delivered by TCP to an external server.

37.1 COMMAND SUMMARY

The following table lists the **lfap** commands. The sections following the table describe the command syntax for each command.

<code>lfap set batch-interval <number></code>
<code>lfap set batch-size <number></code>
<code>lfap set lost-contact-interval <number></code>
<code>lfap set poll-interval <number></code>
<code>lfap set priority <number> low medium high</code>
<code>lfap set send <type></code>
<code>lfap set send-queue-max-size <number></code>
<code>lfap set server <IP address(es)></code>
<code>lfap set server-retry-interval <number></code>
<code>lfap show all</code>
<code>lfap show configuration</code>
<code>lfap show servers</code>
<code>lfap show statistics</code>
<code>lfap show status</code>
<code>lfap start</code>

lfap set batch-interval

Mode

Configure

Format

```
lfap set batch-interval <number>
```

Description

The **lfap set batch-interval** command defines the number of seconds between subsequent transmissions of flow creation and deletion information to a FAS.

Parameter	Value	Meaning
batch-interval	<number>	The number of seconds (from 1 to 2,000, inclusive) between transmission of flow creation and deletion information (the interval). The default value is 1.

Restrictions

None

Example

To set the interval between flow creation and deletion transmissions to 5 seconds:

```
rs(config)# lfap set batch-interval 5
```

lfap set batch-size

Mode

Configure

Format

lfap set batch-size <number>

Description

The **lfap set batch-size** command defines the number of flow creation and deletion records included in batch transmissions to a FAS.

Parameter	Value	Meaning
batch-size	<number>	The number of records (from 1 to 2,000, inclusive) contained in a transmission of flow creation and deletion information to a FAS. The default value is 32.

Restrictions

None

Example

To set the number of flow creation and deletion records contained in a batch transmission to 256:

```
rs(config)# lfap set batch-size 256
```

lfap set lost-contact-interval

Mode

Configure

Format

```
lfap set lost-contact-interval <number>
```

Description

The **lfap set lost-contact-interval** command allows you to define the amount of time (in seconds) the LFAP agent will wait before realizing it has lost contact with a FAS and declare the connection lost.

Parameter	Value	Meaning
lost-contact-interval	<number>	The number of seconds (from 20 to 2,000, inclusive) the LFAP agent waits before realizing that it has lost contact with a FAS. The default value is 60.

Restrictions

None

Example

To set the amount of time the LFAP agent waits before realizing that it has lost contact with a FAS to 30 seconds:

```
rs(config)# lfap set lost-contact-interval 30
```


lfap set poll-interval

Mode

Configure

Format

lfap set poll-interval *<number>*

Description

The **lfap set poll-interval** command allows you to set the time period (in minutes) between subsequent transmissions of accounting data to the FAS server.

The poll-interval indicates how often each flow is updated. If the poll-interval is set to 5, then each flow will be updated every 5 minutes. The flow updates are spread out over time so as not to send all of the update messages at once. For instance, say flow A is updated at time 1 minute and flow B is updated at time 2 minutes. Flow A would be updated next at time 6 minutes, and flow B would be updated at time 7 minutes

Parameter	Value	Meaning
poll-interval	<i><number></i>	Defines the number of minutes (from 1 to 1,440, inclusive) between transmissions of accounting data to the FAS server. The default value is 15.

Restrictions

None

Example

To set the number of minutes between accounting data transmissions to the FAS server to 60 minutes:

```
rs(config)# lfap set poll-interval 60
```

lfap set priority

Mode

Configure

Format

lfap set priority <number>| low | medium| high

Description

The **lfap set priority** command allows you to set the priority level of the LFAP tasks. A higher priority indicates that the LFAP tasks will have a chance to run more often. If a number is given, the lower the value of the number, the higher the task priority. Negate this command to set the LFAP tasks priorities back to the default value, which is between low and medium.

Parameter	Value	Meaning
priority		Sets the priority level of the LFAP tasks. You can specify one of the following:
	<number>	Specify this parameter to set the task priority to a numerical value. Specify any number from 50 to 250.
	low	Specify this parameter to set the task priority to low.
	medium	Specify this parameter to set the task priority to medium.
	high	Specify this parameter to set the task priority to high.

Restrictions

None

Example

To set the priority to LFAP task priority to high:

```
rs(config)# lfap set priority high
```

lfap set send

Mode

Configure

Format

lfap set send <type>

Description

The **lfap set send** command allows you to set which information elements are to be sent up to the server. Note that source and destination addresses are not options, as they are always sent up to the server. By default, all information elements are sent up except for the source and destination autonomous system (AS) numbers (src-as and dest-as). The AS numbers are not sent up due to performance reasons. To get the source AS, an extra expensive call has to be made. All of the other information elements are inexpensive to obtain. One reason to turn off information elements, if they are not desired, is to cause the messages that are sent to the server to be smaller, for bandwidth issues. If the command is negated, the sending of the information element returns to its default state.

Parameter	Value	Meaning
src-port	enable disable	Use this parameter to specify whether or not to send source port information. Default is enable.
protocol	enable disable	Use this parameter to specify whether or not to send the protocol ID. Default is enable.
tos	enable disable	Use this parameter to specify whether or not to send type of service information. Default is enable.
src-cce-addr	enable disable	Use this parameter to specify whether or not to send the source CCE address. Default is enable.
priority	enable disable	Use this parameter to specify whether or not to send priority queue information. Default is enable.
ingress	enable disable	Use this parameter to specify whether or not to send ingress port information. Default is enable.
egress	enable disable	Use this parameter to specify whether or not to send egress port information. Default is enable.
src-as	enable disable	Use this parameter to specify whether or not to send the source autonomous system number. Default is disable.
dest-as	enable disable	Use this parameter to specify whether or not to send the destination autonomous system number. Default is disable.

Restrictions

None.

Example

To configure the LFAP message not to carry priority queue information:

```
rs(config)# lfap set send priority disable
```

lfap set send-queue-max-size

Mode

Configure

Purpose

Sets the maximum number of LFAP messages that the send queue can hold before messages are dropped.

Format

```
lfap set send-queue-max-size <number>
```

Description

The **lfap set send-queue-max-size** command allows you to set the maximum number of LFAP messages that the send queue can hold before messages are dropped.

Parameter	Value	Meaning
send-queue-max-size	<number>	The maximum number of messages (from 100 to 2,000,000, inclusive) that the send queue can hold before messages are dropped. The default is 50,000.

Restrictions

An average LFAP message is approximately 100 bytes. You must consider the amount of memory available before you set a high number for the maximum number of messages in the send queue.

Example

To set the maximum send queue size to 100,000 LFAP messages:

```
rs(config)# lfap set send-queue-max-size 100000
```

lfap set server

Mode

Configure

Format

```
lfap set server ["<IP address> [<IP address>] [<IP address>"]]
```

Description

The **lfap set server** command allows you to set up to three FAS IP servers for the LFAP agent to contact.

Parameter	Value	Meaning
server	<IP address>	Sets the IP address of the FAS servers to contact. You may specify a maximum of three IP servers in the command line, separating each IP address with a space. However, if you specify more than one IP server, you must surround the IP addresses in the command line with double-quotes. (See “Examples” below.)

Restrictions

At least one IP server must be configured before the LFAP agent can be started. Also, in order to delete an address from the list of IP servers to contact, you must enter a new **lfap set server** command line. (Simply negating the previous **lfap set server** command will not appropriately counter the initial command execution.)

Examples

To set one IP server to contact:

```
rs (config)# lfap set server 5.5.5.5
```

To set three IP servers to contact:

```
rs (config)# lfap set server "5.5.5.5 6.6.6.6 7.7.7.7"
```

lfap set server-retry-interval

Mode

Configure

Format

```
lfap set server-retry-interval <number>
```

Description

The **lfap set server-retry-interval** command allows you to customize the amount of time (in seconds) the LFAP agent should wait before attempting to restore contact with a lost FAS. After the LFAP agent has attempted to contact each server, it will then wait the specified number of seconds before attempting to resume contact.

Parameter	Value	Meaning
server-retry-interval	<number>	The number of seconds (from 1 to 2,000, inclusive) the LFAP agent will wait before attempting to re-establish contact with a lost FAS. The default value is 60 seconds.

Restrictions

None

Example

To set the number of seconds between attempts to resume contact with a lost FAS to 45:

```
rs(config)# lfap set server-retry-interval 45
```

lfap show all

Mode

Enable

Format

lfap show all

Description

The **lfap show all** command allows you to analyze the current status of the LFAP agent and any servers to which it is currently connected. In the output of the command execution, you will find data pertaining to the following aspects of the LFAP agent:

- LFAP Agent Status (including connection status)
- LFAP Agent Flow Accounting Servers (FASs)
- LFAP Agent Configuration, including the following:
 - poll interval
 - batch size
 - batch interval
 - lost contact interval
 - server retry interval
 - maximum send queue size
 - task priority
 - information elements to be sent or not sent to the server
- LFAP Agent Statistics, including the following:
 - number of servers
 - up time
 - connection successes and failures
 - messages sent/received
 - lost information
 - flows
 - peaks

Restrictions

None

lfap show configuration

Mode

Enable

Format

lfap show configuration

Description

The **lfap show configuration** command allows you to view the current configuration of the LFAP agent. In the output of the command execution, you will find the following LFAP agent configuration data:

- Poll Interval
- Batch Size
- Batch Interval
- Lost Contact Interval
- Server Retry Interval
- Maximum Send Queue Size
- Task Priority Level
- Information Elements to be sent or not to be sent

Restrictions

None

lfap show servers

Mode

Enable

Format

```
lfap show servers
```

Description

The **lfap show servers** command allows you to view the list of IP servers to which the LFAP agent is currently connected, or will attempt to contact. In the output of the command execution, you will find a list of, at most, three IP addresses of associated FASs.

Restrictions

None.

lfap show statistics

Mode

Enable

Format

```
lfap show statistics
```

Description

The **lfap show statistics** command allows you to view the current statistics of the LFAP agent. In the output of the command execution, you will find data pertaining to the following LFAP agent statistics:

- number of servers
- up time
- connection successes and failures:
 - messages sent/received
 - lost information
 - flows
 - peaks

Restrictions

None

lfap show status

Mode

Enable

Format

lfap show status

Description

The **lfap show status** command allows you to view the current status of the LFAP agent. In the output of the command execution, you will find the following LFAP agent data:

- LFAP Agent Status, defined as one of the following:
 - started
 - stopped
 - failed
- Connection Status, defined as one of the following:
 - connection established
 - connected, no acknowledge received
 - connection lost
 - trying to connect

Restrictions

None

lfap start

Mode

Configure

Format

lfap start

Description

The **lfap start** command issues a command to the LFAP agent to attempt to connect to a FAS server in the list.

Restrictions

At least one IP server must be configured before this command can execute successfully.

38 LOAD-BALANCE COMMANDS

The **load-balance** commands allow you to distribute session load across a pool of servers. These commands provide a way to load balance network traffic to multiple servers.

38.1 COMMAND SUMMARY

The following table lists the **load-balance** commands. The sections following the table describe the command syntax for each command.

load-balance add group-for-mirroring <group-name> ip-of-peer <IPAddr>
load-balance add host-to-group <ipaddr/range> group-name <group name> port <port number> ip [weight <weight>] [status backup] [health-check-cluster <string>]
load-balance add host-to-vip-range <range> vip-range-name <range name> port <port number> ip [weight <weight>] [status backup] [health-check-cluster <string>]
load-balance allow access-to-servers client-ip <ipaddr/range> group-name <group name>
load-balance create group-name <group name> virtual-ip <ipaddr> virtual-port <port number> protocol tcp udp ip [persistence-level vpn tcp ssl sticky ip]
load-balance create health-check-cluster <string> ip-to-check <IPAddr> port-to-check <number>
load-balance create state-mirror-peer <IPAddr> src-ip-to-use <IPAddr>
load-balance create vip-range-name <range name> vip-range <range> virtual-port <port number> protocol tcp udp ip [persistence-level vpn tcp ssl sticky ip]
load-balance set acv-file-size-limit <num>
load-balance set aging-for-src-maps <string> aging-time <num>
load-balance set client-proxy-subnet <group name> subnet <num>
load-balance set ftp-control-port <port number>

load-balance set group-options <string> [ping-int <num>] [ping-tries <num>] [app-int <num>] [app-tries <num>] [read-till-index <num>] [check-port <port number>] [acv-command <string>] [acv-reply <string>] [acv-quit <string>] [acv-command-file <string>] [acv-reply-file <string>] [acv-quit-file <string>] [dns-host-ip <ipaddr>] [dns-host-name <string>] [group-conn-threshold <num>] [policy fastest predictive least-loaded round-robin weighted-round-robin] [response-window-size <num>] [radius-username <string>] [radius-passwd <string>] [radius-md5 <string>] [max-response-time <num>]
load-balance set hash-variant <value>
load-balance set health-check-cluster-options <string> [ping-int <seconds>] [ping-tries <number>] [app-int <number>] [app-tries <number>] [read-till-index <number>] [response-window-size <number>] [acv-command <string>] [acv-reply <string>] [acv-quit <string>] [acv-command-file <string>] [acv-reply-file <string>] [acv-quit-file <string>] [radius-username <string>] [radius-passwd <string>] [radius-md5 <string>] [check-udp] [dns-host-ip <ipaddr>] [dns-host-name <string>] [hcc-conn-thresh <number>] [max-response-time <number>]
load-balance set server-status server-ip <ipaddr/range> server-port <port number> ip group-name <group name> status up down
load-balance set server-options <ipaddr> [port <num> ip] [ping-int <num>] [ping-tries <num>] [app-int <num>] [app-tries <num>] [read-till-index <num>] [check-port <port number>] [acv-command <string>] [acv-reply <string>] [acv-quit <string>] [acv-command-file <string>] [acv-reply-file <string>] [acv-quit-file <string>] [dns-host-ip <ipaddr>] [dns-host-name <string>] [host-conn-threshold <num>] [response-window-size <num>] [radius-username <string>] [radius-passwd <string>] [radius-md5 <string>] [max-response-time <num>]
load-balance set sipp-pat <port>
load-balance set vpn-dest-port <num>
load-balance set wildcard-lsnapt-range <group name> source-port-range <port-number-range>
load-balance show acv-options [group-name <string>] [destination-host-ip <ipaddr>] [destination-host-port <num> ip]
load-balance show hash-stats
load-balance show health-check-clusters
load-balance show session-mirror-info peer-ip <IPAddr>
load-balance show source-mappings [client-ip <ipaddr>] [client-port <port>] [virtual-ip <ipaddr>] [virtual-port <port number> ip] [destination-host-ip <ipaddr>] [type replicated replicated-del sent]
load-balance show statistics group-name <group name> virtual-ip <ipaddr> virtual-port <port number> ip
load-balance show virtual-hosts group-name <group name> virtual-ip <ipaddr> virtual-port <port number> ip

load-balance add group-for-mirroring

Mode

Configure

Format

```
load-balance add group-for-mirroring <group-name> ip-of-peer <ipaddr>
```

Description

The **load-balance add group-for-mirroring** command specifies the load balancing group whose session information will be mirrored. This command is used for the Virtual State Replication Protocol (VSRP).

Parameter	Value	Meaning
group-for-mirroring	<group-name>	Specifies the name of the load balancing server group whose state will be mirrored.
ip-of-peer	<ipaddr>	Specifies the peer to which session information will be sent.

Restrictions

None.

Example

The following example specifies that the sessions of the load balancing group www.fast.net will be mirrored:

```
rs(config)# load-balance add group-for-mirroring www.fast.net ip-of-peer  
100.1.1.2
```

load-balance add host-to-group

Mode

Configure

Format

```
load-balance add host-to-group <ipaddr/range> group-name <group name> port <port number> [ip  
[weight <weight>] [status backup] [health-check-cluster <string>]
```

Description

The **load-balance add host-to-group** command lets you add a server to a server group that was previously-created with the **load-balance create group-name** command.

Parameter	Value	Meaning
host-to-group	<ipaddr/range>	The IP address of the server being added to the group, in the form a.b.c.d or a range of IP addresses in the form 10.10.1.1-10.10.1.3.
group-name	<group name>	The name of the load balancing group to which you are adding the server.
port	<port number>	The port number to be used for load balancing communications for the server being added. Specify a number between 1 and 65535.
	ip	Specify ip if the server will be part of an IP load balancing group.
weight	<weight>	This parameter is only valid if you specify the weighted round robin policy for this group of load balancing servers. The weight determines how many sessions are assigned to this server during its turn in the weighted round robin selection. Specify a number between 1 and 65535. The default value is 1.
status	backup	The status of the server(s) being added to the group: backup specifies that this server is to be sent client requests only if a load balancing server or an application on a load balancing server is “down” (as determined by the RS’s verification checking).
health-check-cluster	<string>	Specifies the health check cluster to which this server should be added.

Restrictions

None.

Examples

To add a server 10.10.13.2 to the server group 'service2':

```
rs(config)# load-balance add host-to-group 10.10.13.2 group-name  
service2 port 80
```

To add servers 10.10.13.3, 10.10.13.4, and 10.10.13.5 to the server group 'service2':

```
rs(config)# load-balance add host-to-group 10.10.13.3-10.10.13.5  
group-name service2 port 80
```

The following is an example of specifying the weighted round robin policy for distributing the workload on the server group 'service2.' To add servers 10.10.13.3, 10.10.13.4, and 10.10.13.5 to the server group 'service2,' a weight must be assigned to each server in the group:

```
rs(config)# load-balance set policy-for-group service2 policy weighted-round-robin  
rs(config)# load-balance add host-to-group 10.10.13.3 group-name service2 port 80  
weight 10  
rs(config)# load-balance add host-to-group 10.10.13.4 group-name service2 port 80  
weight 100  
rs(config)# load-balance add host-to-group 10.10.13.5 group-name service2 port 80  
weight 1000
```

load-balance add host-to-vip-range

Mode

Configure

Format

```
load-balance add host-to-vip-range <range> vip-range-name <range name> port <port number> [ip [weight <weight>] [status backup] [health-check-cluster <string>]]
```

Description

The **load-balance add host-to-vip-range** command lets you add a range of servers to a range of virtual IP addresses that were previously created with the **load-balance create vip-range-name** command. This command adds the first server address in the range to the first virtual IP address, the second server address to the second virtual IP address, and so on. Therefore, the number of servers in the specified range must *equal* the number of virtual IP addresses; if you specified 15 virtual IP addresses with the **load-balance create vip-range-name** command, then you must specify a range of 15 IP addresses in the **load-balance add host-to-vip-range** command.

Parameter	Value	Meaning
host-to-vip-range	<range>	The IP range of the servers being added to the range, in the form 10.10.1.1-10.10.1.3. The number of servers in the range must be the same as the number of virtual IP addresses that were previously-created.
vip-range-name	<range name>	The name of the range of load balancing servers.
port	<port number> ip	The port number to be used for load balancing communications for the server being added. Specify a number between 1 and 65535. Specify ip if the server will be part of an IP load balancing group.
weight	<weight>	This parameter is only valid if you specify the weighted round robin policy for this group of load balancing servers. The weight determines how many sessions are assigned to this server during its turn in the weighted round robin selection. Specify a number between 1 and 65535. The default value is 1.
status	backup	The status of the server(s) being added to the group: backup specifies that this server is to be sent client requests only if a load balancing server or an application on a load balancing server is “down” (as determined by the RS’s verification checking).
health-check-cluster	<string>	Specifies the health check cluster to which this server should be added.

Restrictions

None.

Examples

The following command creates the server groups 'service1' through 'service15' with virtual IP addresses 207.135.89.1 through 207.135.89.15:

```
rs(config)# load-balance create vip-range-name service vip-range  
207.135.89.1-207.135.89.15 virtual-port 80 protocol tcp
```

To add servers 10.10.13.1-10.10.13.15 to the server groups 'service1' through 'service15':

```
rs(config)# load-balance add host-to-vip-range 10.10.13.1-10.10.13.15  
vip-range-name service port 80
```

load-balance allow access-to-servers

Mode

Configure

Format

```
load-balance allow access-to-servers client-ip <ipaddr/range> group-name <group name>
```

Description

Load balancing causes both source and destination addresses to be translated on the RS. It may be undesirable in some cases for a source address to be translated; for example, when data is to be updated on each individual server. The **load-balance allow access-to-servers** command lets you specify the hosts which are allowed to access a group of load balancing servers without address translation.

Note that a host that is allowed to access a group of load balancing servers without address translation *cannot* use the virtual IP address and port to access servers in the group.

Parameter	Value	Meaning
client-ip	<ipaddr/range>	The IP address of the host that is to be granted direct access, in the form a.b.c.d or a range of IP addresses in the form 10.10.1.1-10.10.1.3.
group-name	<group name>	The name of the group of load balancing servers.

Restrictions

None.

Examples

To allow the host 10.23.4.8 to directly access the server group 'service2':

```
rs(config)# load-balance allow access-to-servers client-ip 10.23.4.8  
group-name service2
```

load-balance create group-name

Mode

Configure

Format

```
load-balance create group-name <group name> virtual-ip <ipaddr> [virtual-port <port number>
] protocol tcp|udp|ip [persistence-level vpn|tcp|ssl| sticky|ip]
```

Description

The **load-balance create group-name** command lets you create a load balancing server group and specify a unique “virtual” IP address and port number that is used by a client to access any server in the group. You must also specify the protocol (for example, TCP for HTTP and FTP sessions) to be used by the load balancing servers. After you create the group with this command, use the **load-balance add host** command to add specific server systems to the group.



Note If you want to create many groups, each with a virtual IP address, use the **load-balance create vip-range-name** command.

Parameter	Value	Meaning
group-name	<group name>	The name of this group of load balancing servers.
virtual-ip	<ipaddr>	The address in the form a.b.c.d that will be used as the IP address for this group.
virtual-port	<port number>	The port number to be used for this group. Specify a number between 1 and 65535.
 Note You cannot specify port number 20, as it is the FTP data port. If you create a group on the FTP control port for FTP, an implicit group will be created on port number 20.		
protocol		The protocol used by this group of load balancing servers.
	tcp	Specifies that the group uses TCP.
	udp	Specifies that the group uses UDP.
	ip	Specifies that the group uses IP.
persistence-level		The level of persistence to use for the bindings or connections.

Parameter	Value	Meaning
	ip	Specify ip to load balance IP groups.
	tcp	(Default) TCP application level of persistence.
	ssl	SSL (https) level of persistence.
	sticky	Sticky connections allow a client to connect to the same real server as in previous connections.
	vpn	VPN persistence to load-balance IKE, AH and ESP traffic.

Restrictions

None.

Examples

To configure the server group 'service2':

```
rs(config)# load-balance create group-name service2 virtual-ip  
10.10.100.100 virtual-port 80 protocol tcp
```


load-balance create health-check-cluster

Mode

Configure

Format

```
load-balance create health-check-cluster <string> ip-to-check <IPaddr> port-to-check <number>
```

Description

The `load-balance create health-check-cluster` command creates a group of servers to which the same health check will be applied.

Parameter	Value	Meaning
health-check-cluster	<string>	Identifies the cluster of servers to which the same health check will be applied.
ip-to-check	<IPaddr>	IP address to be used for application content verification for this cluster of servers. Note that this IP address must be a unique address.
port-to-check	<number>	Port to be used for application content verification for this cluster.

Restrictions

None.

Example

To create the health-check-cluster 'fast10':

```
rs(config)# load-balance create health-check-cluster fast10 ip-to-check 10.10.10.1 port-to-check 2
```

load-balance create state-mirror-peer

Mode

Configure

Format

```
load-balance create state-mirror-peer <IPAddr> src-ip-to-use <IPAddr>
```

Description

Use the **load-balance create state-mirror-peer** command to run the Virtual State Replication Protocol (VSRP) on the RS. It specifies to which peer the status information will be sent and the IP address to use when connecting to the mirroring peer.

Parameter	Value	Meaning
state-mirror-peer	<IPAddr>	IP of peer to which session information will be sent.
src-ip-to-use	<IPAddr>	IP address to use when connecting to the mirroring peer

Restrictions

None.

Example

To mirror the sessions of an RS with an IP address of 100.1.1.1, enter the following command:

```
rs(config)# load-balance create state-mirror-peer 100.1.1.2 src-ip-to-use 100.1.1.1
```

After you enter this command, you will also have to enter the **load-balance add group-for-mirroring** command.

load-balance create vip-range-name

Mode

Configure

Format

```
load-balance create vip-range-name <range name> vip-range <range> [virtual-port <port number> ] protocol tcp|udp|ip [persistence-level vpn|tcp|ssl| sticky|ip]
```

Description

The **load-balance create vip-range-name** command lets you specify a range of “virtual” IP addresses and a port number that is used by a client to access a server in the virtual IP address range. You must also specify the protocol (for example, TCP for HTTP and FTP sessions) to be used by the load balancing servers.

This command *implicitly* creates separate server groups for each virtual IP address in the specified range. The *<range name>* you specify becomes the base group name. Thus, the command **load-balance create vip-range-name myrange vip-range 207.135.89.1-207.135.89.15 virtual-port 80 protocol tcp** creates the groups ‘myrange1’ with virtual IP address 207.135.89.1, ‘myrange2’ with virtual IP address 207.135.89.2, etc. This command allows you to create *multiple* server groups, each with unique virtual IP addresses, whereas the **load-balance create group-name** command allows you to only create a *single* group with a *single* virtual IP address.

After you create groups with this command, you can use the **load-balance add host-to-group** command to identify specific server systems in each group. Or, you can use the **load-balance add host-to-vip-range** command to add a range of server IP addresses to each group.

Parameter	Value	Meaning
vip-range-name	<range name>	The base group name for this range of load balancing servers.
vip-range	<range>	The range of virtual IP addresses to be created.
virtual-port	<port number>	The port number to be used for this virtual IP range. Specify a number between 1 and 65535.
 Note You cannot specify port number 20, as it is the FTP data port.		
protocol		The protocol used by this virtual IP range.
	tcp	Specifies that the group uses TCP.
	udp	Specifies that the group uses UDP.
	ip	Specifies that the group uses IP.
persistence-level		The level of persistence to use for the bindings or connections.

Parameter	Value	Meaning
	ip	Specify ip to load balance IP groups.
	tcp	(Default) TCP application level of persistence.
	ssl	SSL (https) level of persistence.
	sticky	Sticky connections allow a client to connect to the same real server as in previous connections.
	vpn	VPN persistence to load-balance IKE, AH and ESP traffic.

Restrictions

None.

Example

To configure the server groups 'service1' through 'service15':

```
rs(config)# load-balance create vip-range-name service vip-range  
207.135.89.1-207.135.89.15 virtual-port 80 protocol tcp
```

load-balance set acv-file-size-limit

Mode

Configure

Format

```
load-balance set acv-file-size-limit <num>
```

Description

The **load-balance set acv-file-size-limit** command sets a limit to the size of the files that contain the application content verification commands.

Parameter	Value	Meaning
acv-file-size-limit	<num>	Specify the file size limit. Enter a value between 1 and 8192.

Restrictions

None.

Example

The following example sets the application content verification file size limit to 2012:

```
rs(config)# load-balance set acv-file-size-limit 2012
```

load-balance set aging-for-src-maps

Mode

Configure

Format

```
load-balance set aging-for-src-maps <string> aging-time <num>
```

Description

The **load-balance set aging-for-src-maps** command sets the aging time for server group mapping. Once the aging time has expired, mapping from a client to a selected server within the group is cleared. This allows the user to better configure timeout values to specific server groups instead of using a general timeout value for all groups.

Parameter	Value	Meaning
aging-for-src-maps	<string>	Specifies the name of the server group.
aging-time	<num>	Specifies the aging time in minutes. Specify a number between 1 and 4320. The default values depend on which persistence level is selected for a group. Persistence levels vpn and tcp has a default value of 3 minutes. Persistence levels ssl and sticky has a default value of 120 minutes.

Restrictions

None.

Example

To set the aging time to 120 minutes for the server group 'group1':

```
rs(config)# load-balance set aging-for-src-maps group1 aging-time 120
```

load-balance set client-proxy-subnet

Mode
Configure

Format

```
load-balance set client-proxy-subnet <group name> subnet <num>
```

Description

The **load-balance set client-proxy-subnet** command sets the subnet used for mapping clients to a specific server group.

Parameter	Value	Meaning
client-proxy-subnet	<group name>	Specifies the name of the server group.
subnet	<num>	Specifies the subnet. Specify a number between 1 and 31.

Restrictions

None.

Example

To set the subnet number to 10 for the server group 'group1':

```
rs(config)# load-balance set client-proxy-subnet group1 subnet 10
```

load-balance set ftp-control-port

Mode

Configure

Format

```
load-balance set ftp-control-port <port number>
```

Description

File Transfer Protocol (FTP) packets require special handling with load balancing, because IP address information is contained within the FTP packet data. You can use the **load-balance set ftp-control-port** command to specify the port number that is used for FTP control. The default is port 21.

Parameter	Value	Meaning
ftp-control-port	<port number>	Specifies the port number used for FTP control. Specify a value between 1 and 65535.

Restrictions

None.

Example

To set the FTP control port to 5000:

```
rs(config)# load-balance set ftp-control-port 5000
```


load-balance set group-options

Mode

Configure

Format

```
load-balance set group-options <string> [ping-int <seconds>] [ping-tries <num>] [app-int
<seconds>] [app-tries <num>] [read-till-index <num>] [check-port <port number>]
[acv-command <string>] [acv-reply <string>] [acv-quit <string>] [acv-command-file <string>]
[acv-reply-file <string>] [acv-quit-file <string>] [radius-username <string>]
[radius-passwd <string>] [radius-md5 <string>] [dns-host-ip <ipaddr>] [dns-host-name
<string>] [group-conn-threshold <num>] policy fastest | predictive | least-loaded |
round-robin | weighted-round-robin] [response-window-size <num>] max-response-time
<num>]
```

Description

The **load-balance set group-options** command allows you to set various parameters for checking server content of a load balancing server group. This group must already be created with the **load-balance create group-name** command.

Parameter	Value	Meaning
group-options	<string>	The name of the group of load balancing servers.
ping-int	<seconds>	Use this parameter to set the ping interval (seconds) for servers in this group. Specify any value between 1 and 3600. The default value is 5.
ping-tries	<num>	Use this parameter to set the number of ping retries before marking the server down. Specify any value between 1 and 255. The default value is 4.
app-int	<seconds>	Use this parameter to set the interval (seconds) between application checks. Specify any value between 1 and 3600. The default value is 15.
app-tries	<num>	Use this parameter to set the number of retries before marking the application down. Specify any value between 1 and 255. The default value is 4.
read-till-index	<num>	Specify this parameter to instruct checking until this index for the start of the 'acv-reply'. Specify a number between 2 and 255.
check-port	<port number>	Use this parameter to set an alternate port for application checks. Specify a number between 1 and 65535.
acv-command	<string>	Use this parameter to set the application content verification command.

Parameter	Value	Meaning
acv-reply	<string>	Use this parameter to set the application content verification reply.
acv-quit	<string>	Use this parameter to set the application content verification command to be sent before closing connection.
acv-command-file	<string>	Use this parameter to specify the name of the file of the application content verification command.
acv-reply-file	<string>	Use this parameter to specify the file name of the application content verification reply command.
acv-quit-file	<string>	Use this parameter to specify the file name of the application content verification command sent before closing the connection.
radius-username	<string>	Specify the user name used for queries to the RADIUS server when a health check is performed.
radius-passwd	<string>	Specify the password used for queries to the RADIUS server when a health check is performed.
radius-md5	<string>	Specify the MD5 key used for queries to the RADIUS server when a health check is performed.
dns-host-ip	<ipaddr>	Specify the IP address that should be in the response of the DNS server to the health check.
dns-host-name	<string>	Specify the name that should be in the response of the DNS server to the health check.
group-conn-threshold	<num>	Specify the maximum number of connections allowed for each server in the group. Enter a value between 1 and 65535, inclusive
policy		Specify how the RS selects the server that will service a new session.
	round-robin	The servers are selected sequentially (round-robin), without regard to the load on individual servers. This is the default policy.
	weighted-round-robin	This policy is a variation of the round-robin policy. The RS still selects servers in turn, but during its turn, each server takes on a number of session connections according to its assigned weight. For example, if 'server1' is assigned a weight of 1000 and 'server2' is assigned a weight of 10, then server1 will be assigned 1000 sessions during its turn and server2 will be assigned 10 sessions during its turn. If you specify this policy, then you should assign different weights to each server in the group with the load-balance add host-to-group or the load-balance add host-to-vip-range command.

Parameter	Value	Meaning
	least - loaded	The server with the fewest number of sessions bound to it is selected to service the new session.
	fastest	Assign the server with the fastest response time.
	predictive	Assign the server with the fastest decreasing response time.
response-window-size	<num>	Use this parameter to set the window size to calculate average response time of previous health check responses. Default is 0 which indicates do not calculate the response time.
max-response-time	<num>	Use this parameter to set the maximum response time in micro-seconds.

Restrictions

None.

Example

To set the load-balancing group-options for the server group 'service2' to ping every 5 seconds:

```
rs(config)# load-balance set group-options service2 ping-int 5
```

load-balance set hash-variant

Mode

Configure

Format

load-balance set hash-variant <value>

Description

The **load-balance set hash-variant** command sets the hash variant that is used to calculate the load-balancing mappings index. You will only need to set this variant if the **load-balance show hash-stats** command output shows extremely uneven distribution of hash table entries.

Parameter	Value	Meaning
hash-variant	<value>	Specifies the hash variant. Specify a value between 0 and 3, inclusive. The default value is 0.

Restrictions

None.

Example

To set the hash variant to 1:

```
rs(config)# load-balance set hash-variant 1
```

load-balance set health-check-cluster-options

Mode

Configure

Format

```
load-balance set health-check-cluster-options <string> [ping-int <seconds>] [ping-tries <number>] [app-int <number>] [app-tries <number>] [read-till-index <number>] [response-window-size <number>] [acv-command <string>] [acv-reply <string>] [acv-quit <string>] [acv-command-file <string>] [acv-reply-file <string>] [acv-quit-file <string>] [radius-username <string>] [radius-passwd <string>] [radius-md5 <string>] [check-udp] [dns-host-ip <ipaddr>] [dns-host-name <string>] [hcc-conn-thresh <number>] [max-response-time <number>]
```

Description

The **load-balance set health-check-cluster-options** command allows you to set parameters for a health check cluster.

Parameter	Value	Meaning
health-check-cluster-options	<string>	The health check cluster for which the options are being set.
ping-int	<seconds>	Ping interval (in seconds) for destination server.
ping-tries	<number>	Number of retries before marking the destination server down.
app-int	<seconds>	Interval (in seconds) between tries of the application check.
app-tries	<number>	Number of retries before marking the application down.
read-till-index	<number>	Check till this index for start of “acv-reply.”
response-window-size	<number>	Window size to calculate average response time of previous health check responses. Default is 0 which indicates do not calculate the response time.
acv-command	<string>	Application content verification command, e.g.: GET /ksrt.html, within double quotes.
acv-reply	<string>	Application content verification reply, e.g.: OK, within double quotes.

Parameter	Value	Meaning
acv-quit	<string>	Application content verification command to be sent before closing connection, e.g.: 'QUIT' for smtp.
acv-command-file	<string>	Use this parameter to specify the name of the file of the application content verification command.
acv-reply-file	<string>	Use this parameter to specify the file name of the application content verification reply command.
acv-quit-file	<string>	Use this parameter to specify the file name of the application content verification command send before closing the connection.
radius-username	<string>	Specify the user name used for queries to the RADIUS server when a health check is performed.
radius-passwd	<string>	Specify the password used for queries to the RADIUS server when a health check is performed.
radius-md5	<string>	Specify the MD5 key used for queries to the RADIUS server when a health check is performed.
dns-host-ip	<ipaddr>	Specify the IP address that should be in the response of the DNS server to the health check.
dns-host-name	<string>	Specify the name that should be in the response of the DNS server to the health check.
hcc-conn-threshold	<num>	Specify the maximum number of connections allowed for each server in the group. Enter a value between 1 and 65535, inclusive
max-response-time	<num>	Use this parameter to set the maximum response time in micro-seconds.
check-udp		Specifies that the health check cluster will use UDP checks.

Restrictions

None.

load-balance set server-status

Mode

Enable

Format

```
load-balance set server-status server-ip <ipaddr/range> server-port <port number> | ip  
group-name <group name> status up|down
```

Description

The **load-balance set server-status** command allows you to set the status of a load balancing server. When the status of a server is set to “down,” no *new* sessions are directed to that server. Current sessions on the server are not affected. This command can be used when server content needs to be updated or to bring one or more backup servers online during peak usage times.

Parameter	Value	Meaning
server-ip	<ipaddr/range>	IP address of the server whose status is to be set.
server-port	<port number> ip	Port number of the server whose status is to be set. Specify ip if the server is an IP load balancing server.
group-name	<group name>	Group name to which this server belongs.
status	up down	Sets the server status to up or down. Setting a server’s status to down will cause new sessions <i>not</i> to be directed to the server.

Restrictions

None.

Example

To set the status for the server 10.10.1.2 to ‘down’:

```
rs# load-balance set server-status server-ip 10.10.1.2 server-port 80  
group-name service2 status down
```

load-balance set server-options

Mode

Configure

Format

```
load-balance set server-options <string> [port <num>|ip] [ping-int <seconds>] [ping-tries <num>] [app-int <seconds>] [app-tries <num>] [read-till-index <num>] [check-port <port number>] [acv-command <string>] [acv-reply <string>] [acv-quit <string>] [acv-command-file <string>] [acv-reply-file <string>] [acv-quit-file <string>] [radius-username <string>] [radius-passwd <string>] [radius-md5 <string>]
```

Description

The **load-balance set server-options** command allows you to set various parameters for a load balancing destination server.

Parameter	Value	Meaning
server-options	<string>	The name of the destination server.
port	<num> ip	Use this parameter to select the port running the application on the destination server. Specify ip to set options for an IP load balancing server.
ping-int	<seconds>	Use this parameter to set the ping interval (seconds) for servers in this group. Specify any value between 1 and 3600.
ping-tries	<num>	Use this parameter to set the number of ping retries before marking the server down. Specify any value between 1 and 255.
app-int	<seconds>	Use this parameter to set the interval (seconds) between application checks. Specify any value between 1 and 3600.
app-tries	<num>	Use this parameter to set the number of retries before marking the application down. Specify any value between 1 and 255.
read-till-index	<num>	Specify this parameter to instruct checking till this index for start of 'acv-reply'. Specify a number between 2 and 255.
check-port	<port number>	Use this parameter to set an alternate port for application checks. Specify a number between 1 and 65535.
acv-command	<string>	Use this parameter to set the application content verification command.

Parameter	Value	Meaning
acv-reply	<string>	Use this parameter to set the application content verification reply.
acv-quit	<string>	Use this parameter to set the application content verification command to be sent before closing connection.
acv-command-file	<string>	Use this parameter to specify the name of the file of the application content verification command.
acv-reply-file	<string>	Use this parameter to specify the file name of the application content verification reply command.
acv-quit-file	<string>	Use this parameter to specify the file name of the application content verification command send before closing the connection.
radius-username	<string>	Specify the user name used for queries to the RADIUS server when a health check is performed.
radius-passwd	<string>	Specify the password used for queries to the RADIUS server when a health check is performed.
radius-md5	<string>	Specify the MD5 key used for queries to the RADIUS server when a health check is performed.
dns-host-ip	<ipaddr>	Specify the IP address that should be in the response of the DNS server to the health check.
dns-host-name	<string>	Specify the name that should be in the response of the DNS server to the health check.
host-conn-threshold	<num>	Specify the maximum number of connections allowed for each server in the group. Enter a value between 1 and 65535, inclusive
response-window-size	<num>	Use this parameter to set the window size to calculate average response time of previous health check responses. Default is 0 which indicates do not calculate the response time.
max-response-time	<num>	Use this parameter to set the maximum response time in micro-seconds.

Restrictions

None.

Example

To set the load-balancing server-options for the destination server 'server2' to ping every 5 seconds:

```
rs(config)# load-balance set server-options server2 ping-int 5
```

load-balance set sipp-pat

Mode

Configure

Format

```
load-balance set sipp-pat <port>
```

Description

The **load-balance set sipp-pat** command allows you to assign a single port to handle all load balancing in the case where the RS is connected to another vender equipment which may not be supported by the RS. This is done by enabling Simple Internet Protocol Plus (SIPP) and Port Address Translation (PAT) on the port. This provides inter-operability between the RS and unsupported hardware.

Parameter	Value	Meaning
sipp-pat	<port>	Specifies a single port number.

Restrictions

None.

Example

To set port 'et.2.1' to handle load balancing for unsupported hardware:

```
rs(config)# load-balance set sipp-pat et.2.1
```

load-balance set vpn-dest-port

Mode

Configure

Format

```
load-balance set vpn-dest-port <num>
```

Description

The **load-balance set vpn-dest-port** command allows you to set the destination port number for load balanced VPNs.

Parameter	Value	Meaning
vpn-dest-port	<num>	Specifies the destination port number. Specify any number between 1 and 65535. Default is 500.

Restrictions

Do not specify port 20, since this is the number designated for the FTP data port.

Example

To set the destination port to port 5000:

```
rs(config)# load-balance set vpn-dest-port 5000
```

load-balance set wildcard-lsnapt-range

Mode

Configure

Format

```
load-balance set wildcard-lsnapt-range <group name> source-port-range <port-number-range>
```

Description

When you create a group of load balancing servers, you define the virtual IP address for the server that clients will use. You can optionally specify a port number to be used for all servers in the group. If you do not specify a port number, a wildcard group is created.

The **load-balance set wildcard-lsnapt-range** command allows you to specify a range of source port numbers that the load balancing servers can use to send requests to the Internet. This allows Network Address Translation (NAT) on the RS to translate the local address, including the source port number, of the load balancing server to a global address for the request. NAT will also translate the global address back to the local address of the server. For example, if a DNS server is being load balanced as part of the wildcard group, the DNS server needs to be able to send requests to the Internet to resolve hostnames that it does not have in its cache.

Parameter	Value	Meaning
	<i><group name></i>	The name of the wildcard group whose servers need to access the Internet.
source-port-range	<i><port-number-range></i>	Specifies a range of port numbers that server requests can use to access the Internet. Specify numbers between 1 and 65535.

Restrictions

Do not specify port 20, since this is the number designated for the FTP data port.

Example

To allow requests to the Internet from the load-balancing servers in the group 'service2' from ports 1024-65535:

```
rs(config)# load-balance set wildcard-lsnapt-range service2
source-port-range 1024-65535
```

load-balance show acv-options

Mode

Enable

Format

```
load-balance show acv-options [group-name <group name>] [destination-host-ip <ipaddr>]  
[destination-host-port <num>|ip]
```

Description

The **load-balance show acv-options** command allows you to display load balancing acv options.

Parameter	Value	Meaning
group-name	<string>	Use this parameter to show acv-options of the servers belonging to this group.
destination-host-ip	<ipaddr>	Use this parameter to show acv-options of the servers that are a part of the group with this virtual IP.
destination-host-port	<num> ip	Use this parameter to show acv-options of servers that are a part of the group with this virtual port. Specify any number between 1 and 65535. Specify ip to display acv-options of servers in an IP load balanced group.

Restrictions

None.

Example

Following is an example of the **load-balance show acv-options** command:

```

RS-8000# load-balance show acv-options
Dest IP: Destination Host IP
DPort: Destination Host Port
PI: Destination Host Ping Interval (in secs.)
PT: Destination Host Ping Tries
AI: Destination Host Application Interval (in secs.)
AT: Destination Host Application Tries
Command: Application Content Verification Command for Destination Host
Reply: Application Content Verification Reply for Destination Host
Quit: Application Content Verification Quit command for Destination Host
RI: Read Index for Reply from Destination Host
HCC: Health Check Cluster
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Dest IP | DPort | PI | PT | AI | AT | Command | Reply | Quit | RI |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 50.1.1.1 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.2 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.3 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.4 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.5 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.6 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.7 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.8 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.9 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.10 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.11 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.12 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.13 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.14 | 25 | 5 | 4 | 15 | 4 | | | | 0 |
| 50.1.1.15 | 25 | 5 | 4 | 15 | 4 | | | | 0 |

Application Content Verification options of 15 host(s) shown.
RS-8000#

```

Table 38-1 Display field descriptions for the load-balance show acv-options command

FIELD	DESCRIPTION
Dest IP	The IP address of the destination host.
DPort	The destination host's port number.
PI	The ping interval, in seconds.
PT	The number of ping tries before the host is considered down.
AI	The interval between application health checks.
AT	The number of application health check tries before the host is considered down.
Command	The application content verification command set for the host.
Reply	The application content verification reply command set for the host.
Quit	The application content verification quit command set for the host.
RI	The RS checks up to this index value for the start of the acv-reply.

load-balance show hash-stats

Mode
Enable

Format

load-balance show hash-stats

Description

The **load-balance show hash-stats** command allows you to display load balancing hash statistics.

Restrictions

None.

Example

Following is an example of the **load-balance show hash-stats** command:

```
rs# load-balance show hash-stats
Total Mappings: 4502

Top 10 Hash Depths:
+-----+-----+-----+
| Index | Hash Depth | Hash Depth Occurrence |
+-----+-----+-----+
| 1      | 0          | 11882                  |
| 2      | 1          | 4226                   |
| 3      | 2          | 138                    |
+-----+-----+-----+

Top 10 Hash Depth Occurrences:
+-----+-----+-----+
| Index | Hash Depth Occurrence | Hash Depth |
+-----+-----+-----+
| 1      | 11882                 | 0          |
| 2      | 4226                  | 1          |
| 3      | 138                   | 2          |
+-----+-----+-----+
```

Table 38-2 Display field descriptions for the load-balance show hash-stats command

FIELD	DESCRIPTION
Index	Identifies the hash depth.
Hash Depth	The number of hash elements in each position in the load balance hash table
Hash Depth Occurrence	The number of times a bucket with this hash depth occurs in the load balance hash table.

load-balance show health-check-clusters

Mode

Enable

Format

```
load-balance show health-check-clusters
```

Description

The **load-balance show health-check-clusters** command allows you to display the options that were set for the load balance health check clusters. Health check cluster options are set with the **load-balance set health-check-cluster-options** command.

Restrictions

None.

Example

Following is an example of the **load balance show health-check-clusters** command.:

```
rs# load-balance show health-check-clusters

HCC Name: Health Check Cluster Name
HCC IP: Health Check Cluster IP
HPort: Health Check Cluster Port
PI: Health Check Cluster Ping Interval (in secs.)
PT: Health Check Cluster Ping Tries
AI: Health Check Cluster Application Interval (in secs.)
AT: Health Check Cluster Application Tries
Command: Application Content Verification Command for Health Check Cluster
Reply: Application Content Verification Reply for Health Check Cluster
Quit: Application Content Verification Quit command for Health Check Cluster
RI: Read Index for Reply from Health Check Cluster
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| HCC Name |   HCC IP   | HPort | PI | PT | AI | AT |   Command   | Reply | Quit | RI |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|hch1      |176.89.10.51| 25    | 5  | 4  |10  | 3  |              |       |      | 0  |
1 Health Check Cluster(s) shown.
```

Table 38-3 Display field descriptions for the load-balance show health-check-clusters command

FIELD	DESCRIPTION
HCC Name	The name of the health check cluster.
HCC IP	The IP address that is used for application content verification for the health check cluster.
HPort	The port that is used for application content verification for the health check cluster.
PI	The ping interval of the health check cluster.
PT	The number of ping tries set for the health check cluster.
AI	The interval between tries of the application check.
AT	Number of retries before the application is considered down.
Command	The application content verification command.
Reply	The application content verification reply.
Quit	The application content verification quit command.
RI	The read-till-index value configured for the health check cluster.

load-balance show session-mirror-info

Mode
Enable

Format

load-balance show session-mirror-info peer-ip <IPAddr>

Description

The **load-balance show session-mirror-info** command allows you to display session mirroring information.

Parameter	Value	Meaning
peer-ip	<IPAddr>	The IP address of the peer whose information is to be shown.

Restrictions

None.

Example

Following is an example of the **load balance show session-mirror-info** command:

```
rs# load-balance show session-mirror-info peer-ip 134.141.179.145

+-----+-----+-----+-----+-----+-----+
|  Peer IP   | Conn. State | State | Msg. Sent | Msg. Rcvd | Msg. to Send |
|           |             |       |           |           |              |
+-----+-----+-----+-----+-----+-----+
|134.141.179.145|Waiting for Conn|Down   |          0|          0|              0|
|           |             |       |           |           |              |
+-----+-----+-----+-----+-----+-----+
|Groups being replicated: http-grp (Init      )|
|           |             |       |           |           |              |
+-----+-----+-----+-----+-----+-----+

1 State Mirroring Peer(s) shown
```

Table 38-4 Display field descriptions for the load-balance show session-mirror-info command

FIELD	DESCRIPTION
Peer IP	The IP address of the peer to which session information is sent.
Conn. State	The status of the connection between the two peers, which are: waiting for conn, retrying, conn, conn in progress, connected, blocked writing.
State	The mirroring peers verify each other's state by sending pings periodically. This field displays the status of the peer.
Msg. Sent	The number of messages sent to its mirroring peer.
Msg. Rcvd	The number of messages received from its mirroring peer.
Msg. to Send	The number of messages that will be sent to its mirroring peer.
Groups being replicated	The load balancing group whose sessions are being replicated.
Init	Indicates the status between the two peers: Init indicates that the connection is being initialized. In Progress indicates that this peer has sent a message to its mirroring peer. Over indicates the peer received the message. No Group indicates that the peer is not part of the same load balancing group.

load-balance show source-mappings

Mode

Enable

Format

```
load-balance show source-mappings [client-ip <ipaddr>] [client-port <port>] [virtual-ip <ipaddr>] [virtual-port <port number>|ip] [destination-host-ip <ipaddr>] [type replicated|replicated-del| sent]
```

Description

The **load-balance show source-mappings** command allows you to display load balancing source-destination bindings.

Parameter	Value	Meaning
client-ip	<ipaddr>	IP address of client whose mappings are to be shown.
client-port	<port number>	Port number of client whose mappings are to be shown.
	ip	Specify ip to display mappings for IP load balanced groups.
virtual-ip	<ipaddr>	Virtual IP address whose mappings are to be shown.
virtual-port	<port number>	Virtual port number whose mappings are to be shown.
	ip	Specify ip to display mappings for IP load balanced groups.
destination-host-ip	<ipaddr>	IP address of the destination server whose mappings are to be shown.
type		Specifies the type of mappings to be shown.
	replicated	Specifies that replicated mapping will be shown.
	replicated-del	Specifies that replicated mappings in the delete state will be shown.
	sent	Specifies that the mappings that were sent to the peer will be shown.

Restrictions

None.

Example

Following is an example of the **load-balance show source-mappings** command:

```
rs# load-balance show source-mappings
Current Mappings:

FC: Flow Count
SPort: Source Port
VPort: Virtual Port
Dport: Destination Port
F: Flags = R: Replicated Map, D: Replicated Map to be deleted, S: Sent to Peer

+-----+-----+-----+-----+-----+-----+-----+-----+
| Src. Address/Mask | SPort | Virtual IP | VPort | Dst. Address | Dport | FC | F |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 192.1.1.45        | 1057  | 192.1.2.194 | *     | 192.1.2.41   | *     | 1  | |
| 192.1.1.45        | 1056  | 192.1.2.194 | *     | 192.1.2.42   | *     | 1  | |
| 192.1.1.45        | 1039  | 192.1.2.194 | *     | 192.1.2.41   | *     | 1  | |
| 192.1.1.45        | 1038  | 192.1.2.194 | *     | 192.1.2.42   | *     | 1  | |
| 192.1.1.45        | 1037  | 192.1.2.194 | *     | 192.1.2.41   | *     | 1  | |
| 192.1.1.45        | 1036  | 192.1.2.194 | *     | 192.1.2.42   | *     | 1  | |
| 192.1.1.45        | 1035  | 192.1.2.194 | *     | 192.1.2.41   | *     | 1  | |
| 192.1.1.45        | 1034  | 192.1.2.194 | *     | 192.1.2.42   | *     | 1  | |
| 192.1.1.45        | 1033  | 192.1.2.194 | *     | 192.1.2.41   | *     | 1  | |
| 192.1.1.45        | 1032  | 192.1.2.194 | *     | 192.1.2.42   | *     | 1  | |
```

Table 38-5 Display field descriptions for the load-balance show source-mappings command

FIELD	DESCRIPTION
Src. Address/Mask	The source address and netmask.
Sport	The source port number.
Virtual IP	The virtual IP address of the load balancing server group.
VPort	The virtual port of the load balancing server group.
Dst. Address	The IP address of the destination server.
Dport	The destination port.
FC	The number of flows between the source and destination,
F	Flag specifying the type of mappings shown: R - replicated map, D - replicate map to be deleted, S - mappings that were sent to the peer.

load-balance show statistics

Mode

Enable

Format

```
load-balance show statistics group-name <group name> virtual-ip <ipaddr> virtual-port  
<port number> | ip
```

Description

The **load-balance show statistics** command allows you to display load balancing statistics.

Parameter	Value	Meaning
group-name	<group name>	Name of the group whose statistics are to be shown.
virtual-ip	<ipaddr>	Virtual IP address whose statistics are to be shown.
virtual-port	<port number> ip	Virtual port number whose statistics are to be shown. Specify ip to display statistics for IP load balanced groups.

Restrictions

None.

Example

Following is an example of the **load balance show statistics** command:

```
rs# load-balance show statistics
Load Balancing Packets Dropped:
  No Such Virtual-IP Packet drop count           : 0
  TTL expired Packet drop count                   : 0
  No Such Virtual-IP Binding drop count           : 0
  No Such Destination Binding drop count          : 0
  Destination Server not in Group Binding drop count : 0
  Unknown Forwarding mode Binding drop count      : 0

Load Balance Group Statistics:

  Group Name: telnet, Virtual-IP: 50.1.1.17, Virtual-Port: 23
    No destination selected Packet drop count      : 0
    Memory Allocation error Packet drop count      : 0
    No forward route found Packet drop count       : 0
    Number of Packets forwarded                    : 23430
    Channel not Load Balancing compliant Packet drop count : 0
    No hosts in group Packet drop count             : 0
    Client in Access List Packet drop count        : 0
    Destination Host 'DOWN' for Replicated binding drop count : 0

Statistics of 1 groups shown.
```

Table 38-6 Display field descriptions for the load-balance show statistics command

FIELD	DESCRIPTION
No Such Virtual-IP Packet drop count	The number of packets that were dropped because the RS could not find a host with the specified virtual IP. For example, if the host is down or the destination port of the host is down.
TTL expired Packet drop count	The number of packets that were dropped because the time-to-live (TTL) timer expired.
No Such Virtual-IP Binding drop count	Used with VSRP. The number of packets that were dropped because the virtual IP of the peer was different from the one configured on the RS.
No Such Destination Binding drop count	Used with VSRP. The number of packets that were dropped because the destination was different from the one configured on the RS.

Table 38-6 Display field descriptions for the load-balance show statistics command (Continued)

FIELD	DESCRIPTION
Destination Server not in Group Binding drop count	Used with VSRP. The number of packets that were dropped because the destination server was not in the same load balancing group.
Unknown Forwarding mode Binding drop count	The forwarding mode was not recognized.
No destination selected Packet drop count	The number of packets that were dropped because a destination server was not selected.
Memory Allocation error Packet drop count	The number of packets that were dropped due to memory allocation problems.
No forward route found Packet drop count	The number of packets that were dropped because a return route was found.
Number of Packets forwarded	The number of packets that were forwarded.
Channel not Load Balancing compliant Packet drop count	The number of packets that were dropped because the module did not support load balancing.
No hosts in group Packet drop count	The number of packets that were dropped because there were no servers in the server group.
Client in Access List Packet drop count	The number of packets that were dropped because of ACLs that denied access to the client.
Destination Host 'DOWN' for Replicated binding drop count	The number of packets that were dropped because a host's mirroring peer was down.

load-balance show virtual-hosts

Mode

Enable

Format

```
load-balance show virtual-hosts group-name <group name> virtual-ip <ipaddr> virtual-port <port number> | ip
```

Description

The **load-balance show virtual-hosts** command allows you to display the hosts in a load balancing group.

Parameter	Value	Meaning
group-name	<group name>	The load balancing group that is to be shown.
virtual-ip	<ipaddr>	IP address of the group that is to be shown.
virtual-port	<port number> ip	Port number of the group that is to be shown. Specify ip to display statistics for IP load balanced Virtual groups.

Restrictions

None.

Example

Following is an example of the **load-balance show virtual-hosts** command::

```
RS-8000# load-balance show virtual-hosts group-name telnet

Load Balanced Groups:
Flow Mode Count: 0

OS: Operational state of server
OA: Operational state of application
AS: Admin state of server
BHA: Backup Hosts Added
BHU: Backup Hosts Up
PL: Persistence Level
CAM: Client Address Mapping Subnet
CMT: Client Mappings Timeout (in mins.)
SeW: Server Weight (used only with Weighted Round Robin)
Policies: RR = Round Robin, WRR = Weighted Round Robin, LL = Least Loaded
          FR = Fastest, PR = Predictive
F = Server Status Flags: B = Backup, U = Backup in use, R = Replaced by backup
MRT: Maximum average response time in micro seconds.
RW: Response window.
ART: Average response time in micro seconds.
```

Group Name	Virtual IP	Port	Hosts Added	Hosts Up	Next Index
telnet	50.1.1.17	23	15	0	0

PL	Proto	Conn. Limit	Policy	CAM	CMT	BHA	BHU
TCP	TCP	10000	RR	Not Set	3	0	0

:

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
Index	Host IP	Port	Client Count	SeW	OS	OA	AS	F	
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
0	50.1.1.1	25	0	1	Down	Down	Up	-	
1	50.1.1.2	25	0	1	Down	Down	Up	-	
2	50.1.1.3	25	0	1	Down	Down	Up	-	
3	50.1.1.4	25	0	1	Down	Down	Up	-	
4	50.1.1.5	25	0	1	Down	Down	Up	-	
5	50.1.1.6	25	0	1	Down	Down	Up	-	
6	50.1.1.7	25	0	1	Down	Down	Up	-	
7	50.1.1.8	25	0	1	Down	Down	Up	-	
8	50.1.1.9	25	0	1	Down	Down	Up	-	
9	50.1.1.10	25	0	1	Down	Down	Up	-	
10	50.1.1.11	25	0	1	Down	Down	Up	-	
11	50.1.1.12	25	0	1	Down	Down	Up	-	
12	50.1.1.13	25	0	1	Down	Down	Up	-	
13	50.1.1.14	25	0	1	Down	Down	Up	-	
14	50.1.1.15	25	0	1	Down	Down	Up	-	
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
Index	Host IP	Conn. Limit	Load Count	MRT	RW	ART			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
0	50.1.1.1	10000	0	5000000	Not Set	0			
1	50.1.1.2	10000	0	5000000	Not Set	0			
2	50.1.1.3	10000	0	5000000	Not Set	0			
3	50.1.1.4	10000	0	5000000	Not Set	0			
4	50.1.1.5	10000	0	5000000	Not Set	0			
5	50.1.1.6	10000	0	5000000	Not Set	0			
6	50.1.1.7	10000	0	5000000	Not Set	0			
7	50.1.1.8	10000	0	5000000	Not Set	0			
8	50.1.1.9	10000	0	5000000	Not Set	0			
9	50.1.1.10	10000	0	5000000	Not Set	0			
10	50.1.1.11	10000	0	5000000	Not Set	0			
11	50.1.1.12	10000	0	5000000	Not Set	0			
12	50.1.1.13	10000	0	5000000	Not Set	0			
13	50.1.1.14	10000	0	5000000	Not Set	0			
14	50.1.1.15	10000	0	5000000	Not Set	0			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									

Table 38-7 Display field descriptions for the load-balance show virtual-hosts command

FIELD	DESCRIPTION
Group Name	The group for which the statistics are displayed.
Virtual IP	The group's virtual IP address.
Port	The group's virtual port.
Hosts Added	The number of hosts in the load balancing group.
Hosts Up	The number of hosts that are operational.
PL	The group's persistence level.
Proto	The group's protocol.
Conn. Limit	The group's maximum number of connections.
Policy	The group's load balancing policy.
CAM	The group's client mapping subnet.
CMT	The group's timeout value for client mappings.
BHA	The number of backup servers in the group.
BHU	The number of backup servers that are active.
Index	Identifies the server.
Host IP	The server's IP address.
Port	The server's port number.
Client Count	The number of clients that have accessed the server.
Sew	If the group's load balancing policy is weighted round robin, this field displays the server's weight.
OS	The server's operational state.
OA	The application's operational state.
AS	The server's administrative state.
F	A flag that indicates the server's status: B - Backup, U - Backup in use, and R - the server was replaced by a backup.
Conn. Limit	The maximum number of connections allowed for the server.
MRT	The server's maximum average response time in micro seconds.
RW	The server's response window size.
ART	The server's average response time in micro seconds.

39 LOGOUT COMMAND

logout

Mode

All modes

Format

logout

Description

The **logout** command ends your CLI session. If you have uncommitted changes in the scratchpad, a message warns you that the changes are not saved and gives you an opportunity to cancel the logout and save the changes.

Restrictions

None.

40 MPLS COMMANDS

The **mpls** commands allow you to configure Multi-Protocol Label Switching (MPLS) features on the RS, as well as display various MPLS parameters.

40.1 COMMAND SUMMARY

The following table lists the **mpls** commands. The sections following the table describe each command in greater detail.

<code>mpls add interface <name> <ip-address> all</code>
<code>mpls clear label-switched-paths <pathname> all</code>
<code>mpls create admin-group <groupname> group-value <number></code>
<code>mpls create l2-policy <polycyname> in-port-list <port list> out-port-list <port list> [backbone-1p <priority>] [backbone-vlanid <vlan-id>] dst-mac <macaddr> any [dst-mac-mask <mask>] src-mac <macaddr> any [src-mac-mask <mask>] [vlan <id>] [incoming-1p <priority>] [preserve-original-1q] [seq-number <number>]</code>
<code>mpls create l2-static-path <pathname> next-hop-mac <macaddr> push <label list></code>
<code>mpls create label-switched-path <pathname> to <ip-address> [from <ip-address>] [admin-group <group-list>] [include <group-list>] [exclude <group-list>] [hop-limit <number>] [preference <number>] [retry-limit <number>] [retry-interval <seconds>] [bps <bits>] [class-of-service <number>] [no-cspf] [no-switchback] [adaptive] [no-decrement-ttl] [no-record-route] [disable] [metric <number>]</code>
<code>mpls create path <pathname> [num-hops <number>]</code>
<code>mpls create policy <polycyname> src-ipaddr-mask <ipaddr/netmask> any dst-ipaddr-mask <ipaddr/netmask> any proto <number> src-port <port> dst-port <port_keyword> tos <tos_value> [tos-mask <tos_mask>]</code>
<code>mpls create static-path <pathname> to <ipaddr> push <number> gateway <ipaddr></code>
<code>mpls set global sw-datapath-enable no-propagate-ttl drop-zero-ttl-packets</code>
<code>mpls set interface <name> <ip-address> all label-map <in-label> next-hop <name> <ip-address> [swap <out-label>] [pop] [push <out-label-list>] [reject] [discard] [pop-count <num-labels>] [preference <number>] [admin-group <group-list>] [override-trunk-behavior] [subscription <ratio>] [bandwidth <bps>] [no-php]</code>
<code>mpls set l2-static-path <pathname> policy <policy></code>

mpls set label-switched-path <pathname> primary <pathname> secondary <pathname> [admin-group <group-list>] [include <group-list>] [exclude <group-list>] [hop-limit <number>] [preference <number>] [retry-limit <number>] [retry-interval <seconds>] [bps <bits>] [class-of-service <number>] [no-switchback] [adaptive] [no-decrement-ttl] [no-cspf] [no-record-route] [standby] [policy <policy>] [disable] [metric <number>] [mtu <number>]
mpls set path <pathname> [type loose strict] ip-addr <ipaddr/netmask> [hop <number>]
mpls set portlist in-port-list <port list> [out-port <port list>] next-hop-mac <macaddr> [label-map <in-label>][pop] [pop-count <num-labels>] [push <outlabel>] [swap <out-label>][discard] [end-of-l2-tunnel-label <label>] [overwrite-ip <priority>] [vlanid <vlan-id>] [overwrite-vlanid <vlan-id>]
mpls set static-path <pathname> preference <number> bps <number> class-of-service <number> policy <policyname> disable [metric <number>] [mtu <number>]
mpls set trace-level <level>
mpls set trace-options <option>
mpls show admin-groups
mpls show all
mpls show global
mpls show hw-cam-tbl port <port-list> [index <index>]
mpls show hw-ilm-err port <port-list> [index <index>]
mpls show hw-ilm-tbl port <port-list> [index <index>]
mpls show hw-ott-err port <port-list> [index <index>]
mpls show hw-ott-tbl port <port-list> [index <index>]
mpls show ilm-tbl <interface-name> <ipaddr> all [brief verbose]
mpls show interface <name> <ip-address> all [label-map <label> brief verbose]
mpls show l2-policy <policyname> all [brief verbose]
mpls show label-switched-paths <pathname> all ingress transit egress [brief verbose]
mpls show ott-table <interface> <ipaddr> all [brief verbose]
mpls show paths <pathname> all [brief verbose]
mpls show policy <policyname> all [brief verbose]
mpls show static-paths <pathname> all [brief verbose]
mpls start

mpls add interface

Mode

Configure

Format

```
mpls add interface <name> | <ip-address> | all
```

Description

The **mpls add interface** command allows you to enable MPLS on an interface. You can configure various MPLS interface parameters with the **mpls set interface** command.

Parameter	Value	Meaning
interface	<name> <ip-address>	Specifies an interface. MPLS is enabled on this interface. Specify an interface name or an IP address.
	all	Specify all to enable MPLS on all interfaces.

Restrictions

None

Example

The following command enables MPLS on the interface 'sector1':

```
rs(config)# mpls add interface sector1
```

mpls clear label-switched-paths

Mode

Enable

Format

```
mpls clear label-switched-paths <pathname> |all
```

Description

The **mpls clear label-switched-paths** command allows you to tear down and restart a specified LSP or all LSPs.

Parameter	Value	Meaning
label-switched-paths	<pathname>	Specifies an LSP.
	all	Specify all to clear all LSPs.

Restrictions

None

Example

The following command clears the LSP 'LSP1':

```
rs# mpls clear label-switched-paths LSP1
```

mpls create admin-group

Mode

Configure

Format

```
mpls create admin-group <groupname> group-value <number>
```

Description

The **mpls create admin-group** command allows you to create an MPLS administrative group, and assign a group value to that group. An administrative group designates certain link attributes, and is used for path setup and selection.

Parameter	Value	Meaning
admin-group	<groupname>	Specifies a name for the administrative group. Specify a character string.
group-value	<number>	Specifies a group value for the administrative group. A group value identifies each administrative group with a specific numerical value. Specify a decimal number between 0 and 31.

Restrictions

None

Example

The following command creates an administrative group 'sector2' and assigns a group value of 10:

```
rs(config)# mpls create admin-group sector2 group-value 10
```

mpls create l2-policy

Mode

Configure

Format

```
mpls create l2-policy <policyname> vlan <id> incoming-1p <priority> [{src-mac <macaddr>|any
[src-mac-mask <mask>] dst-mac <macaddr>|any [dst-mac-mask <mask>]}] in-port-list <port
list> out-port-list <port list> [backbone-1p <priority>] [backbone-vlanid <vlan-id>]
[preserve-original-1q] [seq-number <number>]
```

Description

The **mpls create l2-policy** command allows you to create a policy, a set of address filters, that you can apply to an LSP. Once you create a policy, you may apply the policy to an LSP. By applying a policy to an LSP, only labels that satisfy the policy requirements are allowed to traverse through that LSP.

Parameter	Value	Meaning
l2-policy	<policyname>	Specifies the name of the MPLS policy. Specify a character string.
vlan	<id>	Specifies the ID of the VLAN. This would be a criteria used to filter in label traffic onto the LSP. Specify a number between 1-4095.
incoming-1p	<priority>	The 802.1p priority of the incoming packet. This would be a criteria used to filter in label traffic onto the LSP.
src-mac	<macaddr> any	Specifies a source Media Access Control (MAC) address. This would be a criteria used to filter in label traffic onto the LSP. Specify any for any source MAC address.
src-mac-mask	<ipaddr/netmask>	Specifies a source MAC mask. This would be a criteria used to filter in label traffic onto the LSP.
dst-mac	<macaddr> any	Specifies a destination Media Access Control (MAC) address. This would be a criteria used to filter in label traffic onto the LSP. Specify any for any destination MAC address.
dst-mac-mask	<ipaddr/netmask>	Specifies a destination MAC mask. This would be a criteria used to filter in label traffic onto the LSP.
in-port-list	<port list>	Ports where this policy will be applied. Use commas to specify more than one port.
out-port-list	<port list>	Ports to use when sending traffic out. Use commas to specify more than one port.
backbone-1p	<priority>	The 802.1p priority to use when sending traffic out the MPLS port. Specify a value between 0-7.

Parameter	Value	Meaning
backbone-vlanid	<vlan-id>	The ID of the backbone VLAN to use when sending traffic out the MPLS port. Specify a number between 1-4095.
preserve-original-1q		Specifies that the original customer VLAN ID is preserved when sending traffic out the MPLS port.
seq-number	<number>	Specifies the sequence number of this policy. Specify a value between 0-2047.

Restrictions

None

Example

The following command creates an MPLS policy 'allow1' :

```
rs(config)# mpls create l2-policy allow1 dst-mac any src-mac 000000:01e000 vlan 1  
in-port-list gi.2.1 out-port-list gi.3.1
```

mpls create l2-static-path

Mode

Configure

Format

```
mpls create l2-static-path <pathname> next-hop-mac <macaddr> push <label list>
```

Description

The **mpls create static-path** command lets you configure a layer-2 static multiprotocol label switching (MPLS) path.

Parameter	Value	Meaning
l2-static-path	<pathname>	Specifies the name of the L2 static path. Specify a character string.
next-hop-mac	<macaddr>	Specifies the next hop MAC address. Specify a MAC address in the format xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.
push	<label list>	Specifies one or more labels to be pushed onto the label stack. For each label, specify a decimal number between 0 and 4095. Use commas to separate the list of labels; the first label specified is the bottom of the stack.

Restrictions

None

Example

The following command creates an MPLS L2 static path 'p1' to the MAC address 10:10:10:10:10:21 with labels 50, 60, and 70 (bottom to top) pushed onto the label stack:

```
rs(config)# mpls create l2-static-path p1 next-hop-mac 10:10:10:10:10:21 push  
50,60,70
```

mpls create label-switched-path

Mode

Configure

Format

mpls create label-switched-path <pathname> to <ip-address> [from <ip-address>] [admin-group <group-list>] [include <group-list>] [exclude <group-list>] [hop-limit <number>] [preference <number>] [retry-limit <number>] [retry-interval <seconds>] [bps <bits>] [class-of-service <number>] [no-cspf] [no-switchback] [adaptive] [no-decrement-ttl] [no-record-route] [disable] [metric <number>]

Description

The **mpls create label-switched-path** command allows you to create and configure a dynamic label switched path (LSP).

Parameter	Value	Meaning
label-switched-path	<pathname>	Specifies the name for the LSP. Specify a character string.
to	<ip-address>	Specifies the destination (egress router) for the LSP. All MPLS traffic on this particular LSP will be sent to this destination address. Specify an IP address in the format 'a.b.c.d'.
from	<ip-address>	Identifies the source address for the LSP. Specify an IP address in the format 'a.b.c.d'. This parameter does not affect the outgoing interface used by the LSP. If this parameter is not specified, the router ID of the local router is used.
admin-group	<group-list>	Specifies the administrative groups that are assigned to this LSP. Specify up to 32 separate groups. Enclose multiple groups within quotation marks. For example: "group1 group2 group3".
include	<group-list>	Includes a specified administrative group. Specify up to 16 separate groups. For example: 'group1 group2 group3'.
exclude	<group-list>	Excludes a specified administrative group. Specify up to 16 separate groups. For example: 'group1 group2 group3'.
hop-limit	<number>	Defines the hop limit. The hop limit is the maximum number of hops, including the ingress and egress routers, allowed in the LSP. The default is 255. Specify a decimal number between 1 and 255.
preference	<number>	Assigns a preference value for this LSP. This preference value is useful in the case where there are multiple LSPs between a source and destination. A smaller value signifies a more desirable path. The default preference is 7. Specify a decimal number between 1 and 255.

Parameter	Value	Meaning
retry-limit	<number>	Defines a retry limit for this LSP. Depending on the priority of an LSP, the RS will try to establish the path. However, if the path cannot be set up during the first try, the RS will retry a number of times. Specify a decimal number between 1 and 10000. The default value is 5000.
retry-interval	<seconds>	Defines the retry time interval for this LSP, in seconds. This parameter value specifies a time limit for establishing a path. Specify a decimal number between 1 and 600. The default value is 15.
bps	<number>	Specifies the bandwidth, in bits, allocated to this LSP. Default is 0.
class-of-service	<number>	Specifies a class-of-service (CoS) value for this LSP. CoS values are used for resource reservation features. A higher value specifies a higher class-of-service consideration. Specify a decimal number between 1 and 8.
no-cspf		Specifies not to use constrained shortest path first algorithm to establish an LSP.
 Note If you are configuring an explicit LSP, you must specify the no-cspf parameter. Otherwise, the LSP will wait indefinitely for a valid CSPF response.		
no-switchback		Specifies not to switch back from the secondary path to the primary path when the primary becomes available.
adaptive		Specifies that the LSP exhibit adaptive behavior during path recalculation. When a LSP is adaptive, the LSP waits until the new route is setup before tearing down the old LSP. This prevents traffic disruption.
no-decrement-ttl		Disables normal TTL decrementing for LSPs signaled with RSVP. With normal decrementing, the packet's TTL is decremented by a value of 1 on each LSR on the LSP. Disabling TTL decrementing makes the whole LSP appear as one hop.
no-record-route		Specifies that the route for RSVP-signaled LSPs will not be recorded.
disable		Disables the LSP.
metric	<number>	Specifies the metric for this LSP.

Restrictions

If you are configuring an explicit LSP, you must specify the **no-cspf** parameter. Otherwise, the LSP will wait indefinitely for a valid CSPF response.

Example

The following command creates an LSP 'lsp1' to the egress router 10.10.10.10:

```
rs(config)# mpls create label-switched-path lsp1 no-cspf to 10.10.10.10
```

mpls create path

Mode

Configure

Format

```
mpls create path <pathname> [num-hops <number>]
```

Description

The **mpls create path** command allows you to create an explicitly-routed path through the MPLS domain.

Parameter	Value	Meaning
path	<string>	Creates a path with a specified number of hops within the path. Specify the path name with a character string.
num-hops	<number>	Specifies the maximum number of hops for the path. Specify a decimal number between 1 and 255.

Restrictions

None

Example

The following command creates a path 'path1' with 10 hops:

```
rs(config)# mpls create path path1 num-hops 10
```

mpls create policy

Mode

Configure

Format

```
mpls create policy <polycname> src-ipaddr-mask <ipaddr/netmask>|any dst-ipaddr-mask
<ipaddr/netmask>|any proto <protocol> src-port <port> dst-port <port_keyword>
tos <tos_value> [tos-mask <tos_mask>]
```

Description

The **mpls create policy** command allows you to create a policy, a set of address filters, that you can apply to an LSP. Once you create a policy, you may apply the policy to an LSP. By applying a policy to an LSP, only labels that satisfy the policy requirements are allowed to traverse through that LSP.

Parameter	Value	Meaning
policy	<polycname>	Specifies the name of the MPLS policy. Specify a character string.
src-ipaddr-mask	<ipaddr/netmask> any	Specifies a source IP address and netmask. This would be a criteria used to filter in label traffic onto the LSP. Specify any for any source IP address/netmask.
dst-ipaddr-mask	<ipaddr/netmask> any	Specifies a destination IP address and netmask. This would be criteria used to filter in label traffic onto the LSP. Specify any for any destination IP address/netmask.
proto	<protocol>	Specify one of the following keywords:
	icmp	ICMP
	igmp	IGMP
	ip	IP
	tcp	TCP
	udp	UDP
src-port	<port>	TCP/UDP port number. This would be a criteria used to filter in label traffic onto the LSP. Specify one of the following:
	<port number> <range>	Port number (for example, 25) or range of port numbers (for example 25-100)
	<condition>	Numerical expression, such as >1024, <2048, or !=4096.
	<keyword>	Specify one of the following keywords.
	any	Any port number.
	dns	DNS port (53)

Parameter	Value	Meaning
	finger	Finger port (79)
	ftp-cmd	FTP command port (21)
	ftp-data	FTP data port (20)
	http	HTTP port (80)
	https	HTTP Secure port (443)
	imap3	IMAP3 port (220)
	imap4	IMAP4 port (143)
	lpr	LPR port (515)
	nfs	NFS port (2049)
	nnntp	NNTP port (119)
	ntp	NTP port (123)
	pop3	POP3 port (110)
	portmapper	portmapper port (111)
	rexec	R-Exec port (512)
	rlogin	R-Login port (513)
	rshell	R-Shell port (514)
	smtp	SMTP port (25)
	snmp	SNMP port (161)
	telnet	Telnet port (23)
	tftp	TFTP port (69)
	x11	X11 port (6000)
dst-port		Specifies a destination TCP/UDP port number. This would be a criteria used to filter in label traffic onto the LSP. Specify one of the following keywords.
	any	Any port number.
	dns	DNS port (53)
	finger	Finger port (79)
	ftp-cmd	FTP command port (21)
	ftp-data	FTP data port (20)
	http	HTTP port (80)
	https	HTTP Secure port (443)
	imap3	IMAP3 port (220)

Parameter	Value	Meaning
	imap4	IMAP4 port (143)
	lpr	LPR port (515)
	nfs	NFS port (2049)
	nntp	NNTP port (119)
	ntp	NTP port (123)
	pop3	POP3 port (110)
	portmapper	portmapper port (111)
	rexec	R-Exec port (512)
	rlogin	R-Login port (513)
	rshell	R-Shell port (514)
	smtp	SMTP port (25)
	snmp	SNMP port (161)
	telnet	Telnet port (23)
	tftp	TFTP port (69)
	x11	X11 port (6000)
tos	<tos_value>	Type of service (ToS) value. Specify a value between 1-255.
tos-mask	<tos_mask>	ToS mask for the ToS byte. Specify a value between 1-255. The default is 30.

Restrictions

None

Example

The following command creates an MPLS policy ‘allow1’ that will allow all label traffic with source IP address 100.1.1.0/24:

```
rs(config)# mpls create policy allow1 src-ipaddr-mask 100.1.1.0/24
```

mpls create static-path

Mode

Configure

Format

```
mpls create static-path <pathname> to <ipaddr> push <number> gateway <ipaddr>
```

Description

The **mpls create static-path** command lets you configure a static multiprotocol label switching (MPLS) path.

Parameter	Value	Meaning
static-path	<pathname>	Specifies the name of the static path. Specify a character string.
to	<ipaddr>	Specifies the destination for the static path. All MPLS traffic on this static LSP will be sent to this destination address. Specify an IP address in the format 'a.b.c.d'.
push	<label>	Specifies one or more labels to add to the top of the label stack. The top label will become the active label when the label is sent out. For each label, specify a decimal number between 0 and 4095. Use commas to separate the list of labels; the first label specified is the bottom of the stack.
gateway	<ipaddr>	Specifies an outgoing gateway for this static path. Specify an IP address in the following format: 'a.b.c.d'.

Restrictions

Label values 0 through 15 are reserved values and must not be specified.

Example

The following command creates an MPLS static path 'p1' to the IP address '100.2.2.1' through the gateway '120.1.2.101' with an active label value '25':

```
rs(config)# mpls create static-path p1 to 100.2.2.1 gateway 120.1.2.101 push 25
```

mpls set global

Mode

Configure

Format

```
mpls set global sw-datapath-enable | no-propagate-ttl | drop-zero-ttl-packets
```

Description

The **mpls set global** command allows you to set various global parameters that will be applied to all MPLS interfaces.

Parameter	Value	Meaning
sw-datapath-enable		Specifies whether the software data path is used for ports that do not support label swapping in hardware.
Note The sw-datapath-enable parameter allows MPLS functions to run in software without MPLS-enabled line cards installed in the router. This parameter should only be used to test MPLS signaling in limited environments, as CPU and router performance will be affected. The MPLS features described in this manual should only be run on MPLS-enabled RS line cards in run-time environments.		
no-propagate-ttl		Specifies that all LSPs that pass through this router behave as a single hop for IP packets.
drop-zero-ttl-packets		By default, packets with TTL values of 0 or 1 in the MPLS label are sent to the CPU, and an ICMP time exceed message is sent to the sender. This is necessary when doing traceroute over an MPLS tunnel and is applicable only with MPLS line cards. The drop-zero-ttl-packets parameter causes packets with TTL values of 0 or 1 in the MPLS label to be dropped in the hardware; this saves CPU resources but traceroute will not work.

Restrictions

If you use the **mpls set global drop-zero-ttl-packets** command, you will need to negate and then re-add the command if you hotswap an MPLS line card.

Example

The following command causes all LSPs that pass through the router to behave as a single hop for IP packets:

```
rs(config)# mpls set global no-propagate-ttl
```

mpls set interface

Mode

Configure

Format

```
mpls set interface <name> | <ip-address> | all label-map <in-label> next-hop <name> |
<ip-address> [swap <out-label>] [pop] [push <out-label-list>] [reject] [discard] [pop-count
<num-labels>] [preference <number>] [admin-group <group-list>] [override-trunk-behavior]
[subscription <ratio>] [bandwidth <bps>] [no-php]
```

Description

The **mpls set interface** command allows you to configure various parameters on an MPLS interface. The MPLS interface must be enabled with the **mpls add interface** command.

Parameter	Value	Meaning
interface	<name> <ip-address> all	Specifies an MPLS interface. Specify an interface name or an IP address. Specify all for all interfaces.
label-map	<in-label>	Specifies the incoming label. Specify a decimal number between 0 and 4095. The interface will take any of the following actions on labels matching this label number:
next-hop	<name> <ip-address>	Specifies the next hop. Specify an interface name or IP address.
swap	<out-label>	Swaps the incoming label with a specified label number. The interface sends the label out as an outgoing label with the new label number. Specify a decimal number between 0 and 4095.
pop		Enables the label-pop action on the interface. The label-pop action takes the top label from the label stack, and leaves the next label as the top label on the stack.
push	<out-label-list>	Specifies one or more labels to be pushed onto the label stack. For each label, specify a decimal number between 0 and 4095. Use commas to separate the list of labels; the first label specified is the bottom of the stack.
reject		Discards the label traffic and sends an ICMP error message back to the sender.

Parameter	Value	Meaning
discard		Discards the label traffic without sending an ICMP error message.
pop-count	<i><num-labels></i>	Specifies the number of labels to be popped. Specify a number between 1-3.
preference	<i><number></i>	Specifies the preference of the interface. A smaller value indicates a more desirable interface. Specify a decimal number between 1 and 256.
admin-group	<i><group-list></i>	Specifies the administrative groups that are assigned to this LSP. Specify up to 32 separate groups. Enclose multiple groups within quotation marks. For example: “group1 group2 group3”.
override-trunk-behavior		Disables the default trunk port behavior for the MPLS interface.
subscription	<i><ratio></i>	The bandwidth subscription ratio. Specify a value between 0-64000.
bandwidth	<i><bps></i>	Specifies the bandwidth on the interface, in bits per second (bps). Specify a value between 1-1000000000.
no-php		Specifies that the router on this interface is not to pop the label stack even if it is the PHP LSR in the LSP. By default, an RS router that is a PHP LSR pops the MPLS label stack and forwards the IP packet to the egress LSR. If the no-php parameter is configured on an egress LSR, the egress router will notify the PHP LSR that it is not to pop the label stack. This parameter does not apply to static LSPs.

Restrictions

None

Example

The following command swaps a new label ‘122’ for all labels matching the label-map ‘120’ on the MPLS interface ‘customer1’:

```
rs(config)# mpls set interface customer1 label-map 120 swap 122 next-hop 10.10.10.12
```

mpls set l2-static-path

Mode

Configure

Format

```
mpls set l2-static-path <pathname> policy <policy>]
```

Description

The **mpls set l2-static-path** command allows you to apply an L2 policy to an L2 static path.

Parameter	Value	Meaning
path	<pathname>	Specifies the path name.
policy	<policy>	Specifies the name of the L2 policy created with the mpls create l2-policy command.

Restrictions

None

Example

The following command applies the L2 policy 'l2hipri' to the L2 static path 'cust3':

```
rs(config)# mpls set l2-static-path cust3 policy l2hipri
```

mpls set label-switched-path

Mode

Configure

Format

```
mpls set label-switched-path <pathname> primary <pathname>|secondary <pathname>
[admin-group <group-list>] [include <group-list>] [exclude <group-list>] [hop-limit <number>]
[preference <number>] [retry-limit <number>] [retry-interval <seconds>] [bps <bits>]
[class-of-service <number>] [no-switchback] [adaptive] [no-decrement-ttl] [no-cspf]
[no-record-route] [standby] [policy <policy>] [disable] [metric <number>] [mtu <number>]
```

Description

The **mpls set label-switched-path** command allows you to configure dynamic label switched path (LSP) parameters. The LSP must be created with the **mpls create label-switched-path** command.

Parameter	Value	Meaning
label-switched-path	<pathname>	Specifies the name for the LSP. Specify a character string.
primary	<pathname>	Specifies the name of the primary path. If you do not specify a primary path, the first configured secondary path is used.
secondary	<pathname>	Specifies the name of the secondary path. If you do not specify a primary path, secondary paths are tried in the order that they are configured.
admin-group	<group-list>	Specifies the administrative groups that are assigned to this LSP. Specify up to 32 separate groups. Enclose multiple groups within quotation marks. For example: "group1 group2 group3".
include	<group-list>	Includes a specified administrative group. Specify up to 32 separate groups. Enclose multiple groups within quotation marks. For example: "group1 group2 group3".
exclude	<group-list>	Excludes a specified administrative group. Specify up to 32 separate groups. Enclose multiple groups within quotation marks. For example: "group1 group2 group3".
hop-limit	<number>	Defines the hop limit. The hop limit is the maximum number of hops, including the ingress and egress routers, allowed in the LSP. Specify a decimal number between 1 and 255. The default is 255.
preference	<number>	Assigns a preference value for this LSP. This preference value is useful in the case where there are multiple LSPs between a source and destination. A smaller value signifies a more desirable path. The default is 7. Specify a decimal number between 1 and 255.

Parameter	Value	Meaning
retry-limit	<number>	Defines a retry limit for this LSP. Depending on the priority of an LSP, the RS will try to establish the path. However, if the path cannot be set up during the first try, the RS will retry a number of times. Specify a decimal number between 1 and 10000. The default value is 5000.
retry-interval	<seconds>	Defines the retry time interval for this LSP, in seconds. This parameter value specifies a time limit for establishing a path. Specify a decimal number between 1 and 600. The default value is 15.
bps	<bits>	Specifies the bandwidth allocated to this LSP, in bits. The default is 0.
class-of-service	<number>	Specifies a class-of-service (CoS) value for this LSP. CoS values are used for resource reservation features. A higher value specifies a higher class-of-service consideration. Specify a decimal number between 1 and 8.
no-switchback		Specifies not to switch back from the secondary path to the primary path when the primary becomes available.
adaptive		Specifies that the LSP exhibit adaptive behavior during path recalculation. When a LSP is adaptive, the LSP waits until the new route is setup before tearing down the old LSP. This prevents traffic disruption.
no-decrement-ttl		Disables normal TTL decrementing for LSPs signaled with RSVP. With normal decrementing, the packet's TTL is decremented by a value of 1 on each LSR on the LSP. Disabling TTL decrementing makes the whole LSP appear as one hop.
no-cspf		Specifies not to use constrained shortest path first algorithm to establish an LSP.
 Note If you are configuring an explicit LSP, you must specify the no-cspf parameter. Otherwise, the LSP will wait indefinitely for a valid CSPF response.		
no-record-route		Specifies that the route will not be recorded.
standby		Sets this path in standby mode.
policy	<policy>	Specifies the filter to be applied to this LSP.
disable		Disables the LSP.
metric	<number>	Specifies the metric for this LSP. Specify a value between 1-65534.
mtu	<number>	Specifies the maximum transmission unit (MTU) for the primary or secondary paths.

Restrictions

When configuring an explicit LSP, you must specify the **no-cspf** parameter. Otherwise, the LSP will wait indefinitely for a valid CSPF response.

Example

The following command configures a primary path 'path1' for the explicit LSP 'lsp1':

```
rs(config)# mpls set label-switched-path lsp1 primary path1 adaptive
```

mpls set path

Mode

Configure

Format

```
mpls set path <pathname> [type loose|strict] ip-addr <ipaddr/netmask> [hop <number>]
```

Description

The **mpls set path** command allows you to configure an explicitly-routed MPLS path by specifying each router that the path will traverse through. The path must be created with the **mpls create path** command.

Parameter	Value	Meaning
path	<string>	Specifies the path name.
type		Specifies the type of hop. Specify either loose or strict.
	loose	Specifies that the LSP can go through other hops before going through this hop.
	strict	Specifies that the LSP has to go through this hop. This is the default.
ip-addr	<ipaddr/netmask>	The IP address and netmask of the hop in the path, in the form 1.2.3.4/255.255.0.0 or 1.2.3.4/16.
hop	<number>	Specifies the hop number of the ip-addr in this path. Specify a number between 1-255. The hop number must be within the maximum number of hops for the path set with the num-hops parameter of the mpls create path command.

Restrictions

None

Example

The following command configures the the path 'path1' with a next hop to '130.140.0.1/24':

```
rs(config)# mpls set path path1 ip-addr 130.140.0.1/24
```

mpls set portlist

Mode

Configure

Format

```
mpls set portlist in-port-list <port list> [out-port <port list>] next-hop-mac <macaddr>
[label-map <in-label>][pop] [pop-count <num-labels>] [push <outlabel>] [swap
<out-label>][discard] [end-of-l2-tunnel-label <label>] [overwrite-1p <priority>] [vlanid
<vlan-id>] [overwrite-vlanid <vlan-id>]
```

Description

The **mpls set portlist** command allows you to configure various parameters for an MPLS L2 static path on the transit and egress LSRs.

Parameter	Value	Meaning
in-port-list	<port list>	Specifies the inbound MPLS port(s) for the static path.
out-port	<port list>	Specifies the outbound MPLS port(s) for the static path.
next-hop-mac	<macaddr>	Specifies the next hop MAC address. Specify a MAC address in the format xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.
label-map	<in-label>	Specifies the incoming label. Specify a decimal number between 16 and 4095. The interface will take any of the following actions on labels matching this label number:
pop		Enables the label-pop action on the interface. The label-pop action takes the top label from the label stack, and leaves the next label as the top label on the stack.
pop-count	<num-labels>	Specifies the number of labels to be popped. Specify a number between 1-3.
push	<out-label>	Specifies a new label to add to the top of the label stack. This label will become the active label when the label is sent out. Specify a decimal number between 16 and 4095.
swap	<out-label>	Swaps the incoming label with a specified label number. The interface sends the label out as an outgoing label with the new label number. Specify a decimal number between 16 and 4095.

Parameter	Value	Meaning
discard		Discards the label traffic without sending an ICMP error message.
end-of-l2-tunnel-label	<label>	Specifies the label that is the end of an L2 tunnel. Specify a value between 16-4095.
overwrite-1p	<priority>	Specifies the new 802.1p priority value. Specify a value between 0-7.
vlanid	<vlan-id>	Specifies the incoming VLAN ID. Specify a value between 1-4095.
overwrite-vlanid	<vlan-id>	Specifies the new VLAN ID. Specify a value between 1-4095.

Restrictions

None

Example

The following command specifies that the label 201 signifies the end of an L2 tunnel and will be popped:

```
rs(config)# mpls set portlist in-port-list gi.4.1 end-of-l2-tunnel-label 201
```

The following command replaces the label value '100' with '200' before the L2 frame is forwarded to the next hop:

```
rs(config)# mpls set portlist label-map 100 swap 200 next-hop-mac 00e063:3738ce  
in-port-list gi.4.1 out-port gi.5.1
```

mpls set static-path

Mode

Configure

Format

```
mpls set static-path <pathname> preference <number> bps <number> class-of-service  
<number> policy <policyname> disable [metric <number>] [mtu <number>]
```

Description

The **mpls set static-path** command allows you to configure parameters for a static path.

Parameter	Value	Meaning
static-path	<pathname>	Specifies the name of the static path.
preference	<number>	Assigns a preference value for this static path. This preference value is useful in the case where there are multiple LSPs between a source and destination. A smaller value signifies a more desirable path. Specify a decimal number between 1 and 256.
bps	<number>	Specifies the bandwidth allocated to this static path, in bits. Specify a decimal number between 1 and 10000000.
class-of-service	<number>	Specifies a class-of-service (CoS) value for this static path. CoS values are used for resource reservation features. A higher value specifies a higher class-of-service consideration. Specify a decimal number between 1 and 8.
policy	<policyname>	Specifies a policy to apply to this static path. Specify the name of a policy created with the mpls create policy command.
disable		Disables this static path.
metric	<number>	Specifies the metric for this LSP. Specify a value between 1-255.
mtu	<number>	Specifies the maximum transmission unit (MTU) for this LSP.

Restrictions

None

Example

The following command sets a static path 'path3' with a bandwidth of 100000 bps, and applies 'policy3' to it:

```
rs(config)# mpls set static path path3 bps 100000 policy policy3
```

mpls set trace-level

Mode

Enable/
Configure

Format

```
mpls set trace-level <level>
```

Description

The **mpls set trace-level** command allows you to set the MPLS tracing level.

Parameter	Value	Meaning
trace-level	<level>	Specifies the MPLS tracing level. Specify 0 to disable tracing. Otherwise, specify a value between 1-4, where 4 provides the most detailed level of tracing.

Restrictions

None

Example

The following command sets the tracing level to 4:

```
rs# mpls set trace-level 4
```


mpls set trace-options

Mode

Enable/
Configure

Format

`mpls set trace-options <option>`

Description

The **mpls set trace-options** command allows you to enable the type of tracing that is performed.

Parameter	Value	Meaning
trace-options	<i><option></i>	Specifies the type of tracing to be performed. Specify one or more of the following:
	lsp	Enables label switched path event tracing.
	ftn	Enables FTN tracing.
	ilm	Enables ILM tracing.
	label-mgmt	Enables label management tracing.
	session	Enables session management tracing.
	traffic-control	Enables traffic control tracing.
	timer	Enables timer tracing.
	error	Enables error tracing.
	none	No tracing is displayed.
	all	All tracing is displayed.

Restrictions

None

Example

The following command enables label switched path event tracing:

```
rs# mpls set trace-options lsp
```

mpls show admin-groups

Mode
Enable

Format

mpls show admin-groups

Description

The **mpls show admin-groups** command allows you to display administrative groups configured with the **mpls create admin-group** command.

Parameter	Value	Meaning
admin-groups		Displays administration groups.

Restrictions

None.

Example

The following is an example of the **mpls show admin-groups** command:

```
rs# mpls show admin-groups

      Group          Bit index
      ----          -
sector2             10
```

Table 40-1 Display field descriptions for the mpls show admin-groups command

Field	Description
Group	Name specified with the mpls create admin-group command.
Bit index	Group value specified with the mpls create admin-group command.

mpls show all

Mode

Enable

Format

`mpls show all`

Description

The **mpls show all** commands allows you to display various MPLS information.

Parameter	Value	Meaning
all		Displays all MPLS information.

Restrictions

None.

Example

The following is an example of the **mpls show all** command:

```
rs# mpls show all
MPLS Controller : <mpls_1>
-----
lsr-id      : 0x2020202 protection-lsp-id: 0x4002
trace level : 0
flags       : <merge auto-lsp>
protocols   : <MPLS RSVP>
Label Switched Paths:
-----
Explicit Paths:
-----
Explicit-Path: p1          num-hops: 3
      hop: 15.15.15.1      - strict
      hop: 15.15.15.2      - strict
      hop: 16.16.16.1      - strict
MPLS Interfaces:
-----
Interface      State      Administrative groups
lo              Up          <none>
to_rs9          Up          <none>
to_rs5          Up          <none>
Admin Groups:
-----

      Group              Bit index
      ----              -
      red                 10

MPLS L3 Policies:
-----
```

Name	Type	Destination	Port	Source	Port	TOS Prot	Use
pl1	L3	150.10.0.0	any	0.0.0.0	any	any IP	UNUSED
MPLS L2 Policies:							
Name	Type	Source MAC	Dest MAC	Vlan	Use		

Table 40-2 Display field descriptions for the mpls show all command

Field	Description
MPLS Controller	Displays the values of MPLS global parameters. See the mpls show global command for specific information.
Label Switched Paths	Displays MPLS dynamic path information. See the mpls show label-switched-paths command for specific information.
Explicit Paths	Displays MPLS explicit path information. See the mpls show paths command for specific information.
MPLS Interfaces	Displays MPLS interface information. See the mpls show interface command for specific information.
Admin Groups	Displays configured administrative groups. See the mpls show admin-groups command for specific information.
MPLS L3 Policies	Displays configured L3 policies. See the mpls show policy command for specific information.
MPLS L2 Policies	Displays configured L2 policies. See the mpls show l2-policy command for specific information.

mpls show global

Mode

Enable

Format

```
mpls show global
```

Description

The **mpls show global** command allows you to display MPLS global information.

Parameter	Value	Meaning
global		Displays MPLS global information.

Restrictions

None.

Example

The following is an example of the **mpls show global** command:

```
rs# mpls show global

MPLS Controller : <mpls_1>
-----
lsr-id          : 0x0
trace level    : 0
flags          : <merge auto-lsp swdata >
protocols      : <MPLS RSVP >
```

Table 40-3 Display field descriptions for the mpls show global command

Field	Description
MPLS Controller	Task name.
lsr-id	Router ID.
trace level	Trace level.

Table 40-3 Display field descriptions for the mpls show global command

Field	Description
flags	Configured attributes.
protocols	MPLS, RSVP, or LDP.

mpls show hw-cam-tbl

Mode

Enable

Format

```
mpls show hw-cam-tbl port <port-list> [index <index>]
```

Description

The **mpls show hw-cam-tbl** command allows you to display hardware context addressable memory (CAM) table entries for one or more ports.

Parameter	Value	Meaning
port	<port-list>	Displays the table entry for the specified port(s). Use commas to separate multiple port names.
index	<index>	Displays the table entry for the specified index number. Specify a number between 0-4095.

Restrictions

None.

Example

The following is an example of the **mpls show hw-cam-tbl** command:

```
RS1(mpls-show)# hw-cam-tbl port gi.4.2

Port: gi.4.2
-----
Entry 0, Total: 4096
  dmac/mask   : 0000:0000:0000/0000:0000:0000
  smac/mask   : 0000:0000:0000/0000:0000:0000
  1p/mask     : 0/0
  vlan_id/mask : 0/0
  etype/mask  : 0000/0000
  poe/mask    : 0010/01ff
  ott_index   : 3
  valid       : 1
Entry 1, Total: 4096
  dmac/mask   : 0000:0000:0000/0000:0000:0000
  smac/mask   : 0000:0000:0000/0000:0000:0000
  1p/mask     : 0/0
  vlan_id/mask : 0/0
  etype/mask  : 0000/0000
  poe/mask    : 0034/01ff
  ott_index   : 3
  valid       : 1
  .
  .
  .
(Entries continue)
```

Table 40-4 Display field descriptions for the **mpls show hw-cam-tbl** command

Field	Description
dmac/mask	Destination MAC address and mask.
smac/mask	Source MAC address and mask.
1p/mask	VLAN priority.
vlan_id/mask	VLAN ID.
etype/mask	Ethernet type.
poe/mask	Port of entry.
ott_index	Index to the output tag table.
valid	If set to 1, this is a valid CAM entry.

mpls show hw-ilm-err

Mode

Enable

Format

```
mpls show hw-ilm-err port <port-list> [index <index>]
```

Description

The **mpls show hw-ilm-err** command allows you to display the error in the hardware incoming label map (ILM) table entries for a specific entry for one or more ports.

Parameter	Value	Meaning
port	<port-list>	Displays the table entry for the specified port(s). Use commas to separate multiple port names.
index	<index>	Displays the table entry for the specified index number. Specify a number between 0-31743.

Restrictions

None.

Example

The following is an example of the **mpls show hw-ilm-err** command:

```
RS2# mpls show hw-ilm-err port gi.2.1
Port: gi.2.1
-----
Entry 16
Dropped packets : 0
Entry 17
Dropped packets : 0
Entry 18
Dropped packets : 0
```

Table 40-5 Display field descriptions for the mpls show hw-ilm-err command

Field	Description
Port	The port for which the error in the ILM table is displayed.
Entry	Index number of the ILM table entry.
Dropped packets	Number of packets dropped, either because the LSP was down or the label stack was malformed.

mpls show hw-ilm-tbl

Mode

Enable

Format

```
mpls show hw-ilm-tbl port <port-list> [index <index>]
```

Description

The **mpls show hw-ilm-tbl** command allows you to display hardware incoming label map (ILM) table entries for one or more ports.

Parameter	Value	Meaning
port	<port-list>	Displays the table entry for the specified port(s). Use commas to separate multiple port names.
index	<index>	Displays the table entry for the specified index number. Specify a number between 0-31743.

Restrictions

None.

Example

The following is an example of the **mpls show hw-ilm-tbl** command:

```

RS2# mpls show hw-ilm-tbl port gi.14.1

Port: gi.14.1
-----
Entry 16, UNICAST, Total: 15360
  check vlan      : 0          egress tos : 0
  end of mpls tunnel : 1        egress vlan id : 110
  end of l2 tunnel  : 0        egress vlan priority : 0
  send to cpu      : 0          egress etype : 2048
  exp rewrite      : 0          exp : 0
  vlan overwrite   : 0          output channel : 0
  prio overwrite   : 0          output port : 0
  ip tunnel        : 1          ott index : 0
  lsr hop hide     : 0          exp21qprio : 0
  overwrite tos mode : 0        byte count : 0
  overwritetos     : 0          packet count : 0
  state            : 1          packet drop : 0
Entry 17, UNICAST, Total: 15360
  check vlan      : 0          egress tos : 0
  end of mpls tunnel : 1        egress vlan id : 110
  end of l2 tunnel  : 0        egress vlan priority : 0
  send to cpu      : 0          egress etype : 2048
  exp rewrite      : 0          exp : 0
  vlan overwrite   : 0          output channel : 0
  prio overwrite   : 0          output port : 0
  ip tunnel        : 1          ott index : 0
  lsr hop hide     : 1          exp21qprio : 0
  overwrite tos mode : 0        byte count : 0
  overwritetos     : 0          packet count : 0
  state            : 1          packet drop : 0
Entry 18, UNICAST, Total: 15360
  .
  .
  .
(Entries continue)

```

Table 40-6 Display field descriptions for the mpls show hw-ilm-tbl command

Field	Description
check vlan	If this is set to 1, the input VLAN is checked against the egress VLAN. If the check fails, the packet is dropped.
egress tos	Used to rewrite IP ToS field at egress edge of L3 tunnels.
end of mpls tunnel	Set to 1 if this is the egress end of the L3 tunnel on this LSP.
egress vlan id	If the L2 tunneled frame is 802.1q, this value overwrites the 802.1q information.
end of l2 tunnel	Set to 1 if this is the egress end of the L2 tunnel on this LSP.

Table 40-6 Display field descriptions for the mpls show hw-ilm-tbl command

Field	Description
egress vlan priority	If the L2 tunneled frame is 802.1q and prio overwrite is set to 1, the priority field in the 802.1 information is overwritten with this value.
send to cpu	If set to 1 and state is down, packets for this ILM entry are sent to the CPU.
egress type	Ethertype of L3 protocol that is tunneled through MPLS.
exp rewrite	If set to 1, EXP bits of the top label from the ILM's exp field are rewritten. Applies to transit LSR packets only.
exp	Value used to rewrite top label from the ILM's exp field.
vlan overwrite	If set to 1, overwrite tunneled L2 frame's VLAN field. Applies to end of L2 tunnel only.
output channel	Output channel value 0-31.
prio overwrite	If set to 1, overwrite tunneled L2 frame's VLAN priority field. Applies to end of L2 tunnel only.
output port	Output port 0-15.
ip tunnel	If set to 1, this LSP is an L3 MPLS tunnel carrying IP traffic.
ott index	Index to output tag table.
lsr hop hide	If set to 1 and ip tunnel is 1, the IP packet's TTL field is not copied from the top label's TTL field. If set to 0 and ip tunnel is 1, the IP packet's TTL field is copied from the top label's TTL field. Applies to IP packets at the end of L3 tunnels only.
exp21qprio	Indexed by exp field of the top label to yield an 802.1q priority. This provides a way for the label's exp bits to indicate an internal RS priority when tunneling MPLS packets through the RS.
overwrite tos mode	If set to 0, the TOS field is overwritten by the MPLS label's exp field. If set to 1, the TOS field is overwritten by the ILM's TOS field. Applies to IP packets at the end of L3 tunnels only.
byte count	Number of bytes received on this LSP.
overwritetos	If set to 1 and ip tunnel is 1, the IP packet's TOS field is overwritten, depending on overwrite tos mode.
packet count	Number of packets received on this LSP.
state	If set to 1, this LSP is up. If set to 0, this LSP is down and traffic is dropped unless send to cpu is 1.
packet drop	Number of packets dropped, either because LSP was down or label stack was malformed.

mpls show hw-ott-err

Mode

Enable

Format

mpls show hw-ott-err port <port-list> [index <index>]

Description

The **mpls show hw-ott-err** command allows you to display errors for entries in the hardware output tag table (OTT) for one or more ports.

Parameter	Value	Meaning
port	<port-list>	Displays the table entry for the specified port(s). Use commas to separate multiple port names.
index	<index>	Displays the table entry for the specified index number. Specify a number between 0-15871.

Restrictions

None.

Example

The following is an example of the **mpls show hw-ott-err** command:

```
RS2# mpls show hw-ott-err port gi.2.1
Port: gi.2.1
-----
Entry 1
Dropped packets : 0
```

Table 40-7 Display field descriptions for the mpls show hw-ott-err command

Field	Description
Port	The port for which the error in the OTT table is displayed.

Table 40-7 Display field descriptions for the mpls show hw-ott-err command

Field	Description
Entry	Index number of the OTT table entry.
Dropped packets	Number of packets dropped, either because the LSP was down or the label stack was malformed.

mpls show hw-ott-tbl

Mode

Enable

Format

```
mpls show hw-ott-tbl port <port-list> [index <index>]
```

Description

The **mpls show hw-ott-tbl** command allows you to display hardware output tag table (OTT) table entries for one or more ports.

Parameter	Value	Meaning
port	<port-list>	Displays the entries for the specified port(s). Use commas to separate multiple port names.
index	<index>	Displays the specified entry for the specified port. Specify a number between 0-15871.

Restrictions

None.

Example

The following is an example of the **mpls show hw-ott-tbl** command that shows all entries for the port gi.14.1:

```

RS2# mpls show hw-ott-tbl port gi.14.1

Port: gi.14.1
-----
Entry 1, Total: 7680
dot1p source      : 0          output_vlan id : 110
dot1p enabled     : 0          output_vlan priority : 0
dot1q enabled     : 0          mtu : 1568
overwrite_ttl     : 0          next_hop_mac : 00e0:6311:0012
rate limit violated : 0          php_etype : 2048
rate limit enable : 0          label0 : 16:0:0:0
no exp support    : 0          label1 : 528207
start of l2 tunnel : 0          label2 : 0
trunk lsp        : 0          ip_da : 0
ip tunnel        : 0          byte count : 0
lsr hop hide     : 0          packet count : 0
llc snap encaps  : 0          malformed_label_drops : 0
send to cpu      : 0
state           : 1
Entry 2, Total: 7680
dot1p source      : 0          output_vlan id : 110
dot1p enabled     : 0          output_vlan priority : 0
dot1q enabled     : 0          mtu : 1568
overwrite_ttl     : 0          next_hop_mac : 00e0:6311:0012
rate limit violated : 0          php_etype : 2048
rate limit enable : 0          label0 : 16:0:0:0
no exp support    : 0          label1 : 528207
start of l2 tunnel : 0          label2 : 1048575
trunk lsp        : 0          ip_da : 0
ip tunnel        : 0          byte count : 0
lsr hop hide     : 0          packet count : 0
llc snap encaps  : 0          malformed_label_drops : 0
send to cpu      : 0
state           : 1
.
.
.
(Entries continue)

```

The following is an example of the **mpls show hw-ott-tbl** command that shows entry 3 for port gi.4.2:

```
RS1# mpls show hw-ott-tbl port gi.4.2 index 3

Port: gi.4.2
-----
Entry 3, Total: 7680
dot1p source      : 0          output_vlan id : 0
dot1p enabled     : 0          output_vlan priority : 0
dot1q enabled     : 0          mtu : 0
overwrite_ttl     : 0          next_hop_mac : 0000:0000:0000
rate limit violated : 0          php_etype : 0
rate limit enable : 0          label0 : 0:0:0:0
no exp support    : 0          label1 : 0
start of l2 tunnel : 0          label2 : 0
trunk lsp         : 0          ip_da : 0
ip tunnel         : 0          byte count : 0
lsr hop hide      : 0          packet count : 0
llc snap encaps  : 0          malformed_label_drops : 0
send to cpu       : 0
state             : 0
```

Table 40-8 Display field descriptions for the mpls show hw-ott-tbl command

Field	Description
dot1p source	Specifies where 802.1p information for the MPLS encapsulation is obtained.
output_vlan id	VLAN ID for packets that will be 802.1q encapsulated.
dot1p enabled	If set to 1, MPLS packets will be 802.1q encapsulated. If set to 0 but dot1q enabled is 1, 802.1q encapsulation is done with 1q set to 0.
output_vlan priority	802.1p priority for 802.1 encapsulated packets.
dot1q enabled	If set to 1, MPLS packets will be 802.1q encapsulated with the VLAN taken from the OTT's output_vlan id. If set to 0 and dot1p enabled is 1, 802.1q encapsulation is done with 1q set to 0. If set to 0 and dot1p enabled is 0, no 802.1q encapsulation is done.
mtu	Maximum transmission unit for this LSP. If labeled frame exceeds MTU and the packet is IP, the packet is fragmented.
overwrite_ttl	On ingress LSR for routed packets, the packet's IP TTL is copied to the MPLS TTL of the top label. Otherwise, the TTL is taken from the TTL for the label in the OTT.
next_hop_mac	Destination MAC address (next MPLS hop).
rate_limit violated	The FEC for this OTT entry has violated its rate limit for this time slice.
php_etype	Ethernet type for tunneled L3 frames when doing PHP as an LSR.
rate_limit enable	If set to 1, rate limiting is enabled for this OTT entry.

Table 40-8 Display field descriptions for the mpls show hw-ott-tbl command

Field	Description
label0	Bottom-most label pushed onto the label stack.
no exp support	If set to 1, MPLS exp field on the top label is set to 0.
label1	Next-to-bottom label pushed onto the label stack.
start of l2 tunnel	If set to 1, this is the ingress of an L2 tunnel.
label2	Top label pushed onto the label stack.
trunk lsp	If set to 1, and start of l2 tunnel is 1, tunneled Ethernet frames are 802.1 encapsulated.
ip_da	IP destination address.
ip tunnel	If set to 1, the LSP is carrying IP traffic.
byte count	Number of bytes received on this LSP.
lsp hop hide	If set to 1 and ip tunnel is 1, the IP TTL is decremented for PHP. If set to 0, the MPLS TTL is copied to the tunneled IP packet.
packet count	Number of packets received on this LSP.
llc snap encaps	If set to 1, MPLS packets are emitted as 802.3 with SNAP. If set to 0, MPLS packets are emitted as Ethernet II.
malformed_label_drops	Number of packets dropped due to malformed label stack.
send to cpu	If set to 1 and state is 0, send packets to the CPU.
state	If set to 1, the LSP is up. If set to 0, the LSP is down.

mpls show ilm-tbl

Mode

Enable

Format

```
mpls show ilm-tbl <interface-name>|<ipaddr>|all [brief|verbose]
```

Description

The **mpls show ilm-tbl** command allows you to display the incoming label map (ILM) table information for a specified interface or all interfaces.

Parameter	Value	Meaning
ilm-tbl	<interface-name> <ipaddr>	Displays the table information for the specified interface.
	all	Specify all to display information for all MPLS interfaces.
brief		This optional parameter displays summarized information.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show ilm-table** command:

```
RS2# mpls show ilm-table all
Interface      Labels
-----
lo             16
               17

to_RS1         16
               17
               18
               19

to_RS3         16
               17
               18
               19
```

Table 40-9 Display field descriptions for the mpls show ilm-table command

Field	Description
Interface	Interface name.
Labels	Incoming label values used on this interface.

mpls show interface

Mode
Enable

Format

```
mpls show interface <name> | <ip-address >| all [label-map <label>|brief|verbose]
```

Description

The **mpls show interface** command allows you to display MPLS interface information.

Parameter	Value	Meaning
interface	<name> <ip-address>	Displays MPLS interface information. Specify an interface name or an IP address.
	all	Specify all to display information on all MPLS interfaces.
label-map	<label>	Displays the label mapping for a particular label value. Specify a number between 0-4095.
brief		This optional parameter displays summarized information.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show interface** command:

```
rs# mpls show interface all
Interface      State      Administrative groups
lo             Up         <none>
lo             Up         <none>
R2R3           Up         sector2
R2R1           Up         <none>
R2R1b          Up         sector2
```

Table 40-10 Display field descriptions for the mpls show interface command

Field	Description
Interface	Interface name.
State	Interface state, either Up or Down.
Administrative groups	Administrative group, if any, that is applied to this interface.

The following is an example of the **mpls show interface** command with the **label-map** option:

rs# mpls show interface to_rs9 label-map 16			
Interface	In label	Nexthop	Action
-----	-----	-----	-----
to_rs9	16	0.0.0.0	Default [Discard]

Table 40-11 Display field descriptions for the mpls show interface command with label-map option

Field	Description
Interface	Interface name.
In label	Incoming label value.
Nexthop	Next hop for the labeled packet.
Action	Action for the labeled packet.

The following is an example of the **mpls show interface** command with the **verbose** option:

```
rs# mpls-show)# interface to_rs9 verbose

====>Interface: <to_rs9>
      Index: 3 Vlan: 2 Address 802.2 0:0:1d:a9:a8:6f  Change: <>
      State: <Up Broadcast Multicast Simplex>
      Refcount: 2      Up-down transitions: 1

      12.12.12.1
          Metric: 4      MTU: 1436
          Refcount: 1      Preference: 0      Down: 120
          Broadcast Address: 12.12.12.255
          Subnet Number: 12.12.12 Subnet Mask: 255.255.255

      MPLS active configuration:
      --->proto: <static rsvp>      end-of-tunnel-label: 16
          flags: <>
          (mplsIfId: 0x81f62f38 rsvpIfId: 0x3 ldpIfId: 0x0)
      MPLS saved configuration:
      --->proto: <static rsvp>      end-of-tunnel-label: 0
          flags: <>

      Label-map [Config]:
          in-label:
      Label-map [Active]:
          in-label:

Subscription 100
Incoming Direction:
StaticBW 1000000000bps, AvailableBW 1000000000bps
ReservedBW [0]      0bps [1]      0bps [2]      0bps [3]      0bps
             [4]      0bps [5]      0bps [6]      0bps [7]      0bps
Outgoing Direction:
StaticBW 1000000000bps, AvailableBW 1000000000bps
ReservedBW [0]      0bps [1]      0bps [2]      0bps [3]      0bps
             [4]      0bps [5]      0bps [6]      0bps [7]      0bps
```

Table 40-12 Display field descriptions for the mpls show interface command with verbose option

Field	Description
Interface	Interface name, IP address and interface characteristics.
MPLS active configuration	Currently running MPLS configuration.
MPLS saved configuration	User configured (but not necessarily currently running) MPLS configuration.
Label-map [Config]	User configured (but not necessarily currently running) label mapping.
Label-map [Active]	Currently running label mapping.
Subscription	Percentage of the bandwidth of the link that can be reserved by RSVP.

Table 40-12 Display field descriptions for the mpls show interface command with verbose option

Field	Description
StaticBW	Bandwidth available on the interface.
ReservedBW	Bandwidth reserved for each priority level.

mpls show l2-policy

Mode
Enable

Format

```
mpls show l2-policy <polycyname> [all [brief|verbose]
```

Description

The **mpls show l2-policy** command allows you to display MPLS L2 policy information.

Parameter	Value	Meaning
l2-policy	<polycyname>	Displays MPLS L2 policy information. Specify a policy name.
	all	Specify all to display information on all policies.
brief		This optional parameter displays summarized information. This is the default.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show l2-policy** command:

rs# mpls show l2-policy all					
Name	Type	Source MAC	Dest MAC	Vlan	Use
allow1	L2	000000:01E000	000000:000000	1	UNUSED

Table 40-13Display field descriptions for the mpls show l2-policy command

Field	Description
Name	Name of the L2 policy.
Type	Policy type (L2).
Source MAC	Source MAC specified by this policy.

Table 40-13 Display field descriptions for the mpls show l2-policy command

Field	Description
Dest MAC	Destination MAC specified by this policy. If all zeros are shown, the specified destination MAC is any.
Vlan	VLAN ID specified by this policy.
Use	INUSE shows that the policy is currently applied to a static path. UNUSED shows that the policy is not currently applied to a static path.

The following is an example of the **mpls show l2-policy** command with the **verbose** option:

```
rs# mpls show l2-policy all verbose

Name           : allow1
Type           : L2
Source MAC     : 000000:01E000
Source MAC Mask : FFFFFFFF:FFFFFF
Dest MAC      : 000000:000000
Dest MAC Mask  : 000000:000000
Vlan Id       : 1
1p Priority    : 0
BackBone Vlan Id : 0
BackBone 1p Priority: 0
Preserve Original Vlan Info: No
Input Ports   : gi.2.1
Output Ports  : gi.2.2
Usage        : not in use
```

Table 40-14 Display field descriptions for the mpls show l2-policy command with verbose option

Field	Description
Name	Name of the L2 policy.
Type	Policy type (L2).
Source MAC	Source MAC specified by this policy.
Source MAC Mask	Source MAC mask.
Dest MAC	Destination MAC specified by this policy. If all zeros are shown, the specified destination MAC is any.
Dest MAC Mask	Destination MAC mask.
Vlan	VLAN ID specified by this policy.
1p Priority	802.1p priority of the incoming packet.
BackBone Vlan Id	ID of the backbone VLAN to use for sending out traffic.
BackBone 1p Priority	802.1p priority to use when sending out traffic.

Table 40-14Display field descriptions for the mpls show l2-policy command with verbose option

Field	Description
Preserve Original Vlan Info	Specifies that the original VLAN ID is preserved when sending out traffic.
Input Ports	Ports where this policy is applied.
Output Ports	Ports to use when sending out traffic.
Usage	Shows whether the policy is currently applied to an L2 static path.

mpls show label-switched-paths

Mode

Enable

Format

`mpls show label-switched-paths <pathname> | all | ingress | transit | egress [brief | verbose]`

Description

The **mpls show label-switched-paths** command allows you to display MPLS dynamic path information.

Parameter	Value	Meaning
label-switched-paths	<pathname>	Displays MPLS dynamic path information. Specify a LSP name.
	all	Specify all to display information on all LSPs.
	ingress	Displays information on ingress LSPs only.
	transit	Displays information on transit LSPs only.
	egress	Displays information on egress LSPs only.
brief		This optional parameter displays summarized information. This is the default display.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show label-switched-paths** command:

```

rs# mpls-show label-switched-paths all

Ingress LSP:
LSPname      To      From      State LabelIn LabelOut
lsp1-5       99.1.1.5   7.7.7.7   Down   -      -
lsp1-4       99.1.1.4   7.7.7.7   Down   -      -
lsp1-3       99.1.1.3   7.7.7.7   Down   -      -
lsp1-2       99.1.1.2   7.7.7.7   Down   -      -
lsp1-1       99.1.1.1   7.7.7.7   Down   -      -
dl1         2.2.2.2    7.7.7.7   Up     -      18

Transit LSP:
LSPname      To      From      State LabelIn LabelOut
FIX          3.3.3.3   99.9.9.10 -      18      16
TEST         3.3.3.3   4.4.4.4   -      19      16

Egress LSP:

```

LSPname	To	From	State	LabelIn	LabelOut
dl2_pp2537	7.7.7.7	2.2.2.2	-	16	-

Table 40-15 Display field descriptions for the mpls show label-switched-paths command

Field	Description
Ingress LSP, Transit LSP, Egress LSP	Displays the LSPs for which the local router is an ingress, transit, or egress LSR.
LSPname	Name of the LSP.
To	Destination address for this LSP.
From	Source address for this LSP.
State	State of this LSP.
LabelIn	Incoming label value for this LSP.
LabelOut	Outgoing label value for this LSP.

The following is an example of the **mpls show label-switched-paths** command with the **verbose** option:

```
rs# mpls-show label-switched-paths NEW1 verbose

Label-Switched-Path: "NEW1"
  to: 4.4.4.4          from: 2.2.2.2
  state: Null          lsp-id: 0x6
  proto: <rsvp>         protection: none
  setup-pri: 7         hold-pri: 0
  attributes: <PRI BPS COS HOP_LIMIT RETRY_LIMIT RETRY_INT OPT_INT>

Protection-Path "p1": <Primary>
  state: Null          lsp-id: 0x4001
  attributes: <PREF BPS RETRY_LIMIT OPT_INT>
Path-Signalling-Parameters:
  attributes: <STANDBY RETRYING>
  inherited-attributes: <ADAPTIVE>
  retry-limit: 10       retry-int: 3 sec.
  retry-count: 0        next_retry_int: 0.000000 sec.
  bps: 20000000         preference: 255
  hop-limit: 255        opt-int: 720 sec.
  ott-index: 0          ref-count: 0
  explicit-path: "p1"   num-hops: 3
                      15.15.15.1   - strict
                      15.15.15.2   - strict
                      16.16.16.1   - strict
```

Table 40-16 Display field descriptions for the mpls show label-switched-paths command with verbose option

Field	Description
Label-Switched-Path	Name of the LSP.
to	Destination (egress LSR).
from	Source (ingress LSR).

Table 40-16 Display field descriptions for the mpls show label-switched-paths command with verbose option

Field	Description
state	State of the LSP. It can be either Up, Down, or Null (not initialized).
lsp-id	LSP ID.
proto	RSVP.
protection	Primary, Secondary, or none.
setup-pri	Setup priority value for this LSP. The default value is 7.
hold-pri	Hold priority value for this LSP. The default value is 0.
attributes	Configured LSP attributes.
Protection-Path	Primary or Secondary.
State	State of the path. The state is either Up or Down.
lsp-id	Path ID.
attributes	Configured path attributes.
Path-Signaling-Parameters	Configured or default parameters.
attributes	Configured attributes.
inherited-attributes	Inherited attributes.
retry-limit	Retry limit for this LSP. The default value is 5000.
retry-int	Retry interval for this LSP in seconds. The default is 15 seconds.
retry-count	Number of retries.
next_retry_int	Number of seconds before the next retry interval.
bps	The bandwidth, in bits, allocated to this LSP.
preference	Preference value for this LDP.
hop-limit	Maximum number of hops configured for this LSP.
opt-int	Optimize interval in minutes. The default value is 5 minutes.
ott-index	Index for this LSP in the OTT.
ref-count	OTT reference count.
explicit-path	Name of the explicit path.
num-hops	Number of hops configured for the explicit path. Also shown is the address of the router in this path and whether the address is configured as strict or loose.

mpls show ott-table

Mode

Enable

Format

```
mpls show ott-table <interface>|<ipaddr>|all [brief|verbose]
```

Description

The **mpls show ott-table** command allows you to display software OTT information. The software maintains pointers to entries in the hardware OTT.

Parameter	Value	Meaning
ott-table	<interface> <ipaddr>	Specifies the interface name or IP address. The OTT table for that interface or IP address will be displayed.
	all	Specify all to display the OTT table for all interfaces.
brief		This optional parameter displays summarized information.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show ott-table** command:

RS2# mpls show ott-table all							
Interface	OTT	RefCount	HW-OTT	RefCount	NextHop	Vlan	Labels

lo	3	1	0	0	200.135.89.5	2	[18]
	4	1	0	0	200.135.89.5	2	[19]
	5	1	0	0	200.135.89.5	2	[20]
	6	1	0	0	200.135.89.5	2	[21]
	7	1	0	0	200.135.89.5	2	[22]
	8	1	0	0	200.135.89.5	2	[23]
	9	1	0	0	200.135.89.5	2	[24]
	10	1	0	0	200.135.89.5	2	[17]
	11	1	0	0	101.1.1.11	6	[17]
	12	1	3	1	200.135.89.5	2	[25]
RS7-RS3							
RS7-RS4	12	1	3	1	200.135.89.5	2	[25]

Table 40-17 Display field descriptions for the mpls show ott-table command

Field	Description
Interface	Interface name.
OTT	Index of entry in software OTT table.
RefCount	Reference count.
HW-OTT	Index to entry in hardware OTT table (displayed with the mpls show hw-ott-tbl command).
RefCount	Reference count.
NextHop	Next hop address for this entry.
Vlan	VLAN ID.
Labels	Label value for this entry.

mpls show paths

Mode
Enable

Format

mpls show paths <pathname> [all [brief|verbose]]

Description

The **mpls show paths** command allows you to display MPLS path information.

Parameter	Value	Meaning
paths	<pathname>	Displays MPLS path information. Specify a path name.
	all	Specify all to display information on all paths.
brief		This optional parameter displays summarized information.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show paths** command

```
rs# mpls show paths all

Explicit-Path: p1      num-hops: 3
    hop: 15.15.15.1    - strict
    hop: 15.15.15.2    - strict
    hop: 16.16.16.1    - strict
```

Table 40-18Display field descriptions for the mpls show paths command

Field	Description
Explicit-path	Name specified with the mpls create path command.
num-hops	Number of hops configured for this path.
hop	Address of the router in this path and whether the address is configured as strict or loose.

mpls show policy

Mode
Enable

Format

```
mpls show policy <policyname> | all [brief|verbose]
```

Description

The **mpls show policy** command allows you to display configured MPLS policies, whether or not they are applied to LSPs. You can also use the **ip-policy show** command to display policies, including MPLS policies, that are active (in use).

Parameter	Value	Meaning
policy	<policyname>	Displays MPLS policy information. Specify a policy name.
	all	Specify all to display information on all policies.
brief		This optional parameter displays summarized information. This is the default.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show policy** command:

rs# mpls show policy all								
Name	Type	Destination	Port	Source	Port	TOS	Prot	Use
p1	L3	150.10.0.0	any	0.0.0.0	any	any	IP	INUSE
p3	L3	180.135.89.0	any	0.0.0.0	any	any	IP	
p2	L3	160.10.0.0	any	0.0.0.0	any	any	IP	
pp	L3	96.9.9.0	any	0.0.0.0	any	any	IP	
p1s	L3	160.10.0.0	any	0.0.0.0	any	any	IP	
II	L3	96.0.0.0	any	0.0.0.0	any	any	IP	

Table 40-19Display field descriptions for the mpls show policy command

Field	Description
Name	Name of the policy specified with the mpls create policy command.
Type	Layer 3 (L3) policy.
Destination	Destination IP address, if specified.
Port	Destination port, if specified.
Source	Source IP address, if specified.
Port	Source port, if specified.
TOS	Type of service value.
Prot	Protocol, either TCP, UDP, or IP.
Use	INUSE shows that the policy is currently applied to an LSP. UNUSED shows that the policy is not currently applied to an LSP.

The following is an example of the **mpls show policy** command with the **verbose** option:

rs# mpls show policy all verbose	
Name	: pl1
Type	: L3
Source address	: anywhere
Source Port	: any
Destination address	: 150.10.0.0/16
Destination Port	: any
TOS	: any
TOS Mask	:
Protocol	: IP
Used by	: not in use

Table 40-20Display field descriptions for the mpls show policy command with verbose option

Field	Description
Nmae	Name of the policy specified with the mpls create policy command.
Type	Layer 3 (L3) policy.
Source address	Source IP address.
Source Port	Source port, if specified.
Destination address	Destination IP address.
Destination Port	Destination port, if specified.
TOS	Type of service value.
TOS Mask	Type of service mask.

Table 40-20 Display field descriptions for the mpls show policy command with verbose option

Field	Description
Protocol	Protocol, either TCP, UDP, or IP.
Used by	The name of the LSP to which this policy has been applied.

mpls show static-paths

Mode

Enable

Format

```
mpls show static-paths <pathname> |all [brief|verbose]
```

Description

The **mpls show static-paths** command allows you to display MPLS static path information.

Parameter	Value	Meaning
static-paths	<pathname>	Displays MPLS static path information. Specify a static path name.
	all	Specify all to display information on all static paths.
brief		This optional parameter displays summarized information.
verbose		This optional parameter displays detailed information.

Restrictions

None.

Example

The following is an example of the **mpls show static-paths** command :

rs# mpls show static-paths all					
Ingress LSP:					
LSPname	To	From	State	LabelIn	LabelOut
lsp0	3.1.1.1	2.1.1.1	Up	-	102
					101
					100

Table 40-21Display field descriptions for the mpls show static-paths command

FIELD	DESCRIPTION
LSPname	User-defined name of the static path.
To	Destination address for the static path.
From	Source address for the static path.
State	State of the static path, either Up or Down.

Table 40-21Display field descriptions for the mpls show static-paths command (Continued)

FIELD	DESCRIPTION
LabelIn	Incoming label.
LabelOut	Outgoing label.

The following is an example of the **mpls show static-paths** command with the **verbose** option:

```
rs# mpls show static-paths all verbose

Ingress LSP:

  Label-Switched-Path: "lsp0"
    to: 3.1.1.1          from: 2.1.1.1
    state: Up            lsp-id: 0x1b
    proto: <static>      protection: none
    setup-pri: 7         hold-pri: 0
    attributes: <POLICY>

    Path-Signalling-Parameters:
      attributes: <NO-CSPF>
      inherited-attributes: <>
      retry-limit: 5000   retry-int: 3 sec.
      retry-count: 5000  next_retry_int: 0.000000 sec.
      bps: 0              preference: 7
      hop-limit: 255      opt-int: 600 sec.
      ott-index: 1        ref-count: 1
      mtu: 0
    Policies applied :
      p0

Transit LSP:

Egress LSP:
```

Table 40-22Display field descriptions for the mpls show static-paths command with verbose option

FIELD	DESCRIPTION
Label-Switched-Path	User-defined name of the LSP.
to	Egress router for the LSP.
from	Router ID of the local router, unless a different IP address has been configured.
state	State of the LSP, either Up or Down.
lsp-id	Internal ID for the LSP.
proto:	<static> specifies that this is a static path LSP.
protection	Not applicable for static paths.
setup-pri	Setup priority value for this LSP.

Table 40-22Display field descriptions for the mpls show static-paths command with verbose option

FIELD	DESCRIPTION
hold-pri	Hold priority value for this LSP.
attributes	<POLICY> specifies that a policy has been applied to this LSP.
Path-Signalling-Parameters	Not applicable for static paths.
attributes	Not applicable for static paths.
inherited-attributes	Not applicable for static paths.
retry-limit	Retry limit for this LSP. The default value is 5000.
retry-int	Retry interval for this LSP in seconds. The default is 15 seconds.
retry-count	Number of retries.
next_retry_int	Number of seconds before the next retry interval.
bps	The bandwidth, in bits, allocated to this LSP.
preference	Preference value for this LDP.
hop-limit	Maximum number of hops configured for this LSP.
opt-int	Optimize interval in minutes. The default value is 5 minutes.
ott-index	Index for this LSP in the OTT.
ref-count	Reference count.
mtu	MTU size.
Policies applied	Policies applied to this static path.

mpls start

Mode

Configure

Format

`mpls start`

Description

The **mpls start** command allows you to start MPLS on the RS. You must first enable MPLS on the appropriate interfaces with the **mpls add interface** command.

Parameter	Value	Meaning
start		Starts MPLS functionality.

Restrictions

None

Example

The following commands enable MPLS on the router interface 'sector1' and then starts MPLS:

```
rs(config)# mpls add interface sector1
rs(config)# mpls start
```


41 MTRACE COMMAND

mtrace

Mode

User

Format

```
mtrace <source> [destination <IPaddr>] [group <IPaddr>] [max-hops <number>]
```

Description

The **mtrace** command tracks the multicast path from a source to a receiver. A trace probe is sent in a reverse path from the receiver back to the source. As the probe passes from hop to hop, it collects information such as interface address and packet counts from each router. If the **mtrace** command is executed with only the source parameter, then a multicast path is calculated from the *source* to the RS. One can examine the multicast path between two external hosts by specifying a receiver instead of using the RS as the default receiver.

Parameter	Value	Meaning
mtrace	<source>	IP address of the source.
destination	<IPaddr>	Destination IP address.
group	<IPaddr>	Multicast destination group address.
max-hops	<number>	Maximum number of hops to trace (default: 0, range: 0-32).

Restrictions

None.

Examples

To display the multicast path from IP address 2.2.2.2 to the RS:

```
rs# mtrace 2.2.2.2
```

To display the multicast path from 1.1.1.1 to x.y.z.w for the group 239.1.1.1:

```
rs# mtrace 1.1.1.1 destination x.y.z.w group 239.1.1.1
```

42 MULTICAST COMMANDS

The **multicast** commands let you display information about IP multicast interfaces.

42.1 COMMAND SUMMARY

The following table lists the **multicast** commands. The sections following the table describe the command syntax for each command.

<code>multicast show interface [<ipAddr> <hostname>]</code>
<code>multicast show mroutes [child <IPaddr>] [group <ipaddr>] [parent <IPaddr>]</code>

multicast show interface

Mode
Enable

Format

multicast show interface [*<ipAddr>*|*<hostname>*]

Description

The **multicast show interface** command displays interfaces that are running IGMP or DVMRP.



Note This command is a superset of the **dvmrp show interface** and **igmp show interface** commands.

Parameter	Value	Meaning
interface	<i><ipAddr></i> <i><hostname></i>	IP address or hostname of the interface.

Restrictions

None.

Examples

To display IP multicast information about interface 10.50.89.90:

```
rs# multicast show interface 10.50.89.90
```

The following example shows a larger listing.

```
rs# multicast show interface

Address: 12.12.12.40          Subnet: 12.12.12/24          Met: 1   Thr: 1
Name   : icast_client        State: Dn   Igmp

Address: 1.1.10.20           Subnet: 1.1/16              Met: 1   Thr: 1
Name   : icast_svr           State: Up   Igmp Querier Leaf
Groups : 224.2.190.110
         224.2.127.254

Address: 20.20.20.20         Subnet: 20.20.20/24          Met: 1   Thr: 1
Name   : r3-r2               State: Up   Dvmrp
Peer   : 20.20.20.2          Version:   3.255             Flags:0xf  GID:
0x4678
rs#
```

Table 42-1 Display field descriptions for the multicast show interface command

FIELD	DESCRIPTION
Address	IP address of the interface
Subnet	Subnet of the interface
Met	DVMRP cost of the interface
Thr	Time-To-Live (TTL) Threshold of the interface. Any incoming packets with a TTL that is less than or equal to the threshold may be consumed locally but will not be forwarded.
Name	Name of the interface
State	Up—Indicates that this interface is up Dn—Indicates that this interface is down Querier—Indicates that this interface is an IGMP querier Leaf—Indicates that this interface is a leaf node in the multicast distribution tree Igmp—Indicates that IGMP is enabled on this interface Dvmrp—Indicates that DVMRP is enabled on this interface
Groups	List of the groups that are present on this interface. If no groups are listed, it means that there are no multicast receivers on this interface.
Peer	IP address of DVMRP peer(s)
Flags	Flags in the DVMRP probe message that the listed peer sent
Version	Version of DVMRP that the listed peer is running
GID	Peer's Generation ID—changes every time the router reboots or DVMRP restarts

multicast show mroutes

Mode

Enable

Format

```
multicast show mroutes [child <ipaddr>] [group <ipaddr>] [parent <ipaddr>]
```

Description

The **multicast show mroutes** command displays the IP multicast forwarding table entries.

This command lists all the multicast distribution trees, showing the parent interface (from where the traffic is coming), and the children distribution interfaces (to which the traffic is being forwarded). It would also show any cache information available either in hardware forwarding mechanism or in the main processor (for software based forwarding).



Note

The cache information can be timed out when not enough traffic is present, but multicast routes can still be present. Cache information is presented in number of flows (Layer 4 sessions). Multicast routes stay at least for 5 minutes, while the hardware forwarding mechanism can time out a flow faster. Any pruning information, if present, is also shown.

The search can always be narrowed by looking at a particular group, and/or looking at a particular parent interface, and/or looking at a particular child interface. Multicast routes are not the same as DVMRP routes.

Parameter	Value	Meaning
child	<ipaddr>	Address of a child interface.
group	<ipaddr>	Address of a multicast group.
parent	<ipaddr>	Address of a parent interface.

Restrictions

None.

Examples

To display the IP multicast route entry for the group 225.0.0.10:

```
rs# multicast show mroutes group 225.0.0.10
```


Here is a fuller example of the output from this command.

```
rs# multicast show mroutes
Multicast Routing Cache Table (SG Entries: 2 , Cache Entries: 2 )

Network: 12.12.12/24      Group: 224.2.190.110    Age: 5m
Parent : C2              Child: r2-r1
Source : 12.12.12.12     Pkts: 0                Flows: 0

Network: 1.1/16          Group: 224.2.190.110    Age: 61s
Parent : r2-r1           Child: C2
Source : 1.1.10.1        Pkts: 5801             Flows: 2
```

Table 42-2 Display field descriptions for the multicast show mroutes command

FIELD	DESCRIPTION
Network	Source subnet
Group	Destination multicast group
Age	Age, in seconds, of this entry
Parent	Name of incoming interface
Child	Name(s) of outgoing interface(s)
Source	IP address of the multicast source
Pkts	Number of packets that have been switched on this route
Flows	Number of L3 flows that have been used for switching this route

43 NAT COMMANDS

The `nat` commands allow you to define Network Address Translation (NAT) bindings for local (inside) and global (outside) network addresses.

43.1 COMMAND SUMMARY

The following table lists the **nat** commands. The sections following the table describe the command syntax for each command.

<code>nat clear-err-stats out-of-globals port-mode</code>
<code>nat create dynamic local-acl-pool <local-acl> global-pool <ip-addr/ip-addr-range/ip-addr-list> [matches-interface <interface>] [enable-ip-overload]</code>
<code>nat create static protocol ip tcp udp local-ip <local-ip-addr/address range> global-ip <global-ip-addr/address range> [local-port <tcp/udp-local-port> any] [global-port <tcp/udp-global-port> any]</code>
<code>nat flush-dynamic-binding all pool-specified [local-acl-pool <local-acl>] [global-pool <ip-addr/ip-addr-range> type-specified owner-specified [dns ftp-control ftp-data]</code>
<code>nat set dns-session-timeout <num></code>
<code>nat set dns-translation-state enable</code>
<code>nat set dynamic-binding-timeout <minutes> disable</code>
<code>nat set ftp-control-port <port number></code>
<code>nat set ftp-session-timeout <minutes></code>
<code>nat set interface <name> inside outside</code>
<code>nat set secure-plus on off</code>
<code>nat set sipp-pat <port></code>
<code>nat show [translations] [timeouts] [statistics]</code>

nat clear-err-stats

Mode

Enable

Format

```
nat clear-err-stats out-of-globals| port-mode
```

Description

The **nat clear-err-stats** command allows you to clear specific NAT error statistics such as out-of-globals messages in the case of dynamic bindings and port misconfiguration.

Parameter	Value	Meaning
clear-err-stats	out-of-globals	Clears error statistics during dynamic binding in the case where there are no more global IP addresses in the global address pool.
	port-mode	Clears error statistics that occur because of port misconfigurations. Such cases are where the port is set to either destination-based forwarding or host-flow based forwarding.

Restrictions

None

Example

To clear all out-of-global error statistics:

```
rs(config)# nat clear-err-stats out-of-globals
```

nat create dynamic

Mode

Configure

Format

```
nat create dynamic local-acl-pool <local-acl> global-pool <ip-addr/ip-addr-range/ip-addr-list>
[matches-interface <interface>] [enable-ip-overload]
```

Description

The **nat create dynamic** command lets you specify the local-acl pool and global IP address pool that are to be used for dynamic address binding. With dynamic address translation, IP address bindings last only until the data flow ages out or the dynamic binding is manually deleted. Global IP addresses defined for dynamic translation are reassigned whenever they become free. The local address pool for dynamic bindings are defined via an ACL profile, while the global address pool must be specified as a single IP address, an address range, an IP address and mask, or an IP list. You can also specify multiple global pools for the same local-acl pool, if you have more than one connection to the Internet on different interfaces.

Parameter	Value	Meaning
local-acl-pool	<local-acl>	The ACL that corresponds to the local IP address pool. The ACL may contain either permit or deny keywords. Note that only the source IP address information in the ACL is used; other ACL parameters are ignored. Used in the case of address translation from an inside private to an outside public network.
global-pool	<ip-addr/ip-addr-range/ip-addr-list>	The global address pool, defined in one of the following ways: • A single IP address in the form a.b.c.d • An IP address range in the form 10.10.1.1-10.10.1.50 • IP address and mask in the form 1.2.0.0/255.255.0.0 or 1.2.3.0/16 • A list of IP addresses, separated by spaces and enclosed in quotation marks. Used in the case of address translation from an inside private to an outside public network.
 Note Do not specify more than 64K global addresses.		

Parameter	Value	Meaning
matches-interface	<interface>	Specifies the interface to use for multiple global pools. Used in the case of address translation from an inside private to an outside public network.
enable-ip-overload		Enables Port Address Translation (PAT) if no global addresses are available from the pool. This allows many local addresses to be bound to a single global address using port numbers 1024 through 4999 (port numbers are not configurable). With PAT, multiple IP addresses can map to a single IP address with multiple numbers. Used in the case of address translation from an inside private to an outside public network.
 Note Protocols like ICMP do not work with the enable-ip-overload option. Thus, the ping command will not work if this option is used.		

Restrictions

None.

Examples

To configure address pools for dynamic address bindings, first configure the ACL that corresponds to the local IP address pool. In the following example, the ACL 'lcl' corresponds to IP addresses from 10.1.1.1 to 10.1.1.254:

```
rs(config)# acl lcl permit ip 10.1.1.0/24
```

Then, specify this ACL for the local IP address pool for dynamic address bindings with global addresses 136.1.1.1 to 136.1.1.254:

```
rs(config)# nat create dynamic local-acl-pool lcl global-pool 136.1.1.0/24
```

The following examples show the use of Port Address Translation, where the global pool consists of only two specified IP addresses. In the following example, the ACL 'lcl' corresponds to IP addresses from 10.1.1.1 to 10.1.1.254:

```
rs(config)# acl lcl permit ip 10.1.1.0/24
```

Then, specify this ACL for the local IP address pool for dynamic address bindings with global addresses 136.1.1.1 and 136.1.1.2 with Port Address Translation enabled:

```
rs(config)# nat create dynamic local-acl-pool lcl global-pool 136.1.1.1-136.1.1.2
enable-ip-overload
```

Port numbers 1024 through 4999 can be used for global addresses 136.1.1.1 and 136.1.1.2, so you can have a maximum of about 4000 bindings per global address.

nat create static

Mode

Configure

Format

```
nat create static protocol ip|tcp|udp local-ip <local-ip-addr/address range> global-ip
<global-ip-addr/address range> [local-port <tcp/udp-local-port> | any] [global-port
<tcp/udp-global-port> | any]
```

Description

The **nat create static** command lets you define fixed address translation from the local network to the global network. The one-to-one binding of the local to the global address does not expire until this command is negated. If the protocol used is TCP or UDP, you can also specify port address translation (PAT).

Parameter	Value	Meaning
protocol	ip tcp udp	Specifies either only IP address translation, IP and TCP port address translation, or IP and UDP port address translation.
local-ip	<local-ip-addr/address range>	Either a single IP address, in the form a.b.c.d, or an address range, in the form 10.10.1.1-10.10.1.50.
global-ip	<global-ip-addr/address range>	Either a single IP address, in the form a.b.c.d, or an address range, in the form 10.10.1.1-10.10.1.50.
local-port	<tcp/udp-local-port> any	The local TCP or UDP port number. Specify a number between 1-65535, or any for no port translation. This parameter is only valid if you specified tcp or udp .
 Note The number of IP addresses in the local range should be equal to the number of IP addresses in the global range.		
global-port	<tcp/udp-global-port> any	The global TCP or UDP port number. Specify a number between 1-65535, or any for no port translation. This parameter is only valid if you specified tcp or udp .

Restrictions

None.

Examples

To configure a static binding of a local and a global IP address:

```
rs(config)# nat create static protocol ip local-ip 10.1.1.13 global-ip 136.1.1.13
```

To configure a static binding of local and global IP address ranges:

```
rs(config)# nat create static protocol ip local-ip 10.1.1.1-10.1.1.50 global-ip  
136.1.1.1-136.1.1.50
```

To configure a static binding of local and global IP and UDP port addresses:

```
rs(config)# nat create static local-ip 10.1.1.13 global-ip 136.1.1.13 local-port 18  
global-port 36 protocol udp
```


nat flush-dynamic-binding

Mode

Enable

Format

```
nat flush-dynamic-binding all| pool-specified [local-acl-pool <local-acl>]  
[global-pool <ip-addr/ip-addr-range/ ip-addr-list>]| type-specified| owner-specified  
[dns| ftp-control| ftp-data]
```

Description

The **nat flush-dynamic-binding** command deletes dynamic address bindings. You can delete the dynamic address bindings for specific address pools or delete all dynamic bindings.

Parameter	Value	Meaning
all		Deletes all NAT dynamic bindings.
pool-specified		Deletes NAT dynamic bindings based on local and global acl pools:
local-acl-pool	<local-acl>	The ACL that corresponds to the local IP address pool.
global-pool	<ip-addr/ip-addr-range>	The global address pool, defined in one of the following ways: • A single IP address in the form a.b.c.d • An IP address range in the form 10.10.1.1-10.10.1.50 • IP address and mask in the form 1.2.0.0/255.255.0.0 or 1.2.3.0/16
type-specified		Deletes NAT dynamic bindings based on the type of dynamic binding.
owner-specified		Deletes NAT dynamic bindings based on the type of application utilizing the bindings:
	dns	Deletes NAT dynamic bindings created by DNS (domain name server).
	ftp-control	Deletes NAT dynamic bindings created by FTP control connection.
	ftp-data	Deletes NAT dynamic bindings created by FTP data connection.

Restrictions

None.

Examples

To delete dynamic address bindings for the local address pool that corresponds to the ACL 'lcl' and the global address pool that corresponds to 136.1.1.1-136.1.1.254:

```
rs# nat flush-dynamic-binding pool-specified local-acl-pool lcl global-pool  
136.1.1.0/24
```

To delete all dynamic address bindings:

```
rs# nat flush-dynamic-binding all
```

nat set dns-session-timeout

Mode

Configure

Format

```
nat set dns-session-timeout <num>
```

Description

The **nat set dns-session-timeout** command sets the timeout for DNS application-specific sessions. The default DNS session timeout is **30** minutes.

Parameter	Value	Meaning
dns-session-timeout	<num>	The timeout for the DNS session, in minutes. Specify a value between 3-2880. Default is 30 minutes.

Restrictions

None.

Example

To set the DNS session timeout to 60 minutes:

```
rs(config)# nat set dns-session-timeout 60
```

nat set dns-translation-state

Mode

Configure

Format

```
nat set dns-translation-state enable
```

Description

The **nat set dns-translation state** command enables NAT DNS translation. NAT DNS translation is disabled by default.

Parameter	Value	Meaning
enable		Enables NAT DNS translation.

Restrictions

None.

nat set dynamic-binding-timeout

Mode

Configure

Format

```
nat set dynamic-binding-timeout <minutes>|disable
```

Description

Dynamic address bindings time out after a period of non-use. The **nat set dynamic-binding-timeout** command lets you set the timeout for dynamic address bindings. The default is 1440 minutes (24 hours).

Parameter	Value	Meaning
dynamic-binding-timeout	<minutes>	The number of minutes before an dynamic address binding times out. Specify a value between 3-2880.
	disable	Disables timeout of dynamic address bindings.

Restrictions

None

Example

To set the timeout for dynamic address bindings to 3 minutes:

```
rs(config)# nat set dynamic-binding-timeout 3
```

To disable timeout of dynamic address bindings:

```
rs(config)# nat set dynamic-binding-timeout disable
```

nat set ftp-control-port

Mode

Configure

Format

```
nat set ftp-control-port <port number>
```

Description

File Transfer Protocol (FTP) packets require special handling with NAT, because IP address information is contained within the FTP packet data. You can use the nat **set ftp-control-port** command to specify the port number that is used for FTP control.

The default port for FTP control is port **21**.

Parameter	Value	Meaning
ftp-control-port	<port number>	Specifies the port number used for FTP control. Specify a value between 1 and 65535.

Restrictions

None.

Example

To set the FTP control port to 100:

```
rs(config)# nat set ftp-control-port 100
```

nat set ftp-session-timeout

Mode

Configure

Format

```
nat set ftp-session-timeout <minutes>
```

Description

The **nat set ftp-session-timeout** command sets the timeout for the FTP session.

The default FTP session timeout is **30** minutes.

Parameter	Value	Meaning
ftp-session-timeout	<minutes>	The timeout for the FTP session. Specify a value between 3-2880.

Restrictions

None.

Example

To set the FTP session timeout to 60 minutes:

```
rs(config)# nat set ftp-session-timeout 60
```

nat set interface

Mode

Configure

Format

```
nat set interface <name> inside|outside
```

Description

The **nat set interface** command allows you to define an interface as inside or outside. When NAT is enabled using the **nat create static** or **nat create dynamic** command, address translation is applied only to packets that arrive on these interfaces.

Parameter	Value	Meaning
interface	<name>	Is the name of the interface to which address translation will apply.
	inside outside	Specifies the interface(s) as inside or outside.

Restrictions

None.

Examples

To create the interface '10-net' and define it as an inside interface for NAT:

```
rs(config)# interface create ip 10-net address-netmask 10.1.1.1/24 port et.2.1
rs(config)# nat set interface 10-net inside
```

To create the interface '192-net' and define it as an outside interface for NAT:

```
rs(config)# interface create ip 192-net address-netmask 192.50.20.1/24 port et.2.2
rs(config)# nat set interface 192-net outside
```


nat set secure-plus

Mode

Configure

Format

```
nat set secure-plus on|off
```

Description

The **nat set secure-plus** command forces all flows from the inside local network to the outside global network to go through network address translation. Any possibility of bypassing the NAT process is eliminated.

Parameter	Value	Meaning
secure-plus	on off	Specify on to enable secure-plus feature. Specify off to disable secure-plus feature.

Restrictions

None.

nat set sipp-pat

Mode

Configure

Format

```
nat set sipp-pat <port>
```

Description

The **nat set sipp-pat** command allows you to assign a single port to handle all NAT in the case where the RS is connected to another vender equipment which may not be supported by the RS. This is done by enabling Simple Internet Protocol Plus (SIPP) and Port Address Translation (PAT) on the port. This provides inter-operability between the RS and unsupported hardware.

Parameter	Value	Meaning
sipp-pat	<port>	Specifies a single port number.

Restrictions

None.

Example

To set port 'et.2.1' to handle network address translation for unsupported hardware:

```
rs(config)# nat set sipp-pat et.2.1
```

nat show

Mode

Enable

Format

```
nat show [translations <type>] [timeouts] [statistics]
```

Description

The **nat show** command allows you to display NAT address translations, timeouts, and statistics.

Parameter	Value	Meaning
translations	<type>	Displays NAT translations. Specify one of the following keywords:
all		Shows all translations.
type	static dynamic overl oaded-dynamic	Shows static, dynamic, or IP overloaded dynamic translations.
owner	dns ftp-control ftp- data	Shows dynamic translation created by dns, overloaded dynamic ftp control connection translations, or overloaded dynamic ftp data connection translations.
local-filter-in	<local-ip-addr>	Shows translations of the specified local IP address. The IP address must be in the form a.b.c.d.
global-filter-in	<global-ip-addr>	Shows translations of the specified global IP address. The IP address must be in the form a.b.c.d.
timeouts		Displays the current set of timeouts.
statistics		Displays NAT statistics.
verbose		Displays NAT translations in greater detail.

Restrictions

None.

Examples

To display active NAT translations:

```
rs# nat show translations all
```

Proto	Local/Inside	Global/Outside IP	Type	No. of flows
-----	-----	-----	-----	-----
TCP	15.15.15.15:1896	100.1.1.1:1026	Dyn. ovr.	2
TCP	15.15.15.15:1897	100.1.1.1:1028	Dyn. ovr.	0
TCP	15.15.15.15:1894	100.1.1.1:1024	Dyn. ovr.	2
TCP	15.15.15.15:1895	100.1.1.1:1025	Dyn. ovr.	2
TCP	15.15.15.15:1892	100.1.1.1:1027	Dyn. ovr.	0
IP	10.10.10.10:*	200.1.1.1:*	Dynamic	20
IP	4.4.4.4:*	202.1.1.1:*	Static	789

If there are many active NAT translations, you can filter the display by specifying **local-filter-in**, **global-filter-in**, or **type** parameters for the **nat show translations** command.

To display NAT timeouts:

```
rs# nat show timeouts
```

All values in minutes			
Flow	FTP Sess.	DNS Sess.	Dyn. Sess.
-----	-----	-----	-----
2	30	30	1440

To display NAT statistics:

```
NAT current status
-----
active

NAT secure-plus status
-----
inactive

Interface Information
-----
No. of Interfaces: 1
Interface: 20net, configured as nat: outside

STATIC Binding Information
-----
No. of Static Bindings: 1

DYNAMIC Binding Information
-----
No. of Dynamic Bindings: None

Local Acl pool  Max. globals  Globals used  Max. ports  Ports Used  Out
of globa
ls/ports
-----
local           1           0           3975         0           0
```


44 NEGATE COMMAND

negate

Mode

Configure

Format

```
negate <cmd-number>|all active-config|scratchpad
```

Description

The **negate** command allows you to negate one or more commands by specifying the command number of the commands you want to negate. The command number for each command can be found using the Configure mode **show** command. You can negate specific commands or all the commands from the active running system or non-committed commands from the scratchpad. By default, if you do not specify **active-config** or **scratchpad**, the command to negate is assumed to be in the **active-config**.

Parameter	Value	Meaning
	<cmd-number>	The number of the command(s) you want to negate. Use the show command to display the command numbers.
all		Negate all the commands
scratchpad		Negate the specified non-committed command from the scratchpad.
active-config		Negate the specified command from the active running system.

Restrictions

The specified command number must represent a command that exists.

Examples

To negate command 23 from the active configuration:

```
rs# negate 23 active-config
```

To negate commands 3, 5, 6 and 7 from the scratchpad:

```
rs# negate 3,5-7 scratchpad
```

To negate all of the commands from the active configuration:

```
rs# negate all active-config
```


45 NO COMMAND

no

Mode

Configure

Format

`no <command-to-negate>`

Description

The **no** command allows you to negate a previously executed command. Following the keyword **no**, one can specify the command to negate in its entirety or use the wildcard character (*) to negate a group of commands. In addition to the **no** command, one can also use the **negate** command to negate a group of commands using the command number.

Parameter	Value	Meaning
no	<command>	The CLI command you want to negate. You do not have to enter the entire command. You can use the wildcard character, *, to negate matching commands. For example, if you specify no acl 100 * then all commands starting with the words acl 100 will be negated.

Restrictions

The command to negate must already be in the active configuration. You cannot negate a command that hasn't been entered.

Examples

To negate the specified **arp add** command, enter the following. By negating this command, the system removes the ARP entry for *nfs2* from the ARP table.

```
rs# no arp add nfs2 macaddr 080020:13a09f exit-port et.3.1
```

To negate all commands starting with the word “acl”:

```
rs# no acl *
```

46 NTP COMMANDS

The **ntp** commands configure and display the characteristics of the NTP (Network Time Protocol) client.

46.1 COMMAND SUMMARY

The following table lists the ntp commands. The sections following the table describe the command syntax.

<code>ntp set server <host> [interval <minutes>] [source <ipaddr>] [version <num>]</code>
<code>ntp show all</code>
<code>ntp synchronize server <host></code>

ntp set server

Mode

Configure

Format

```
ntp set server <host> [interval <minutes>] [source <ipaddr>] [version <num>]
```

Description

The **ntp set server** command instructs the RS' NTP client to periodically synchronize its clock. By default, the RS specifies an NTPv3 client that sends a synchronization packet to the server every 60 minutes. This means the RS will attempt to set its own clock against the server once every hour. The synchronization interval as well as the NTP version number can be changed.

Note To ensure that NTP has the correct time, you need to specify the time zone, as well. You can set the time zone by using the **system set timezone** command. When specifying daylight saving time, you'll need to use the **system set daylight-saving** command.

Parameter	Value	Meaning
server	<host>	Specifies the hostname or the IP address of the NTP server.
interval	<minutes>	Specifies how often (in minutes) the RS should synchronize with the server. The default synchronization interval is 60 minutes. Valid interval is between 1 minute to 10080 minutes (7 days).
source	<ipaddr>	Specifies the source IP address to be used by the RS for sending the NTP packet. The IP address must belong to one of the interfaces on the RS.
version	<num>	Specifies the NTP version number of the packet. The default version number is 3 (NTPv3). Valid value is 1-3.

Restrictions

None.

Examples

To send NTP packets to the NTP server 10.13.1.1 with default parameters:

```
rs(config)# ntp set server 10.13.1.1
```

To synchronize with a NTP server every 15 minutes with a specific source IP address:

```
rs(config)# ntp set server 10.13.1.1 interval 15 source 10.15.3.3
```

ntp show all

Mode

Enable

Format

ntp show all

Description

The **ntp show all** command displays various NTP information about the RS, for example, the last time a successful synchronization was made, synchronization interval, NTP version number, etc.

Restrictions

None.

Example

```
rs# ntp show all
NTP status:
Synchronization interval: 60 mins
Version: NTPv3
Last successful contact: Thu Jan 23 23:08:15 1999
```

ntp synchronize server

Mode

Enable

Format

ntp synchronize server <host>

Description

The **ntp synchronize server** command forces the RS to immediately synchronize its clock with the NTP server. Unlike the Configuration mode **ntp set server** command, this Enable mode command does not send periodic synchronization packets to the server. Instead, each time this command is executed, the RS synchronizes itself with the server. To have the RS synchronizes itself periodically, use the **ntp set server** command.

Parameter	Value	Meaning
server	<host>	Specifies the hostname or the IP address of the NTP server.

Restrictions

None.

Examples

To synchronize the RS against the NTP server 10.13.1.1:

```
rs(config)# ntp synchronize server 10.13.1.1
%NTP-I-TIMESYNC, Time synchronized to Thu Jan 23 23:11:28 1999
```


47 OSPF COMMANDS

The **ospf** commands let you display and set parameters for the Open Shortest Path First (OSPF) routing protocol.

47.1 COMMAND SUMMARY

The following table lists the ospf commands. The sections following the table describe the command syntax.

ospf add interface <interfacename-or-IPaddr> to-area <area-id> backbone [type broadcast non-broadcast point-to-multipoint]
ospf add label-switched-path <pathname> to-area <ipaddr> [backbone]
ospf add nbma-neighbor <hostname-or-IPaddr> to-interface <hostname-or-IPaddr> [eligible]
ospf add network summary-range <IPaddr/mask> to-area <area-addr> [restrict] [host-net]
ospf add nssa-network <IPaddr/mask> to-area <area-id> [restrict] [host-net]
ospf add pmp-neighbor <IPaddr> to-interface <hostname-or-IPaddr>
ospf add stub-host <IPaddr> to-area <area-id> backbone cost <num>
ospf add summary-filters to-area <area-id> backbone [filter <number-or-string>][network <IPaddr/mask> all default] exact refines between <number> host-net
ospf add virtual-link <number-or-string> neighbor <IPaddr> transit-area <area-id>
ospf clear database
ospf clear statistics [interface <IPaddr>] [neighbour <IPaddr>]
ospf create area <area-id> [backbone]
ospf create-monitor destination <hostname-or-IPaddr> auth-key <string>
ospf monitor interfaces [destination <hostname-or-IPaddr>][auth-key <string>]
ospf monitor neighbors [destination <hostname-or-IPaddr>][auth-key <string>]
ospf monitor next-hop-list [destination <hostname-or-IPaddr>][auth-key <string>]
ospf monitor routes [type all asbrs-in-area area-border-routers asbrs-other-areas networks-in-area networks-other-area as-routes] [destination <hostname-or-IPaddr>] [auth-key <string>]
ospf monitor version [destination <hostname-or-IPaddr>][auth-key <string>]

ospf set advertise-subnet on off
ospf set area <area-id> backbone [stub] [stub-cost <num>] [authentication-method none simple md5] [no-summary][retransmit interval <num>][transit-delay <num>][priority <num>]hello-interval <num>][router-dead-interval <num>][poll-interval<num>][key-chain <num>][advertise-subnet on off][nssa][nssa-cost][nssa-type]
ospf set ase-defaults {[preference <num>] [cost <num>] [type <num>]} [inherit-metric]} [tag <num>][as]
ospf set authentication-method none simple key-chain <string> md5 key-chain <string>
ospf set export-interval <num>
ospf set export-limit <num>
ospf set hello-interval <num>
ospf set igp-shortcuts on off
ospf set interface <interfacename-or-IPaddr> all [state disable enable] [cost <num>] [retransmit-interval <num>] [transit-delay <num>] [priority <num>] [hello-interval <num>] [router-dead-interval <num>] [poll-interval <num>][key-chain <num-or-string>] [authentication-method none simple md5] [advertise subnet on off][passive]
ospf set monitor-auth-method none simple md5
ospf set opaque-capability on off
ospf set poll-interval <number>
ospf set preference <num>
ospf set priority <number>
ospf set ref-bwtdth
ospf set retransmit-interval <number>
ospf set router-dead-interval <number>
ospf set spf-holdtime <num>
ospf set traffic-engineering on off
ospf set transit-delay <number>
ospf set virtual-link <number-or-string> [state disable enable] [cost <num>] [retransmit-interval <num>] [transit-delay <num>] [priority <num>] [hello-interval <num>] [router-dead-interval <num>] [poll-interval <num>] [key-chain <string>] [authentication-method none simple md5]
ospf show adjacency-down-reason
ospf show all
ospf show areas <area-id> backbone all
ospf show as-external-lsdb
ospf show border-routes
ospf show database asbr-summary <ip-addr> external database-summary network nssa-external router summary link-id <ip-addr> adv-router

ospf show export-policies
ospf show globals
ospf show import-policies
ospf show interfaces [detail]
ospf show lsa [area-id <area-id>][type router-links network-links summary-networks summary-asbr as-external] [ls-id <IPaddr>][adv-rtr <routerID>]
ospf show neighbor
ospf show statistics [interface <IPaddr>][neighbour <IPaddr>]
ospf show summary-asb
ospf show ted
ospf show timers
ospf show virtual-links
ospf start stop

ospf add interface

Mode

Configure

Format

```
ospf add interface <interfacename-or-IPaddr> to-area <area-id>|backbone  
[type broadcast|non-broadcast|point-to-multipoint]
```

Description

Associates an interface with an OSPF area.

Parameter	Value	Meaning
interface	<interfacename-or-IPaddr>	An interface name or an IP address.
to-area	<area-id>	OSPF area with which this interface is to be associated.
	backbone	Backbone area with which this interface is to be associated.
type	broadcast	Specifies the interface is broadcast.
	non-broadcast	Specifies the interface is non-broadcast.
	point-to-multipoint	Specifies the interface is point-to-multipoint.

Restrictions

None.

ospf add label-switched-path

Mode

Configure

Format

ospf add label-switched-path <pathname> to-area <ipaddr> [backbone]

Description

Associates a label switched path (LSP) with an OSPF area.

Parameter	Value	Meaning
label-switched-path	<pathname>	Name of the label switched path.
to-area	<ipaddr>	OSPF area with which this LSP is to be associated.
	backbone	Backbone area with which this interface is to be associated.

Restrictions

None.

ospf add nbma-neighbor

Mode

Configure

Format

ospf add nbma-neighbor <hostname-or-IPaddr> to-interface <interfacename-or-IPaddr> [eligible]

Description

Specifies a neighboring router that is reachable on a Non-Broadcast Multi-Access (NBMA) network.

Parameter	Value	Meaning
nbma-neighbor	<hostname-or-IPaddr>	Identifies the neighboring router on the NBMA network.
to-interface	<interfacename-or-IPaddr>	Adds the neighbor to the specified OSPF interface.
eligible		Specifies whether an OSPF NBMA neighbor is eligible to be a designated router.

Restrictions

None.

ospf add network|summary-range

Mode

Configure



Note Because the **OSPF add network** command is misinterpreted with commands having similar syntax from other vendors, this command will eventually be dropped from the RS's host of CLI commands. The new command is **ospf add summary-range**. At this time, however, both are acceptable CLI commands, hence both are dealt with in this section.

Format

```
ospf add network | summary-range <IPaddr/mask> to-area <area-id> [restrict]
[host-net]
```

Description

Configures summary-ranges on Area Border Routers (ABRs). This allows you to reduce the amount of routing information propagated between areas.

On the RS, summary-ranges are created using the `ospf add summary-range` command – the networks specified using this command describe the scope of an area. Intra-area Link State Advertisements (LSAs) that fall within the specified ranges are not advertised into other areas as inter-area routes. Instead, the specified ranges/networks are advertised as summary network LSAs. If you specify the `restrict` option, the summary network LSAs are not advertised. Each intra-area LSA that does not fall into any range is advertised as an OSPF Type-3 or 4 LSA.

Parameter	Value	Meaning
summary-range	<IPaddr/mask>	IP Address and network mask value representing the summary-range. Example: 16.122.0.0/255.255.0.0 or 16.122.0.0/16.
to-area	<area-id>	OSPF Area with which this summary-range is to be associated.
restrict		If the restrict option is specified for a network/summary-range, then that network is not advertised in summary network LSAs.
host-net		Specifies that the network is an OSPF Host Network.

Restrictions

None.

Example

In the following example, two summary ranges are created:

```
ospf add summary-range 207.135.16.0/24 to-area 207.135.0.0
ospf add summary-range 207.135.17.0/24 to-area 207.135.0.0 restrict
```

Intra-area Link State Advertisements (LSAs) that fall within the range 207.135.16.0/24 are not advertised into other areas as inter-area routes. Instead, the specified range 207.135.16.0/24 is advertised as summary network LSA.

Because the summary range 207.135.17.0/24 has the restrict option associated with it, intra-area link state advertisements (LSAs) that fall within it are not advertised as summary network LSA. Using this mechanism, one can have “hidden networks” within an area, which are not advertised to other areas.

ospf add nssa-network

Mode

Configure

Format

```
ospf add nssa-network <IPaddr/mask> to-area <area-id> [restrict] [host-net]
```

Description

Specifies a network to be included in a Not-So-Stubby Area (NSSA). NSSAs originate and advertise Type 7 LSAs.

Parameter	Value	Meaning
nssa-network	<IPaddr/mask>	IP Address and network mask value representing the network. Example: 16.122.0.0/255.255.0.0 or 16.122.0.0/16.
to-area	<area-id>	NSSA area with which this network is to be associated.
restrict		If the restrict option is specified for a network, then that network is not advertised in Type 7 LSAs.
host-net		Specifies that the network is an OSPF host network.

Restrictions

None

ospf add pmp-neighbor

Mode

Configure

Format

```
ospf add pmp-neighbor <IPaddr> to-interface <hostname-or-IPaddr>
```

Description

The **ospf add pmp-neighbor** configures a Point-to-Multipoint neighbor router on an interface. A Point-to-Multipoint connectivity is used when the network does not provide full connectivity to all routers in the network. As in the case of NBMA (non-broadcast multiple access) networks, a list of neighboring routers reachable over a PMP network should be configured so that the router can discover its neighbors.

Parameter	Value	Meaning
pmp-neighbor	<IPaddr>	Specifies the point-to-multipoint neighbor.
to-interface	<hostname-or-IPaddr>	Adds the neighbor to the specified OSPF interface.

Restrictions

None.

Example

To add a point-to-multipoint neighbor with IP address 134.141.179.141 to the OSPF interface 134.141.179.152:

```
rs(config)# ospf add pmp-neighbor 134.141.179.141 to-interface 134.141.179.152
```

ospf add stub-host

Mode

Configure

Format

```
ospf add stub-host <IPaddr> to-area <area-id>|backbone cost <num>
```

Description

Specifies an interface that is directly attached to the router.

Parameter	Value	Meaning
stub-host	<IPaddr>	The IP address of the interface.
to-area	<area-id>	OSPF area to which you are adding a stub host
	backbone	Backbone area to which you are adding a stub host
cost	<num>	The cost that should be advertised for this directly attached stub host. Specify a number from 0 – 65535.

Restrictions

None.

ospf add summary-filters

Mode

Configure

Format

```
ospf add summary-filters to-area <area-id>|backbone [filter <number-or-string>][network <IPaddr/mask>|all|default] exact|refines|between <number> |host-net
```

Description

Specifies which summary LSAs to filter from the stub area. Summary LSAs are compared against the summary-filters list. If a match is found, the summary LSA is not injected into the stub area. For normal operations, summary-filters should only be used in stub areas that have a default route.

Parameter	Value	Meaning
to-area	<area-id>	OSPF area to which you are applying the summary filter.
	backbone	OSPF area to which you are applying the summary filter.
filter	<number-or-string>	Specifies the filter to be applied.
network	<IPaddr/mask>	Specifies the network to be filtered.
	all	Specifying all is equivalent to the network specification of 0.0.0.0/0.0.0.0.
	default	Specify default for the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.
exact		Specifies that the mask of the destination must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		Specifies that the mask of the destination must be more specific (i.e. longer) than the supplied mask. This is used to match subnets and/or hosts of a network, but not the network.
between	<number>	Specifies that the mask of the destination must be as long as or longer than the lower limit and as long as or shorter than the upper limit.
host-net		Use this option if the specified network is a host. To match, the address must exactly match the specified host and the network mask must be a host mask (i.e. all ones).

Restrictions

None

ospf add virtual-link

Mode

Configure

Format

ospf add virtual-link <number-or-string> neighbor <IPaddr> transit-area <area-id>

Description

Creates an OSPF Virtual Link.

Parameter	Value	Meaning
virtual-link	<number-or-string>	A number or character string identifying the virtual link.
neighbor	<IPaddr>	The IP address of an OSPF virtual link neighbor.
transit-area	<area-id>	The Area ID of the transit area.

Restrictions

None.

ospf clear database

Mode

Enable

Format

```
ospf clear database
```

Description

Clears the OSPF database.

Restrictions

None.

ospf clear statistics

Mode

Enable

Format

```
ospf clear statistics [interface <IPaddr>] [neighbour <IPaddr>]
```

Description

Clears OSPF statistics.

Parameter	Value	Meaning
interface	<IPaddr>	The IP address of the interface for which statistics will be cleared.
neighbour	<IPaddr>	The IP address of the neighbor for which statistics will be cleared.

Restrictions

None.

ospf create area

Mode

Configure

Format

```
ospf create area <area-id> | backbone
```

Description

Creates an OSPF area.

Parameter	Value	Meaning
area	<area-id>	The area ID. Normally, area IDs are formatted like IP addresses: <num>.<num>.<num>.<num>.
	backbone	Specifies that the area you are adding is the backbone area.

Restrictions

None.

ospf create-monitor

Mode

Enable

Format

ospf create-monitor destination *<hostname-or-IPaddr>* auth-key *<string>*

Description

Create an OSPF monitor destination.

Parameter	Value	Meaning
destination	<i><hostname-or-IPaddr></i>	Specifies the destination whose OSPF activity is to be monitored.
auth-key	<i><string></i>	Specifies an authorization key for the OSPF destination.

Restrictions

None.

ospf monitor interfaces

Mode

Enable

Format

```
ospf monitor interfaces [destination <IPaddr>] [auth-key <string>]
```

Description

Shows information about all interfaces configured for OSPF.

Parameter	Value	Meaning
destination	<IPaddr>	Specifies the remote Riverstone Networks RS Switch Router to be monitored. This option is required to display the OSPF tables of a remote RS. Default is the router on which the command is executed.
auth-key	<string>	Specifies the authorization key for the OSPF destination. This option is not needed if the OSPF destination does not require a key or if an authorization was specified using the ospf monitor create-destination command.

Restrictions

None.

Example

Following is an example of the **ospf monitor interfaces** command. Information reported includes the area ID, interface IP address, interface type, interface state, cost, priority, and IP addresses of the Designated Router and Backup Designated Router for the network.

```
rs# ospf monitor interfaces
>sent to 127.0.0.1

Source <<127.0.0.1      >>

Area: 0.0.0.0
IP Address      Type  State      Cost Pri DR          BDR
-----
172.23.1.5      Bcast BackupDR 2    2   172.23.1.6    172.23.1.5
10.12.1.2       Bcast BackupDR 1    2   10.12.1.1     10.12.1.2
172.23.1.21     Bcast BackupDR 1    2   172.23.1.22   172.23.1.21
done
```

ospf monitor neighbors

Mode

Enable

Format

```
ospf monitor neighbors [destination <hostname-or-IPaddr>] [auth-key <string>]
```

Description

Shows information about all OSPF routing neighbors.

Parameter	Value	Meaning
destination	<hostname-or-IPaddr>	Specifies the remote Riverstone Networks RS Switch Router to be monitored. This option is required to display the OSPF tables of a remote RS. Default is the router on which the command is executed.
auth-key	<string>	Specifies the authorization key for the OSPF destination. This option is not needed if the OSPF destination does not require a key or if an authorization was specified using the <code>ospf monitor create-destination</code> command.

Restrictions

None.

Example

Following is an example of the **ospf monitor neighbors** command:

```
rs# ospf monitor neighbors
Interface: 190.135.89.227 Area: 190.135.89
Router Id      Nbr IP Addr    State    Mode    Options    Pri
-----
1.1.1.1        190.135.89.228 Full     MS      E        1
```

Information reported includes the following for each neighbor:

- the router's interface on which the neighbor is located
- the area ID
- the router ID
- the IP address of the neighbor's interface that is attached to the network
- OSPF functional state
- mode; refers to the master/slave relationship negotiated with the neighbor
- router priority of the neighbor

ospf monitor next-hop-list

Mode

Enable

Format

```
ospf monitor next-hop-list [destination <hostname-or-IPaddr>]  
[auth-key <string>]
```

Description

Shows information about all valid next hops mostly derived from the SPF calculation.

Parameter	Value	Meaning
destination	<hostname-or-IPaddr>	Specifies the remote Riverstone Networks RS Switch Router to be monitored. This option is required to display the OSPF tables of a remote RS. Default is the router on which the command is executed.
auth-key	<string>	Specifies the authorization key for the OSPF destination. This option is not needed if the OSPF destination does not require a key or if an authorization was specified using the ospf monitor create-destination command.

Restrictions

None.

Example

Following is an example of the **ospf monitor next-hop-list** command:

```
rs# ospf monitor next-hop-list
```

Next hops:

Address	Type	Refcount	Interface
10.12.1.1	Neighbor	6	10.12.1.2 to-c4500
10.12.1.2	Direct	1	10.12.1.2 to-c4500
150.1.0.1	Direct	1	150.1.0.1 to-aval-eth5
172.23.1.5	Direct	3	172.23.1.5 to-RS6
172.23.1.6	Neighbor	5	172.23.1.5 to-RS6
172.23.1.21	Direct	3	172.23.1.21 to-RS1
172.23.1.22	Neighbor	19	172.23.1.21 to-RS1
172.23.1.25	Direct	3	172.23.1.25 lo
222.1.1.1	Direct	1	222.1.1.1 to-linux1

This table lists the following information about each next hop:

- IP address
- type of link
- ref count
- address of the interface
- name of the interface

ospf monitor routes

Mode

Enable

Format

```
ospf monitor routes [type all|asbrs-in-area|area-border-routers|  
asbrs-other-areas|networks-in-area|networks-other-area |as-routes]  
[destination <hostname-or-IPaddr>] [auth-key <string>]
```

Description

Displays the OSPF routing table. This table reports the AS border routes, area border routes, summary AS border routes, networks, summary networks and AS external networks currently managed via OSPF.

Parameter	Value	Meaning
type		Specifies the type of routes to display.
	all	Shows all OSPF routes.
	asbrs-in-area	Shows routes to AS boundary routers in this area.
	area-border-routers	Shows routes to area border routers for this area.
	asbrs-other-areas	Shows summary routes to AS boundary routers in other areas.
	networks-in-area	Shows routes to networks in this area.
	networks-other-areas	Shows routes to networks in other areas.
	as-routes	Shows AS routes to non-OSPF networks.
destination	<hostname-or-IPaddr>	Specifies the remote Riverstone Networks RS Switch Router to be monitored. This option is required to display the OSPF tables of a remote RS. Default is the router on which the command is executed.
auth-key	<string>	Specifies the authorization key for the OSPF destination. This option is not needed if the OSPF destination does not require a key or if an authorization was specified using the ospf monitor create-destination command.

Restrictions

None.

Example

Following is an example of the **ospf monitor routes** command:

rs# ospf monitor routes						
DTp	Destination ID	ML	Area	PthTp	Cost	Ty2 Cost NextHop(s)
rtr	1.1.1.1	32	190.135.89	intra	20	notdef 190.135.89.228
net	4.4.4.4	32	190.135.89	inter	32	notdef 190.135.89.228
rtr	6.6.6.6	32	190.135.89	intra	40	notdef 190.135.89.228
rtr	7.7.7.7	32	190.135.89	intra	infinite	notdef none
net	22.1	16	190.135.89	inter	40	notdef 190.135.89.228
net	33.33.33	24	190.135.89	intra	20	notdef 33.33.33.33
net	73.1.1.2	32	190.135.89	intra	3	notdef 73.1.1.2
net	99.9.9	24	190.135.89	inter	62	notdef 190.135.89.228
net	100.1.1	24	190.135.89	intra	20	notdef 100.1.1.1
net	125.1	16	190.135.89	inter	42	notdef 190.135.89.228
net	130.1	16	190.135.89	inter	42	notdef 190.135.89.228
net	131.1	16	190.135.89	inter	42	notdef 190.135.89.228
net	132.1	16	190.135.89	inter	42	notdef 190.135.89.228
net	133.1	16	190.135.89	inter	42	notdef 190.135.89.228
net	134.1	16	190.135.89	inter	62	notdef 190.135.89.228
net	190.135.89	26	190.135.89	intra	40	notdef 190.135.89.228
net	190.135.89.32	27	190.135.89	intra	20	notdef 190.135.89.33
net	190.135.89.224	28	190.135.89	intra	20	notdef 190.135.89.227
net	200.135.89	28	190.135.89	inter	22	notdef 190.135.89.228
net	201.135.89.128	26	190.135.89	inter	42	notdef 190.135.89.228

The information displayed includes the following:

- destination type
- destination ID, including the multicast length (**ML**)
- area
- path type and cost
- path type and cost for AS external routes (**Ty2** and **Cost**)
- next hop address

ospf monitor version

Mode

Enable

Format

```
ospf monitor version [destination <hostname-or-IPaddr>] [auth-key <string>]
```

Description

Shows information about all OSPF versions.

Parameter	Value	Meaning
destination	<hostname-or-IPaddr>	Specifies the remote Riverstone Networks RS Switch Router to be monitored. This option is required to display the OSPF tables of a remote RS. Default is the router on which the command is executed.
auth-key	<string>	Specifies the authorization key for the OSPF destination. This option is not needed if the OSPF destination does not require a key or if an authorization was specified using the ospf monitor create-destination command.

Restrictions

None.

Example

Following is an example of the **ospf monitor version** command:

```
rs# ospf monitor version

    gated
    pid 0x807d3508   started 2000-06-27 20:47:30

    system
```


ospf set advertise-subnet

Mode

Configure

Format

ospf set advertise-subnet on|off

Description

Specify whether the point-to-point interface should be advertised as a subnet.

Parameter	Value	Meaning
advertise-subnet	on	Specify on to advertise the point-to-point interface as a subnet.
	off	Specify off to stop advertising the point-to-point interface as a subnet. The default is off .

Restrictions

None.

ospf set area

Mode

Configure

Format

```
ospf set area <area-id>|backbone [stub] [stub-cost <num>] [authentication-method
none|simple|md5] [no-summary] [retransmit-interval <num>] [transit-delay <num>]
[priority <num>] [hello-interval <num>] [router-dead-interval <num>] [poll-interval
<num>] [key-chain <num-or-string>] [advertise-subnet on|off] [nssa] [nssa-cost]
[nssa-type]
```

Description

Sets the parameters for an OSPF area.

Parameter	Value	Meaning
area	<area-id>	The area ID.
	backbone	Specify backbone to set parameters for a backbone area.
stub		Makes this area a stub area.
stub-cost		Specifies the cost to be used to inject a default route into the area. Specify a number from 1 – 65535.
authentication-method		Specifies the authentication method used within the area.
	none	Does not use authentication.
	simple	Uses a simple string (password) of up to 8 characters in length for authentication. If you choose this authentication method, then you should also specify a key-chain identifier using the key-chain option.
	md5	Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters.
no-summary		Specifies that this is a fully stub area.
retransmit-interval	<num>	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. Specify a number equal to or greater than 1. The default is 5.
transit-delay	<num>	The estimated number of seconds required to transmit a link state update over this interface. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.

Parameter	Value	Meaning
priority	<num>	A number between 0 and 255 specifying the priority for becoming the designated router on this interface. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255. The default is 1.
hello-interval	<num>	The length of time, in seconds, between hello packets that the router sends on this interface. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.
router-dead-interval	<num>	The number of seconds a router does not receive Hello packets from its neighbor before it declares its neighbor is down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.
poll-interval	<num>	The interval at which OSPF packets are sent, before an adjacency is established with a neighbor. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.
key-chain	<num-or-string>	Identify the key-chain containing the authentication keys. Note that the key-chain must have been previously created with the ip-router authentication create key-chain command.
advertise-subnet	on	Specify on to advertise the point-to-point interface as a subnet. .
	off	Specify off to stop advertising the point-to-point interface as a subnet. The default is off .
nssa		Specify this keyword to establish the area as an NSSA area.
nssa-cost		Specify the cost used to inject a default route into the area
nssa-type		Routes exported from the GateD routing table into OSPF default to type 2 ASEs. This default may be explicitly changed here and overridden in export policy.

Restrictions

None.

ospf set ase-defaults

Mode

Configure

Format

```
ospf set ase-defaults [preference <num>][[cost <num>]][type  
<num>][[inherit-metric][tag <num>]][as]
```

Description

Sets the defaults used when importing OSPF ASE routes into the routing table and exporting routes from the routing table into OSPF ASEs.

Parameter	Value	Meaning
preference	<num>	Specifies the preference of OSPF ASE routes. Specify a number between 1 and 255.
cost	<num>	Specifies the cost used when exporting non-OSPF route into OSPF as an ASE. Specify a number from 0 – 65535.
type	<num>	Specifies the ASE type. Routes exported from the routing table into OSPF default to becoming type 1 ASEs. You can change the default using the type option. You also can override the type in OSPF export policies. Specify either 1 or 2.
	inherit-metric	Allows an OSPF ASE route to inherit the metric of the external route when no metric is specified on the export. A metric specified with the export command takes precedence. The cost specified in the default is used if you do not specify inherit-metric.
tag	<num>	OSPF ASE routes have a 32 bit tag field that is not used by the OSPF protocol, but may be used by an export policy to filter routes. When OSPF is interacting with an egg, the tag field may be used to propagate AS path information, in which case the 'as' option is specified and the tag is limited to 12 bits of information. If not specified, the tag is set to zero.
as		When OSPF is interacting with an egg, the tag field may be used to propagate AS path information, in which case the as option is specified and the tag is limited to 12 bits of information. If not specified, the tag is set to zero.

Restrictions

None.

Example

To specify the cost used when exporting non-OSP routes into OSPF as ASE routes:

```
rs(config)# ospf set ase-defaults cost 4
```

ospf set authentication-method

Mode

Configure

Format

```
ospf set authentication-method none|simple key-chain <string>|md5 key-chain <string>
```

Description

Specifies the authentication method used.

Parameter	Value	Meaning
authentication-method	none	Does not use authentication.
	simple	Uses a simple string (password) up to 8 characters in length for authentication. If you choose this authentication method, then you should also specify a key-chain identifier using the key-chain option.
	md5	Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters.
key-chain	<string>	Identify the key-chain containing the authentication keys. Note that the key-chain must have been previously created with the ip-router authentication create key-chain command.

Restrictions

None.

ospf set export-interval

Mode

Configure

Format

ospf set export-interval *<num>*

Description

Specifies the interval at which ASE LSAs will be generated and flooded into OSPF. The default is once per second.

Parameter	Value	Meaning
export-interval	<i><num></i>	The interval in seconds. Specify a number equal to or greater than 1. The default is 1.

Restrictions

None.

ospf set export-limit

Mode

Configure

Format

```
ospf set export-limit <num>
```

Description

Specifies how many ASEs will be generated and flooded in each batch.

Parameter	Value	Meaning
export-limit	<num>	The export limit. Specify a number equal to or greater than 1. The default is 100.

Restrictions

None.

ospf set hello-interval

Mode

Configure

Format

ospf set hello-interval *<num>*

Description

Sets the interval between the transmission of hello packets.

Parameter	Value	Meaning
hello-interval	<i><num></i>	The length of time, in seconds, between the transmission of hello packets. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.

Restrictions

None.

ospf set igp-shortcuts

Mode

Configure

Format

```
ospf set igp-shortcuts on|off
```

Description

The **ospf set igp-shortcuts** command allows you to enable or disable the use of label switched paths (LSPs) as IGP shortcuts.

Parameter	Value	Meaning
igp-shortcuts	on	Enables use of LSPs as IGP shortcuts.
	off	Disables use of LSPs as IGP shortcuts.

Restrictions

None.

Example

To enable LSPs to be used as IGP shortcuts:

```
rs(config)# ospf set igp-shortcuts on
```

ospf set interface

Mode

Configure

Format

```
ospf set interface <name-or-IPaddr>|all
[state disable|enable] [cost <num>]
[retransmit-interval <num>] [transit-delay <num>]
[priority <num>] [hello-interval <num>]
[router-dead-interval <num>] [poll-interval <num>]
[key-chain <num-or-string>] [authentication-method none|simple|md5][advertise-subnet
on|off][passive]
```

Description

Sets parameters for an OSPF interface.

Parameter	Value	Meaning
interface	<name-or-IPaddr>	The OSPF interface for which you are setting OSPF parameters.
	all	Specifies that you are setting parameters for all OSPF interfaces.
state	disable	Disables OSPF on the interface.
	enable	Enables OSPF on the interface.
cost	<num>	The cost associated with this interface. Specify a number from 1 – 65535. The total cost to get to a destination is calculated by adding up the cost of all interfaces that a packet must cross to reach a destination. The RS calculates the default cost of an OSPF interface using the reference bandwidth and the interface bandwidth. The default reference bandwidth is 1000. It can be changed by using the ospf set ref-bw command. A VLAN that is attached to an interface could have several ports of differing speeds. The bandwidth of an interface is represented by the highest bandwidth port that is part of the associated VLAN. The cost of an OSPF interface is inversely proportional to this bandwidth. The cost is calculated using the following formula: $\text{Cost} = \text{reference bandwidth} * 1,000,000 / \text{interface bandwidth (in bps)}$

Parameter	Value	Meaning
retransmit-interval	<num>	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. Specify a number equal to or greater than 1. The default is 5.
transit-delay	<num>	The estimated number of seconds required to transmit a link state update over this interface. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.
priority	<num>	A number between 0 and 255 specifying the priority for becoming the designated router on this interface. When two routers attached to a network, both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255. The default is 1.
hello-interval	<num>	The length of time, in seconds, between hello packets that the router sends on this interface. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.
router-dead-interva	<num>	The number of seconds not hearing a router's Hello packets before the router's neighbors will declare it down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.
poll-interval	<num>	Before an adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.
key-chain	<num-or-string>	Identify the key-chain containing the authentication keys. Note that the key-chain must have been previously created with the ip-router authentication create key-chain command.
authentication-method		Specifies the authentication method used within the area.
	none	Does not use authentication.
	simple	Uses a simple string (password) up to 8 characters in length for authentication. If you choose this authentication method, then you should also specify a key-chain identifier using the key-chain option.
	md5	Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters.
advertise-subnet	on	Specifies that the point-to-point interface should be advertised as a subnet.

Parameter	Value	Meaning
	off	Specifies that the point-to-point interface should not be advertised as a subnet.
passive		Specify this option on an interface so it neither sends nor receives packets. An example of when passive is used is if this is the only route on the network, passive has the effect of originating a stub link to this interface into the domain.

Restrictions

None.

ospf set monitor-auth-method

Mode

Configure

Format

```
ospf set monitor-auth-method none|simple key-chain <string>|md5 key-chain <string>
```

Description

You can query the OSPF state using the OSPF-Monitor utility. This utility sends non-standard OSPF packets that generate a text response from OSPF. By default these requests are not authenticated. If you specify an authentication key, the incoming requests must match the specified authentication key.

Parameter	Value	Meaning
monitor-auth-method		The authentication method used within the area.
	none	Does not use authentication.
	simple	Uses a simple string (password) up to 16 characters in length for authentication. If you choose this authentication method, then you should also specify a key-chain identifier using the key-chain option.
	md5	Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters.
key-chain	<string>	Identify the key-chain containing the authentication keys. Note that the key-chain must have been previously created with the ip-router authentication create key-chain command.

Restrictions

None.

ospf set opaque-capability

Mode

Configure

Format

ospf set opaque-capability on|off

Description

Turns on support for opaque LSAs (RFC 2370), which are used for MPLS traffic engineering. Using this ability may enlarge the link state database unnecessarily, and does not affect normal protocol operation. The default is on.

Parameter	Value	Meaning
opaque-capability	on	Specify on to turn on support for RFC 2370 opaque LSAs.
	off	Turns off support for RFC 2370 opaque LSAs.

Restrictions

None.

ospf set poll-interval

Mode

Configure

Format

ospf set poll-interval <num>

Description

Sets the interval at which OSPF packets are sent before an adjacency is established.

Parameter	Value	Meaning
poll-interval	<num>	Before adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.

Restrictions

None.

ospf set preference

Mode

Configure

Format

ospf set preference <num>

Description

Sets the preference of routes learned from OSPF.

Parameter	Value	Meaning
preference	<num>	Enter a value between 1 and 255 inclusive. The default preference is 10.

Restrictions

None.

ospf set priority

Mode

Configure

Format

```
ospf set priority <num>
```

Description

Sets the router's priority for becoming the designated router.

Parameter	Value	Meaning
priority	<num>	A number between 0 and 255 specifying the priority for becoming the designated router. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255. The default is 1.

Restrictions

None.

ospf set ref-bw

Mode

Configure

Format

ospf set ref-bw <num>

Description

Set the reference bandwidth in mbps to calculate the interface cost. The cost is calculated using the following formula:

$$\text{Cost} = \text{reference bandwidth} * 1,000,000 / \text{interface bandwidth (in bps)}$$

Parameter	Value	Meaning
ref-bw	<num>	Enter a value between 100 and 65535, inclusive. The default is 1000.

Restrictions

None.

ospf set retransmit-interval

Mode

Configure

Format

```
ospf set retransmit-interval <num>
```

Description

Sets the interval between link state advertisement retransmissions for adjacencies.

Parameter	Value	Meaning
retransmit-interval	<num>	The number of seconds between link state advertisement retransmissions for adjacencies. Specify a number equal to or greater than 1. The default is 5.

Restrictions

None.

ospf set router-dead-interval

Mode

Configure

Format

```
ospf set router-dead-interval <num>
```

Description

Sets the interval during which a router does not receive hello packets before it considers its neighbor to be down

Parameter	Value	Meaning
router-dead-interval	<num>	The number of seconds a router does not receive hello packets before it declares its neighbor to be down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.

Restrictions

None.

ospf set spf-holdtime

Mode

Configure

Format

ospf set spf-holdtime <num>

Description

Sets the minimum time, in seconds, between SPF calculations.

Parameter	Value	Meaning
spf-holdtime	<num>	Enter a value between 0 and 65535 inclusive. The default is 5 seconds. If you enter 0, the SPF calculations will be done one immediately after the other.

Restrictions

None.

ospf set traffic-engineering

Mode

Configure

Format

ospf set traffic-engineering on|off

Description

The **ospf set traffic-engineering** command allows you to enable or disable traffic engineering metrics.

Parameter	Value	Meaning
traffic-engineering	on	Enables traffic engineering metrics.
	off	Disables traffic engineering metrics.

Restrictions

None.

Example

To disable traffic engineering metrics:

```
rs(config)# ospf set traffic-engineering off
```

ospf set transit-delay

Mode

Configure

Format

```
ospf set transit-delay <num>
```

Description

Sets the estimated interval required to transmit a link state update.

Parameter	Value	Meaning
transit-delay	<num>	The estimated number of seconds required to transmit a link state update. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.

Restrictions

None.

ospf set virtual-link

Mode

Configure

Format

```
ospf set virtual-link <number-or-string>
[state disable|enable] [cost <num>] [retransmit-interval <num>]
[transit-delay <num>] [priority <num>] [hello-interval <num>]
[router-dead-interval <num>] [poll-interval <num>] [authentication-method
none|simple|md5] [key-chain <string>]
```

Description

Sets the parameters for an OSPF virtual link.

Parameter	Value	Meaning
virtual-link	<number-or-string>	The identifier for this virtual link.
state	disable	Disables the virtual link.
	enable	Enables the virtual link.
cost	<num>	The cost associated with this virtual link. The cost of all interfaces that a packet must cross to reach a destination are added to get the cost to that destination. The default cost of the OSPF interface is 1, but another non-zero value may be specified. Specify a number from 1– 65535.
retransmit-interval		The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. Specify a number equal to or greater than 1.
transit-delay		The estimated number of seconds required to transmit a link state update over this virtual link. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1.
priority		A number between 0 and 255 specifying the priority for becoming the designated router on this virtual link. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255.
hello-interval		The length of time, in seconds, between hello packets that the router sends on this virtual link. Specify a number from 0 – 255. The default is 60 seconds.

Parameter	Value	Meaning
router-dead-interval		The number of seconds not hearing a router's Hello packets before the router's neighbors will declare it down. Specify a number from 0 – 255. The default value for this parameter is 4 times the value of the <code>hello-interval</code> parameter
poll-interval		Before adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number from 1 – 255. The default is 120 seconds.
authentication-method		The authentication method used within the area.
	none	Does not use authentication.
	simple	Uses a simple string (password) up to 16 characters in length for authentication. If you choose this authentication method, then you should also specify a key-chain identifier using the key-chain option.
	md5	Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters.
key-chain	<string>	Identify the key-chain containing the authentication keys. Note that the key-chain must have been previously created with the ip-router authentication create key-chain command.

Restrictions

None.

ospf show adjacency-down-reason

Mode

Enable

Format

```
ospf show adjacency-down-reason
```

Mode

Displays why a router's OSPF adjacency went down.

Restrictions

None

Example

ospf show all

Mode

Enable

Format

ospf show all

Description

Displays all OSPF tables:

- globals
- timers
- area
- interface
- LSA
- next-hop
- export policies
- import policies

For an example and description of each of these tables, refer to the appropriate ospf show command.

Restrictions

None

ospf show areas

Mode

Enable

Format

ospf show areas <IPaddr>|backbone|all

Description

Displays OSPF areas.

Parameter	Value	Meaning
areas		Displays information about the specified OSPF areas.
	<IPaddr>	The area specified by the IP address.
	backbone	Backbone area.
	all	All areas.

Restrictions

None

Example

Following is an example of the **ospf show areas all** command:

```
Area 190.135.89

  Transit Capability: 0
  Area Border Routers: 2
  AS Border Routers: 0
  Spf count: 42
  Local Virtual Links: 0
  Router Vertex: 81d509a0
  Default Summary Vertex: 0

  No Configured Stub Links

  No network summarization ranges

  No active tree walks

  Interfaces:
Internet Address 100.1.1.1/24, Area 190.135.89
  Router ID 7.7.7.7, Network Type Broadcast, Cost: 20
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 7.7.7.7, Interface address 100.1.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 14:58:33
```

ospf show as-external-lsdb

Mode

Enable

Format

```
ospf show as-external-lsdb
```

Description

Displays OSPF Autonomous System (AS) external link state advertisements (LSAs) in the database.

Restrictions

None

Example

Following is an example of the **ospf show as-external-lsdb** command

```
ospf show as-external-lsdb
  global external database:
    type AEX id 44 advrt 7.7.7.7 seq 0x80000009 [mem: 81d50cc0]
    left 81d50cc0 right 81d50c20 bitindex 0x1
    age 1450 cksum 0xde8c len 36 flags <>
    time now 16727 install 5277 nextrecv 0 nextsend 15282
    refcount 0 spfcount 0 options <E>
    wrapsave 0
    ospf route 815decb0
      [Static] rentry 81d62c18 cost 0 tag 0 pref1/2 5/0
      ls origin 0.0.0.0 area 0.0.0.0 dest type AEX
      options spfcount 0 flags <EXPORT>
    netmask 0xff000000 (8)
    type 1 forward 0.0.0.0 tag 0x96
    tos 0 metric 1

    type AEX id 55 advrt 7.7.7.7 seq 0x80000009 [mem: 81d50c20]
    left 81d50950 right 81d50c20 bitindex 0x2
    age 1450 cksum 0xc7ca len 36 flags <>
    time now 16727 install 5277 nextrecv 0 nextsend 15282
    refcount 0 spfcount 0 options <E>
    wrapsave 0
    ospf route 815deabc
      [RIP] rentry 81d83650 cost 2 tag 0 pref1/2 100/0
```

ospf show border-routes

Mode

Enable

Format

ospf show border-routes

Description

Display border and boundary router information.

Restrictions

None.

ospf show database

Mode

Enable

Format

```
ospf show database asbr-summary <ip-addr>|external| database-summary |  
network|nssa-external|router|summary|link-id <ip-addr>|adv-router
```

Description

Displays database summary.

Parameter	Value	Meaning
asbr-summary	<ip-addr>	Displays ASBR summary link states.
external		Displays external link states.
database-summary		Displays a summary of the database.
network		Displays network link states.
nssa-external		Displays NSSA external link states.
router		Displays router link states.
summary		Displays network summary link states.
link-id	<ip-addr>	Displays link state ID (as an IP address).
adv-router		Displays the link states of the advertising router.

Restrictions

None.

ospf show export-policies

Mode
Enable

Format

ospf show export-policies

Description

Displays OSPF export policies.

Restrictions

None

Example

Following is an example of the **ospf show export-policies** command:

```
sc-lab-YagoNMS# ospf show export-policies

Export controls:
-----
type 1,2:
Protocol      : Direct
AdvFlag       :
Destination   Netmask      AdvFlag  Type      Flags
-----
134.141.178   255.255.255.224 None     None
134.141.179.192 255.255.255.224 None     None
```

ospf show globals

Mode

Enable

Format

ospf show globals

Description

Displays OSPF global parameters.

Restrictions

None

Example

Following is an example of the **ospf show globals** command:

```
Router-1# ospf show globals

Globals:
-----

Task Name       : OSPF
Send buffer size : 4096
Recv buffer size : 65536
Priority        : 41
Protocol        : 89

OSPF Globals:
-----

Router ID       : 10.50.7.1
Border Router   : AreaAS
Inter/Intra Pref : 10
External Pref   : 150
Default Metric  : 1
Default Tag     : 0 Path: (1) 0 EGP
Default Type    : 2
SPF count       : 4
LSAs originated : 4
LSAs received   : 0
Router         : 40
SumNet          : 2

Syslog first 16, then every 256
Monitor authentication: none

Router-1#
```

The output displays the following information:

- the sizes of the buffers
- the IP protocol OSPF runs over; OSPF runs over IP protocol 89
- the router ID
- the preference value of OSPF inter and intra-area routes
- the preference value of OSPF-external routes
- the default metric
- the number of LSAs received and generated

ospf show import-policies

Mode

Enable

Format

```
ospf show import-policies
```

Description

Displays OSPF import policies.

Restrictions

None

ospf show interfaces

Mode

Enable

Format

ospf show interfaces [detail]

Mode

Displays OSPF interfaces.

Restrictions

None

Example

Following is an example of the **ospf show interfaces** command:

```
Router-1# ospf show interfaces
Internet Address 4.4.4.4, Transit Area 201.135.89
  Router ID 2.2.2.2, Network Type Virtual, Cost: 20
  Transmit Delay is 1 sec, State Pt2Pt, Priority 1
  Designated Router (ID) 0.0.0.0, Interface address 4.4.4.4
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 19:32:49
  Neighbor Count is 1
```

```
Router-1# conf
```

ospf show lsa

Mode

Enable

Format

```
ospf show lsa [area-id <area-id>] [type router-links|network-links | summary-networks
|summary-asbr |as-external] [ls-id <IPaddr>] [adv-rtr <routerID>]
```

Description

The **ospf show lsa** command allows you to display link state advertisements, by type. There are five types of LSAs, as described below. All LSAs, except for the as-external LSAs are flooded throughout a single area. The as-external LSAs are flooded throughout the entire autonomous system (AS), except through the stub area.:

- router-links - These LSAs describe the router's working connections (interfaces and links). The router generates router link LSAs for each area to which it belongs.
- network-links - These LSAs describe all routers attached to the network. These LSAs are generated by the designated router of a broadcast or NBMA network.
- as-external - These LSAs describe routes to destinations that are external to the AS. These LSAs are generated by AS boundary routers.

The following two LSAs describe inter-area routes, and enable the condensing of routing information at area borders. Both types are generated by area border routers.

- summary-network - These are summary LSAs that describe routes to the network specified by the LSA ID.
- summary-asbr - These are summary LSAs that describe routes to the AS boundary router specified by the LSA ID.

Parameter	Value	Meaning
area-id	<area-id>	Specifies the IP address of the OSPF area being described.
type		Specifies the type of LSA to be displayed.
	router-links	Specifies the router links advertisements. They describe the status of the router's interfaces. Set the LSA ID (ls-id field) to the originating router's router ID.
	network-links	Specifies the network links advertisements. They describe the set of routers attached to the network specified by the LSA ID. Set the LSA ID (ls-id field) to the IP interface address of the network's designated router.
	summary-networks	Specifies the summary links advertisements. They describe the set of routers attached to the network specified by the LSA ID. Set the LSA ID (ls-id field) to the destination network's IP address.

Parameter	Value	Meaning
	summary-asbr	Specifies the summary link advertisements. They describe routes to AS boundary routers. Set the LSA ID (ls-id field) to the router ID of the AS boundary router being described.
	as-external	Specifies the AS external link advertisements. They describe routes to destinations external to the AS. Set the LSA ID (ls-id field) to the destination network's IP address.
ls-id	<IPaddr>	The LSA ID. It identifies the part of the routing domain that is being described by the LSA. Its value depends on the LSA type specified.
adv-rtr	<routerID>	Router ID of the router which originated the LSAs.

Restrictions

None.

ospf show neighbor

Mode

Enable

Format

ospf show neighbor

Description

Displays the OSPF neighbors.

Restrictions

None.

ospf show statistics

Mode

Enable

Format

```
ospf show statistics [interface <IPaddr>|neighbor <IPaddr>]
```

Description

Displays OSPF statistics for an interface.

Parameter	Value	Meaning
interface	<IPaddr>	Specify the IP address of the interface for which statistics will be displayed.
neighbor	<IPaddr>	Specify the IP address of the neighbor for which statistics will be displayed.

Restrictions

None

Example

Following is an example of the **ospf show statistics interface** command:

```
rs# ospf show statistics interface 16.128.11.7

Statistics for Interface 16.128.11.7:

Packets Received:
  Monitor                0      Hello                1622
  Database Description    178    LS Request          144
  LS Update              1496    LS Acknowledgement 244

Packets Sent:
  Monitor                0      Hello                1623
  Database Description    179    LS Request          143
  LS Update              410    LS Acknowledgement 3389

Errors:
  Packet too short                0
  Invalid header length           0      Invalid version                0
  Invalid checksum                0      Invalid authentication type    0
  No such multicast interface      0      No such interface              0
  Invalid interface               0      Invalid Mask                   0
  Invalid Hello interval          0      Invalid Router Dead interval   0
  Unknown neighbour              0      Options mismatch               0
  Master flag mismatch            0      Initialize flag mismatch       0
  DD sequence number mismatch     0      Invalid LS type                0
  Bad LS Request                  0      No such virtual interface      0
  Invalid area ID                 0      Confusing Master/Initial flags 0
  Invalid MD5 digest              0      Own packet received            0
  Invalid authentication key       0      DD Options mismatch            0
  Packet on passive interface     0      Packet on down virtual interface 0
  Packet with same router id as ours 0

rs#
```

ospf show summary-asb

Mode

Enable

Format

ospf show summary-asb

Description

Displays OSPF border routes.

Restrictions

None

ospf show ted

Mode

Enable

Format

ospf show ted

Description

Displays OSPF traffic engineering database.

Restrictions

None

ospf show timers

Mode
Enable

Format

ospf show timers

Description

Displays OSPF timers.

Restrictions

None

Example

The following is an example of the **ospf show timers** command:

Router-1# ospf show timers							
Timers:							

Timer	State	Last	Next	Intvl	Jitter	Flags	

OSPF_Lock	Active	11:10:07	11:10:12	5	-		
OSPF_LSAGenSum	Active	10:40:18	11:10:18	30:00	-		
OSPF_Lock	Active	11:10:07	11:10:12	5	-		
OSPF_LSAGenAse	Active	11:10:05	11:10:12	7	-		
OSPF_AseQueue	Inactive	-	-	-	-	OneShot Inactive	
OSPF_Ack	Inactive	-	-	-	-	HiPrio OneShot I	
nactive							
OSPF_LSDBAseAge	Active	11:09:53	11:10:54	1:01	-		
OSPF_LSDBSumAge	Active	10:56:24	11:11:24	15:00	-		
OSPF_LSDBIntAge	Active	10:55:20	11:10:20	15:00	-		
OSPF_LSAGenInt	Active	10:51:34	11:21:34	30:00	-		

ospf show virtual-links

Mode

Enable

Format

ospf show virtual-links

Description

Displays OSPF virtual links.

Restrictions

None

Example

Following is an example of the **ospf show virtual-links** command:

```
rs# ospf show virtual-links
Internet Address 2.2.2.2, Transit Area 201.135.89
  Router ID 3.3.3.3, Network Type Virtual, Cost: 20
  Transmit Delay is 1 sec, State Pt2Pt, Priority 1
  Designated Router (ID) 0.0.0.0, Interface address 2.2.2.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 15:39:53
  Neighbor Count is 1

Internet Address 4.4.4.4, Transit Area 201.135.89
  Router ID 3.3.3.3, Network Type Virtual, Cost: 1
  Transmit Delay is 1 sec, State Down, Priority 1
  Designated Router (ID) 0.0.0.0, Interface address 4.4.4.4
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 0
```

ospf start|stop

Mode

Configure

Format

ospf start|stop

Description

Start or stop the OSPF protocol. OSPF is disabled by default on the RS.

Parameter	Value	Meaning
ospf	start	Starts OSPF.
	stop	Stops OSPF.

Restrictions

None.

48 PING COMMAND

ping

Mode

User or Enable

Format

```
ping <hostname-or-IPaddr> packets <num> size <num> wait <num> [flood] [dontroute]
```

Description

The **ping** command tests the connection between the RS and an IP host. The **ping** command sends ICMP echo packets to the host you specify.

- If the packets reach the host, the host sends a ping response to the RS and the CLI displays messages stating that the host can be reached.
- If the host does not respond, the RS assumes the host cannot be reached from the RS and the CLI display messages stating that the host did not reply.

Parameter	Value	Meaning
ping	<hostname-or-IPaddr>	The host name or IP address you want to ping.
packets	<num>	The number of ping packets you want to send. The default is 1.
size	<num>	The packet size. For Ethernet, specify a number from 0 – 1364.
wait	<num>	The number of seconds the RS will wait for a positive response from the host before assuming that the host has not responded. The default is 1.
flood		Causes the RS to send a new ping request as soon as a ping reply is received. If you do not specify the flood option, the RS waits to send a new request. The amount of time the RS waits is specified by the wait option.
dontroute		Restricts the ping to locally attached hosts.

Restrictions

If you enter this command from the User mode, the only parameter you can use is *<hostname-or-IPaddr>*. To use any of the other parameters, you must be in Enable mode.

49 PORT COMMANDS

The port commands set and display the following parameters:

- Port state (enabled or disabled)
- Bridging status (flow-based or address-based)
- Port operating mode (half duplex or full duplex)
- Port speed for the 10/100 ports (10-Mbps or 100-Mbps)
- Port mirroring (used for analyzing network traffic)
- Port shut down if broadcast threshold is reached
- Channelized T1, E1 and T3 port parameters
- Clear Channel T3 and E3 port parameters

49.1 COMMAND SUMMARY

Tables in this section:

- [“Ethernet Port Commands”](#)
- [“Gigabit Ethernet Port Commands”](#)
- [“Channelized E1 Port Commands”](#)
- [“Channelized T1 Port Commands”](#)
- [“Channelized T3 Port Commands”](#)
- [“Clear Channel E3 Port Commands”](#)
- [“Clear Channel T3 Port Commands”](#)
- [“CMTS Port Commands”](#)
- [“HSSI Port Commands”](#)
- [“Packet-over-SONET Port Commands”](#)
- [“Serial Port Commands”](#)

Ethernet Port Commands

The following table lists the port commands for Ethernet ports.

Table 49-1 Ethernet Port Commands

<code>port auto-negotiate enable <port-list> disable <port-list> restart <port-list></code>
<code>port bmon <port-list> [rate <number>] [duration <number>] [shutdown <number>] [packets-limited all broadcast]</code>
<code>port clear per-vlan-stats [port <port> {vid <number> vlan <string>}] [vid <number> port <port>][vlan <string> port <port>]</code>
<code>port description <port-list> <desc></code>
<code>port disable <port-list> force_link_down</code>
<code>port enable 8021p port <port-list></code>
<code>port enable per-vlan-stats ports <port-list></code>
<code>port flow-bridging <port-list> all-ports</code>
<code>port set <port-list> all-ports [auto-negotiation on off] [auto-negotiation-speed 10Mbps 100Mbps 10_100Mbps] [auto-negotiation-duplex half full both] [duplex full half] [hash-mode m0 m1 m2 m3 m-auto] [ifg <number>] [input-encapsulation forced-ethernet_ii] [speed 10Mbps 100Mbps]</code>
<code>port show 8021p <port-list> all-ports</code>
<code>port show autonegotiation <port-list> all-ports</code>
<code>port show autonegotiation-capabilities <port-list> all-ports</code>
<code>port show bmon [config] [detail] [port <port-list>] [stats]</code>
<code>port show bridging-status <port-list> all-ports</code>
<code>port show description <port-list> all-ports</code>
<code>port show hash-mode <port-list> all-ports</code>
<code>port show MAU <port-list> all-ports</code>
<code>port show MAU-statistics <port-list> all-ports</code>
<code>port show mc-vlan-encap <port-list> all-ports</code>
<code>port show mtu <port-list> all-ports</code>
<code>port show per-vlan-stats port show per-vlan-stats [port <port> {vid <number> vlan <string>}] [vid <number> port <port>][vlan <string> port <port>]</code>
<code>port show port-status <port-list> all-ports all-SmartTRUNKs</code>
<code>port show stp-info <port-list> all-ports</code>
<code>port show pvst-info <port-list> all-ports</code>
<code>port show vlan-info <port-list> all-ports</code>
<code>port show mirroring-status <slot> all-slots</code>

Gigabit Ethernet Port Commands

The following table lists the port commands for Gigabit Ethernet ports.

Table 49-2 Gigabit Ethernet Port Commands

port auto-negotiate enable <port-list> disable <port-list> restart <port-list>
port bmon <port-list> [rate <number>] [duration <number>] [shutdown <number>] [packets-limited all broadcast]
port clear per-vlan-stats port <port> vid <number> vlan <string> port <port>
port description <port-list> <desc>
port disable <port-list> force_link_down
port enable 8021p port <port-list>
port enable per-vlan-stats ports <port-list>
port flow-bridging <port-list> all-ports
port set <port-list> all-ports [auto-negotiation on off] [auto-negotiation-flowctl off asymmetric symmetric both] [hash-mode m0 m1 m2 m3 m-auto] [ifg <number>] [link-timer <number>] [mtu <number>]
port show 8021p <port-list> all-ports
port show autonegotiation <port-list> all-ports
port show autonegotiation-capabilities <port-list> all-ports
port show bmon [config] [detail] [port <port-list>] [stats]
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show hash-mode <port-list> all-ports
port show MAU <port-list> all-ports
port show MAU-statistics <port-list> all-ports
port show mc-vlan-encap <port-list> all-ports
port show mtu <port-list> all-ports
port show per-vlan-stats port <port> vid <number> vlan <string> port <port>
port show port-status <port-list> all-ports all-SmartTRUNKs
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports
port show mirroring-status <slot> all-slots

ATM Port Commands

The following table lists the port commands for ATM ports.

Table 49-3 ATM Port Commands

port description <port-list> <desc>
port disable <port-list> force_link_down
port set <port-list> all-ports [framing cbit-parity m23 esf g832 g751] [hash-mode m0 m1 m2 m3 m-auto] [ifg <number>] [mtu <number>] [transmit-clock-source local loop]
port show hash-mode <port-list> all-ports
port show mtu <port-list> all-ports
port show port-status <port-list> all-ports all-SmartTRUNKs
port show vlan-info <port-list> all-ports

Channelized E1 Port Commands

The following table lists the port commands for Channelized E1 ports.

Table 49-4 Channelized E1 Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop
port description <port-list> <desc>
port disable <port-list> force_link_down
port loopback <port-list> local network-line network-payload none
port set <port-list> clock-source internal loop
port set <port-list> crc 16-bit 32-bit
port set <port-list> framing crc4 nocrc4 none wan-encapsulation frame-relay ppp cisco-hdlc
port set <port-list> idle-code <value>
port set <port-list> impedance 75ohm 120ohm
port set <port-list> international-bits 0 1
port set <port-list> invert-data
port set <port-list> line-coding ami hdb3
port set <port-list> national-bits <value>
port set <port-list> speed-56 speed-64
port set <port-list> timeslots {<start-slot>[-<end-slot>][,...]} wan-encapsulation frame-relay ppp cisco-hdlc
port set <port-list> ts16 wan-encapsulation frame-relay ppp cisco-hdlc

Table 49-4 Channelized E1 Port Commands (Continued)

port set <port-list> wan-encapsulation frame-relay ppp cisco-hdlc
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show dsx-stats <port-list> interval <numbrer>
port show port-status <port-list> all-ports all-SmartTRUNKs
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports

Channelized T1 Port Commands

The following table lists the port commands for Channelized T1 ports.

Table 49-5 Channelized T1 Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop
port description <port-list> <desc>
port disable <port-list> force_link_down
port loopback <port-list> local network-line network-payload niu-remote-line-fdl-ansi niu-remote-line-inband remote-line-inband remote-payload-fdl-ansi remote-line-fdl-ansi remote-line-fdl-bellcore none
port set <port-list> cablelength <length-in-feet>
port set <port-list> clock-source internal loop
port set <port-list> crc 16-bit 32-bit
port set <port-list> fdl ansi bellcore none
port set <port-list> framing sf esf sf-japan esf-japan {none wan-encapsulation frame-relay ppp cisco-hdlc}
port set <port-list> idle-code <value>
port set <port-list> invert-data
port set <port-list> lbo 0db -7.5db -15db -22.5db
port set <port-list> line-coding ami b8zs
port set <port-list> remote-loopback-enable enable disable
port set <port-list> speed-56 speed-64
port set <port-list> timeslots {<start-slot>[-<end-slot>][,...]} wan-encapsulation frame-relay ppp cisco-hdlc
port set <port-list> wan-encapsulation frame-relay ppp cisco-hdlc

Table 49-5 Channelized T1 Port Commands (Continued)

port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show dsx-stats <port-list> interval <numbrer>
port show port-status <port-list> all-ports all-SmartTRUNKs
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports

Channelized T3 Port Commands

The following table lists the port commands for Channelized T3 ports.

Table 49-6 Channelized T3 Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop (This can be applied only to a T1 line within the Channelized T3, for example, t3.2.1:1.)
port description <port-list> <desc>
port disable <port-list> force_link_down
port loopback <port-list> local network-line niu-remote-line-fdl-ansi niu-remote-line-inband none
port set <port-list> cablelength <length-in-feet>
port set <port-list> clock-source internal loop
port set <port-list> crc 16-bit 32-bit
port set <port-list> fdl ansi bellcore none
port set <port-list> framing c-bit m23
port set <port-list> idle-code <value>
port set <port-list> invert-data
port set <port-list> line-coding ami b8zs
port set <port-list> remote-loopback-enable enable disable
port set <port-list> speed-56 speed-64
port set <port-list> timeslots {<start-slot>[-<end-slot>][,...]} wan-encapsulation frame-relay ppp cisco-hdlc
port set <port-list> wan-encapsulation frame-relay ppp cisco-hdlc
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports

Table 49-6 Channelized T3 Port Commands (Continued)

port show dsx-stats <port-list> interval <numbrer>
port show port-status <port-list> all-ports all-SmartTRUNKs
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports
port testport <port-list> monitor break-out [line-coding ami b8zs]

Clear Channel E3 Port Commands

The following table lists the port commands for Clear Channel E3 ports.

Table 49-7 Clear Channel E3 Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop
port description <port-list> <desc>
port disable <port-list> force_link_down
port loopback <port-list> local network-line none
port set <port-list> cablelength <length-in-feet> [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> clock-source internal loop [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> crc 16-bit 32-bit [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> framing g751 g832 [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> invert-data [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> national-bits 1 0 [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> scrambling-mode enabled disabled
port set <port-list> wan-encapsulation frame-relay ppp cisco-hdlc
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show dsx-stats <port-list> interval <numbrer>
port show port-status <port-list> all-ports all-SmartTRUNKs
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports

Table 49-7 Clear Channel E3 Port Commands (Continued)

port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports

Clear Channel T3 Port Commands

The following table lists the port commands for Clear Channel T3 ports.

Table 49-8 Clear Channel T3 Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop
port description <port-list> <desc>
port disable <port-list> force_link_down
port loopback <port-list> local network-line remote-line-feac none
port set <port-list> cablelength <length-in-feet> [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> clock-source internal loop [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> crc 16-bit 32-bit [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> framing c-bit m23 [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> invert-data [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> remote-loopback-enable enable disable [wan-encapsulation frame-relay ppp cisco-hdlc]
port set <port-list> scrambling-mode enabled disabled
port set <port-list> wan-encapsulation frame-relay ppp cisco-hdlc
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show dsx-stats <port-list> interval <numbrer>
port show port-status <port-list> all-ports all-SmartTRUNKS
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports

CMTS Port Commands

The following table lists the port commands for CMTS ports.

Table 49-9 CMTS Port Commands

port description <port-list> <desc>
port disable <port-list> force_link_down
port show hash-mode <port-list> all-ports
port show mtu <port-list> all-ports
port show port-status <port-list> all-ports all-SmartTRUNKs
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports

HSSI Port Commands

The following table lists the port commands for HSSI ports.

Table 49-10 HSSI Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop
port description <port-list> <desc>
port disable <port-list> force_link_down
port set <port-list> all-ports [clock <clock-source>] [hash-mode m0 m1 m2 m3 m-auto] [wan-encapsulation frame-relay ppp cisco-hdlc] [speed <number>]
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show dsx-stats <port-list> interval <numbrer>
port show hash-mode <port-list> all-ports
port show mtu <port-list> all-ports
port show port-status <port-list> all-ports all-SmartTRUNKs
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports
port show mirroring-status <slot> all-slots
port testport <port-list> monitor break-out [cablelength <length-in-feet>] [line-coding ami b8zs hdb3]

Packet-over-SONET Port Commands

The following table lists the port commands for Packet-over-SONET (POS) ports.

Table 49-11 Packet-over-SONET Port Commands

port description <port-list> <desc>
port disable <port-list> force_link_down
port set <port-list> all-ports [hash-mode m0 m1 m2 m3 m-auto] [mc-vlan-encap <number>] [mtu <number>]
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show hash-mode <port-list> all-ports
port show mtu <port-list> all-ports
port show port-status <port-list> all-ports all-SmartTRUNKs
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports
port show vlan-info <port-list> all-ports

Serial Port Commands

The following table lists the port commands for Serial ports.

Table 49-12 Serial Port Commands

port bert <port-list> pattern <pattern> interval <minutes> start stop
port description <port-list> <desc>
port disable <port-list> force_link_down
port set <port-list> all-ports [hash-mode m0 m1 m2 m3 m-auto] [speed <number>] [wan-encapsulation frame-relay ppp cisco-hdlc]
port show bridging-status <port-list> all-ports
port show description <port-list> all-ports
port show dsx-stats <port-list> interval <numbrer>
port show hash-mode <port-list> all-ports
port show mtu <port-list> all-ports
port show port-status <port-list> all-ports all-SmartTRUNKs
port show serial-link-info <port-list> all-ports [brief all]
port show stp-info <port-list> all-ports
port show pvst-info <port-list> all-ports

Table 49-12Serial Port Commands (Continued)

port show vlan-info <port-list> all-ports
port show mirroring-status <slot> all-slots
port testport <port-list> monitor break-out [cablelength <length-in-feet>] [line-coding ami b8zs hdb3]

WDM Port Commands

The following table lists the port commands for Wave Division Multiplexing (WDM) ports

port enable wdm <port-list>

port auto-negotiate

Mode

Enable

Format

port auto-negotiate enable <port-list> | disable <port-list> | restart <port-list>

Description

The **port auto-negotiate** command allows you to enable auto-negotiation on a port, disable auto-negotiation on a port, and/or restart auto-negotiation on a port. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

Parameter	Value	Meaning
enable	<port-list>	Enables auto-negotiation on the port or set of ports.
disable	<port-list>	Disables auto-negotiation on the port or set of ports.
restart	<port-list>	Restarts auto-negotiation on the port or set of ports.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To enable auto-negotiation on port **et.2.1**:

```
rs# port auto-negotiate enable et.2.1
```

port bert

Mode

Enable

Format

```
port bert <port-list> [pattern <pattern>] [interval <minutes>] [start|stop]
```

Description

The **port bert** command is used to configure BERT testing on a specified physical or logical port. Use the **port show serial-link-info** command to view the results.

The BERT test is started by issuing the **port bert start** command. The BERT test will stop automatically after the interval specified by <minutes>. To stop the BERT test before this, use the **port bert stop** command. The default **interval** is 1 minute and the default **pattern** is **2^11**.



Note Use the **port show serial-link-info <port-list> all** command to view the results.

The following table describes the parameters of the command.

Parameter	Value	Meaning
bert	<port-list>	Configure and enable BERT testing on a specified physical or logical port (see Section 1.4, "<port-list> Syntax.").
pattern	<pattern>	Specifies the pseudo-random or repetitive pattern to be used for the BERT test. This can be one of the following:
	0s	Repetitive test pattern of all zeros (as 00000...).
	1s	Repetitive test pattern of all ones (as 11111...).
	2^11	Pseudo-random test pattern (2,048 bits long). This is the default.
	2^15	Pseudo-random O.151 test pattern (32,768 bits long).
	2^20-0153	Pseudo-random O.153 test pattern (1,048,575 bits long)
	2^20-QRSS	Pseudo-random QRSS O.151 test pattern (1,048,575 bits long).
	2^23	Pseudo-random O.151 test pattern (8,388,607 bits long).
	alt-0-1	Repetitive alternating test pattern of zeros (0s) and ones (1s), as 01010101...
interval	<minutes>	Specifies the duration of the BERT test in minutes, from 1 to 1440 minutes (24 hours). The default is 1 minute.

Parameter	Value	Meaning
start		Used to start the BERT test.
stop		Used to stop the BERT test.

Restrictions

- The line must first be put in loopback and then the BERT test run, unless external test equipment is used.
- Currently, BERT testing is only supported on Channelized T1, E1 and T3 interfaces, and Clear Channel T3 and E3 interfaces, due to hardware restrictions. For Channelized T1 and E1 interfaces, BERT testing is limited to running only on a single test per board at any one time. For Channelized T3 interfaces, BERT testing is limited to one test at a time per upper two ports, and one test per lower two ports. In addition, BERT testing can be applied only to a T1 line within the Channelized T3, for example, t3.2.1:1.

Examples

To specify BERT testing on the third T1 port in slot 5 for one hour:

```
rs# port bert t1.5.3 pattern 2^20-0153 interval 60
```

To start BERT testing, then terminate the test before the test interval expires:

```
rs# port bert t1.5.3 start
rs# port show serial-link-info t1.5.3 all
T1 Slot 5 Port 3:      Channelized
.
.
.
Remote loopback enable:  enabled
BERT state:             Running
BERT status:            not available
BERT start time:        Mon Oct 16 09:59:27 2000
BERT end time:          running
BERT time remaining:    01H 00M 00S
BERT pattern:           2^20-0153
BERT interval (minutes): 60
BERT sync count:        0
BERT total errors:      0
BERT total mb:          0
BERT errors since sync: 0
BERT kb since sync:     0
.
.
.
rs# port bert t1.5.3 stop
```


port bmon

Mode

Configure

Format

```
port bmon <port-list> [rate <number>] [duration <number>] [shutdown <number>]  
[packets-limited all | broadcast]
```

Description

The **port bmon** command allows you to monitor the broadcast traffic on one or more ports and shut down a port if its broadcast traffic reaches and sustains a certain rate limit for a specified length of time. You can specify the duration of the port shut down.

This command is useful in the case where excess traffic is degrading performance. With this command, you can define monitoring thresholds on a port or set of ports. If those thresholds are met or exceeded, then the port can be shutdown. This reduces the risk of the control module becoming overloaded by traffic.

Parameter	Value	Meaning
bmon	<port-list>	Specifies the ports that are being monitored for broadcasts (see Section 1.4, "<port-list> Syntax.").
rate	<number>	The rate limit, in Kpkts per second, which will trigger a port shut down if the rate is sustained for the specified duration. The range of <number> is 1 to 1000. The default value is 10.
duration	<number>	The number of seconds that the specified rate limit is sustained, after which the port will be shut down. The range of <number> is 1 to 3600. The default value is 1.
shutdown	<number>	The number of seconds that the port will be shut down if the rate threshold is reached. The range of <number> is 60 to 36000. The default value is 300.
packets-limited		Specifies the type of packets to monitor for shutdown.
	all	Specify all to monitor all packets. This is the default.
	broadcast	Specify broadcast to only monitor broadcast packets.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Examples

To monitor broadcast traffic on port **et.1.3** and shut it down for 5 minutes if the rate of 10,000 packets per second is sustained for 1 second:

```
rs(config)# port bmon et.1.3
```

To monitor broadcast traffic on port **et.1.3** and shut it down for 3 minutes if the rate of 25,000 packets per second is sustained for 5 seconds:

```
rs(config)# port bmon et.1.3 rate 25 duration 5 shutdown 180
```

To configure a 360 second shutdown on port **et1.3** whenever 100000 packets are counted within 100 seconds:

```
rs(config)# port bmon packets 100 time-interval 100 shutdown 360
```

port clear per-vlan-stats

Mode

Enable

Format

```
port clear per-vlan-stats [port <port> {vid <number> | vlan <string>}] [vid <number> port <port>] [vlan <string> port <port>]
```

Description

Use the **port clear per-vlan-stats** command to clear the layer-2 octet and frame counters associated with the specified port and VLAN.

Parameter	Value	Meaning
port	<port>	Specifies the port within a VLAN for which statistics are cleared (see Section 1.4, "<port-list> Syntax.").
vid	<number>	Specifies the VLAN by ID number for which statistics on a particular port are cleared.
vlan	<string>	Specifies the VLAN for which statistics on a particular port are cleared.

Restrictions

Can be used only with 10/100 and Gigabit Ethernet ports set up as 802.1Q trunk ports.

Example

To clear statistics for VLAN BLUE on et.3.1:

```
rs# port clear per-vlan-stats port et.3.1 vlan blue
```

port clear phy-errors

Mode
Enable

Format

port clear <port-list> | all-ports

Description

The **port clear phy-errors** command clears potential physical error statistics collected with the **port show phy-errors** command. When you clear statistics, the RS sets the counters for the cleared statistics to 0.

Parameter	Value	Meaning
clear	<port-list>	Clears statistics for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
	all-ports	Clears statistics for all ports.

Restrictions

You *cannot* use this command to clear physical layer errors for WAN ports or ports on the following line cards:

- POS OC-12
- ATM OC-12
- Serial line cards
- CMTS line cards

Examples

To clear potential physical error statistics for all ports:

```
rs# port clear all-ports
```

port description

Mode

Configure

Format

port description *<port-list>* *<desc>*

Description

The **port description** command allows you to define a character string description for a port. This is useful for management purposes.

Parameter	Value	Meaning
description	<i><port-list></i>	Specifies the port(s). Valid for Ethernet and WAN ports only (see Section 1.4, "<port-list> Syntax.").
	<i><desc></i>	Specifies the character string used for the description of the port. The string must be 125 characters or less.

Restrictions

This command is valid for Ethernet and WAN only.

Example

To set port **et.2.1** with the description **vlan1-2**:

```
rs(config)# port description et.2.1 vlan1-2
```

port disable

Mode

Configure

Format

```
port disable <port-list>
```

Description

The **port disable** command disables specified ports. Disabled ports do not send or receive any traffic. You might want to disable unused ports to prevent network users from inadvertently or unscrupulously connecting to unoccupied but enabled ports on the RS.

Parameter	Value	Meaning
disable	<port-list>	Specifies the ports you are disabling (see Section 1.4, "<port-list> Syntax.").
	force_link_down	In addition to disabling the port, this option forces the link-state of the port to <i>down</i> .

Restrictions

None.

Examples

To disable port **et.1.3** on the RS:

```
rs(config)# port disable et.1.3
```

To disable ports 1 through 5 on the Ethernet line card in slot 3 of the RS chassis, and to force each port's link-state to the down state:

```
rs(config)# port disable et.3.1-5 force_link_down
```

port enable 8021p

Mode

Configure

Format

```
port enable 8021p port <port-list> | all-ports
```

Description

The **port enable 8021p** command enables 802.1p encapsulation on the specified ports. The 802.1p standard provides the ability to classify traffic into eight priority categories or classes of service. This classification scheme is based on MAC frame information and is used for QoS (Quality of Service) for VLANs.

Parameter	Value	Meaning
port	<port-list>	Specifies the port(s) you are enabling (see Section 1.4, "<port-list> Syntax.").
	all-ports	Specify all-ports to enable 802.1p encapsulation on all relevant ports.

Restrictions

None.

Example

To enable 802.1p encapsulation on port **et.1.3**:

```
rs(config)# port enable 8021p port et.1.3
```

port enable per-vlan-stats

Mode
Configure

Format

port enable per-vlan-stats ports <port-list>

Description

The **port enable per-vlan-stats** command enables the collection of per-VLAN statistics. When you use this command, the RS tracks the inbound and outbound frame and octet counts per-port, per-VLAN.

Parameter	Value	Meaning
ports	<port-list>	Specifies the port(s) on which you are enabling the collection of per-VLAN statistics (see Section 1.4, "<port-list> Syntax.").

Restrictions

Can be used only with 10/100 and Gigabit Ethernet ports set up as 802.1Q trunk ports.



Note This command can become memory-intensive if enabled on an RS with many different layer-2 flows. Also, as the number of table entries increase, there is a linear decrease in the flow learning rate. As a result, this feature should be enabled on a highly conservative basis. For example, only on VLAN trunk ports where there is multiple VLAN traffic on a port.

Example

To enable per-VLAN statistics on port **et.1.3**:

```
rs(config)# port enable per-vlan-stats ports et.1.3
```


port enable wdm ports

Mode

Configure

Format

port enable wdm ports *<port-list>*

Description

The **port enable wdm ports** command enables the functioning of Wave Division Multiplexing (WDM) ports. .

Parameter	Value	Meaning
ports	<i><port-list></i>	Specifies the WDM port(s) to enable (see Section 1.4, "<port-list> Syntax.").

Restrictions

Can be used only with WDM ports.

Example

To enable WDM port **gi.1.3**:

```
rs(config)# port enable wdm ports gi.1.3
```

port flow-bridging

Mode

Configure

Format

```
port flow-bridging <port-list> | all-ports
```

Description

The **port flow-bridging** command changes the specified ports from using address-based bridging to using flow-based bridging. Ports use only one type of bridging at a time.

Each port has an L2 lookup table where MAC address or flows are stored:

- If the port is configured for address-based bridging (default), each L2 table entry consists of a MAC address and a VLAN ID.
- If the port is configured for flow-based bridging, each L2 table entry consists of a source MAC address, a destination MAC address, and a VLAN ID.

Suppose that a port on the RS is connected to a hub that is connected to three workstations, A, B, and C. If each workstation is talking to one another and sending broadcast traffic, the L2 table on the RS's port would contain the following entries for the workstations. Assume that the VLAN ID is "1" for all entries.

If the ports are configured for address-based bridging:

- MAC address A
- MAC address B
- MAC address C
- MAC broadcast address

If the ports are configured for flow-based bridging:

- MAC addresses A->B
- MAC addresses A->C
- MAC addresses B->A
- MAC addresses B->C
- MAC addresses C->A
- MAC addresses C->B
- MAC addresses A->broadcast
- MAC addresses B->broadcast
- MAC addresses C->broadcast

Parameter	Value	Meaning
flow-bridging	<port-list>	Specifies the ports to change to flow-based bridging (see Section 1.4, "<port-list> Syntax.").
	all-ports	The keyword all-ports changes all the ports on the RS to flow-based bridging.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Examples

To configure Ethernet port **et.3.7** for flow-based bridging:

```
rs(config)# port flow-bridging et.3.7
```

port loopback

Mode

Enable

Format

Channelized T1 interfaces:

```
port loopback <port-list> local|network-line|network-payload|niu-remote-line-fdl-ansi|
niu-remote-line-inband|remote-line-inband|remote-payload-fdl-ansi|remote-line-fdl-ansi
|remote-line-fdl-bellcore|none
```

Channelized E1 interfaces:

```
port loopback <port-list> local|network-line|network-payload|none
```

Channelized T3 interfaces:

```
port loopback <port-list> local|network-line|niu-remote-line-fdl-ansi|
niu-remote-line-inband|none
```

Clear Channel T3 interfaces only:

```
port loopback <port-list> local|network-line|remote-line-feac|none
```

Clear Channel E3 interfaces only:

```
port loopback <port-list> local|network-line|none
```

E3 interfaces only:

```
port loopback <port-list> local
port loopback <port-list> network-line
port loopback <port-list> none
```

Description

The **port loopback** command is used for network diagnosis. A line is put into loopback and then some form of testing performed – for example BERT or ‘ping’. Due to the low-level nature of this function, there are different forms for each type of interface.

The following parameters are common to all interfaces:

Parameter	Value	Meaning
loopback	<port-list>	The port(s) that are to be placed in the specified loopback mode (see Section 1.4 , "<port-list> Syntax.").
none		Disable loopbacks on the specified port(s).

For Channelized T1 interfaces:

Parameter	Value	Meaning
local		Loops the router output data back toward the router at the T1 framer level and sends an AIS signal out toward the network.
network-line		Loops the data back to the network before the T1 framer and automatically sets a local loopback at the HDLC controllers.
network-payload		Loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers.
niu-remote-line-fdl-ansi		Sends a T1 loopup code to the Network Interface Unit (NIU)/SmartJack, per the ANSI T1.403 Specification. Uses the repeating, 16-bit ESF data link code word (0001001011111111) to request the NIU to enter into a network loopback. The T1 line must be in ESF framing mode.
niu-remote-line-inband		Sends a T1 loopup code to the remote Network Interface Unit (NIU)/SmartJack. Uses a 5 bit inband code (11000), to request the NIU to enter into a network loopback. The line must be in ESF framing mode.
remote-payload-fdl-ansi remote-line-fdl-ansi remote-line-fdl-bellcore		Sends a repeating, 16-bit ESF data link code word (00001110 11111111) to the remote end requesting that it enter into a network line loopback. Specify the ansi keyword to enable the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, per the ANSI T1.403 Specification. Specify the bellcore keyword to enable the remote SmartJack loopback on the T1 channel, per the TR-TSY-000312 Specification.
remote-line-inband		Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.

For Channelized E1 interfaces:

Parameter	Value	Meaning
local		Loops the router output data back toward the router at the E1 framer level and sends an AIS signal out toward the network.

Parameter	Value	Meaning
network-line		Loops the data back to the network before the E1 framer and automatically sets a local loopback at the HDLC controllers.
network-payload		Loops the payload data back toward the network at the E1 framer and automatically sets a local loopback at the HDLC controllers.

For Channelized T3 interfaces:

Parameter	Value	Meaning
local		Loops the data back toward the router and sends an AIS signal out toward the network.
network-line		Network line loopback loops the data back toward the network (before the framer).
niu-remote-line-fdl-ansi †		Sends a T1 loopup code to the Network Interface Unit (NIU)/SmartJack, per the ANSI T1.403 Specification. Uses the repeating, 16-bit ESF data link code word (0001001011111111) to request the NIU to enter into a network loopback. The T1 line must be in ESF framing mode.
niu-remote-line-inband †		Sends a T1 loopup code to the remote Network Interface Unit (NIU)/SmartJack. Uses a 5 bit inband code (11000), to request the NIU to enter into a network loopback. The line must be in ESF framing mode.

† These apply only to T1 lines within the Channelized T3 port (for example, **t3.2.1:1**).

For Clear Channel T3 interfaces:

Parameter	Value	Meaning
local		Loops the data back toward the router and sends an AIS signal out toward the network.
network-line		Network line loopback loops the data back toward the network (before the framer).
remote-line-feac remote-line-feac-none		A loopback request to the far end device that uses the C-bit field in the T3 frame to loop the entire T3 line. This option is only supported on T3 lines that are in C-bit parity mode.

For Clear Channel E3 interfaces:

Parameter	Value	Meaning
local		Loops the data back toward the router and sends an AIS signal out toward the network.
network-line		Network line loopback loops the data back toward the network (before the framer).

Restrictions

This command applies to Channelized T1, E1 and T3 ports, and Clear Channel T3 and E3 ports.

These loopback modes are specific to particular interfaces. The following parameters are available on a Channelized T1 interface only if ESF framing is in use:

remote-payload-fdl-ansi
remote-line-fdl-ansi
remote-line-fdl-bellcore

Examples

To put the third T1 in slot 7 in a network line loopback:

```
rs# port loopback t1.7.3 network-line
```

port set

Mode

Configure

Format

Ethernet interfaces:

```
port set <port-list>|all-ports [auto-negotiation on|off] [auto-negotiation-speed 10Mbps|
100Mbps|10_100Mbps] [auto-negotiation-duplex half|full|both] [duplex full|half]
[hash-mode m0|m1|m2|m3|m-auto] [ifg <number>] [input-encapsulation forced-ethernet_ii]
[speed 10Mbps|100Mbps]
```

Gigabit Ethernet interfaces:

```
port set <port-list>|all-ports [auto-negotiation on|off] [auto-negotiation-flowctl off|
asymmetric|symmetric|both] [hash-mode m0|m1|m2|m3|m-auto] [ifg <number>] [link-timer
<number>] [mtu <number>]
```

ATM T1, E1 and T3 interfaces:

```
port set <port-list>|all-ports [hash-mode m0|m1|m2|m3|m-auto] [mtu <number>]
[transmit-clock-source local|loop] [framing cbit-parity|m23|esf|g832|g751]
```

Clear Channel T3

```
port set <port-list>[wan-encapsulation ppp|frame-relay|cisco-hdlc] [cablelength <number>]
[clock-source internal|loop] [crc 16-bit|32-bit] [framing cbit-parity|m23] [invert-data]
[scrambling-mode enable|disable]
```

Clear Channel E3

```
port set <port-list>[wan-encapsulation ppp|frame-relay|cisco-hdlc] [ifg <number>]
[cablelength <number>] [clock-source internal|loop] [crc 16-bit|32-bit] [framing
g832|g751] [invert-data] [scrambling-mode enable|disable][national-bits 1|0]
```

HSSI interfaces:

```
port set <port-list>|all-ports [clock <clock-source>] [hash-mode m0|m1|m2|m3|m-auto]
[speed <number>] [wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

POS interfaces:

```
port set <port-list>|all-ports [hash-mode m0|m1|m2|m3|m-auto] [mtu <number>]
[mc-vlan-encap <number>]
```

Serial interfaces:

```
port set <port-list>|all-ports [speed <number>] [hash-mode m0|m1|m2|m3|m-auto]
[wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

Description

The parameters you can set with the **port set** command depend on the media type of the port.



Note By default, all ports use autosensing to detect the operating mode and speed of the network segment to which they are connected. If you use this command to set a port parameter, the setting disables autosensing for that parameter on the port. For example, if you set the speed of a segment to 10-Mbps, that segment no longer uses autosensing for the port speed and will always attempt to operate at 10-Mbps.

Parameter	Value	Meaning
set	<port-list>	Specifies the ports (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword applies the settings you select to all the relevant ports.
duplex		Sets the operating mode. This option is valid for 10/100 Mbps ethernet only.
	full	Set the operating mode to full duplex.
	half	Set the operating mode to half duplex.
speed		Sets the port speed to 10-Mbps or 100-Mbps, or to a specified value.
	10Mbps	Set the port speed to 10-Mbps.
	100Mbps	Set the port speed to 100-Mbps.
	<number>	A value in the range 1 to 51840000 bps.
auto-negotiation		Turns on or off auto-negotiation for Gigabit ethernet ports. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.
	on	Turns on auto-negotiation.
	off	Turns off auto-negotiation.
auto-negotiation-speed		Sets the auto-negotiation speed on a fast ethernet port.
	10Mbps	Sets the auto-negotiation line speed capability to 10Mbits/sec.
	100Mbps	Sets the auto-negotiation line speed capability to 100Mbits/sec.
	10_100Mbps	Sets the auto-negotiation line speed capability to 10Mbits/sec and 100Mbits/sec.
auto-negotiation-duplex		Sets the auto-negotiation duplex mode on a fast ethernet port.

Parameter	Value	Meaning
	half	Sets the auto-negotiation duplex mode to half-duplex.
	full	Sets the auto-negotiation duplex mode to full-duplex.
	both	Sets the auto-negotiation duplex mode to half-duplex and full-duplex.
auto-negotiation-flowctl		Sets the flow-control on a full-duplex Gigabit ethernet port.
	off	Clears the flow-control capability advertised by the port.
	asymmetric	Sets the flow-control capability advertised to asymmetric pause.
	symmetric	Sets the flow-control capability advertised to symmetric pause.
	both	Sets the flow-control capability advertised to asymmetric and symmetric pause.
hash-mode		Sets the Layer 2 hash mode for this port. This hash mode defines the algorithm scheme that will be used to calculate the hash value used for the Layer 2 and Layer 3 lookup table. The 48 bit MAC address is hashed into 8 bit groupings, represented by either B5, B4, B3, B2, B1, or B0. Assuming a MAC address of the value B5B4:B3B2:B1B0, the following describes the various hash modes and the resulting MAC address format.
	m0	B5B4:B3B2:B1B0
	m1	B5B4:B3B2:B0B1
	m2	B5B4:B2B3:B1B0 (default hash mode)
	m3	B4B5:B3B2:B1B0
	m-auto	Auto-hashing periodically queries the L2 or L3 tables for hash bucket overflow on a port. If the number of overflows exceed a certain threshold level, auto-hashing will automatically change the hash mode for that port. Eventually a <i>best</i> hash mode for the particular traffic will be found, which will provide optimal distribution across the L2 or L3 lookup table.

Parameter	Value	Meaning
wan-encapsulation		Sets the encapsulation for the WAN port to frame-relay, ppp or cisco-hdlc. See Section 1.5, "Use of wan-encapsulation." for details on the use of wan-encapsulation.
	frame-relay	Sets the encapsulation to Frame-Relay.
	ppp	Sets the encapsulation to PPP.
	cisco-hdlc	Sets the encapsulation to Cisco HDLC.
ifg	<number>	Changes the Interframe Gap (IFG) for the port by the amount specified by <number>. The <number> is a delta value in 40-nanosecond units for the IFG. The possible values for <number> are -12 through 64.
mtu	<number>	Sets the Maximum Transmit Unit (MTU) for the port by the amount specified by <number>. The MTU is a factor in negotiating PPP connections, and is important for interoperability between multi-vendor networks. Possible values for <number> are 64 through 65535. The default value is 1522. This parameter is not valid for ethernet ports.
mc-vlan-encap	<number>	Transmits packet VLAN encapsulation on a 802.1Q trunk port that cannot replicate a packet to multiple VLANs on this port. Possible values for <number> are 0 through 4095. This parameter is not valid for ethernet ports.
input-encapsulation	forced-ethernet_ii	Changes the interpretation of the input MAC encapsulation to Ethernet II.
link-timer	<number>	Sets the auto-negotiation link timer to the number of milliseconds specified by <number>. <number> is a value between 0 and 20. This option is valid for Gigabit ports only.
clock		Sets the clock source. This parameter is applicable only when the wan-encapsulation parameter is specified for a HSSI port that will be connected back-to-back with a HSSI port on another router.
	external-clock	External transmit clock (DCE provided).
	internal-clock-51mh	Internal transmit clock at 51.84 Mhz.
	internal-clock-25mh	Internal transmit clock at 25.92 Mhz.
	external-rx-clock	External receive clock for transmit clocking.
transmit-clock-source		Sets the ATM port transmit clock source.

Parameter	Value	Meaning
	local	Selects the onboard crystal oscillator as the clock source. This is the default value.
	loop	Selects the receiver inputs as the clock source.
framing		Specifies the type of framing used by the ATM port, which can be one of the following:
	cbit-parity ¹	Valid for T3 only.
	m23 ¹	Valid for T3 only.
	esf ¹	Valid for T1 only.
	g832 ¹	Valid for E3 only.
	g751 ¹	Valid for E3 only.

¹ For Channelized T1, E1 and T3 ports, and Clear Channel T3 and E3 ports, see the separate description for “port set framing” on page 49-42.

Restrictions

This command applies to Ethernet, Gigabit Ethernet, ATM, HSSI, POS and Serial ports.

- For 10/100 Mbps Ethernet, you must set both the operating mode and the speed. You cannot set one without setting the other.
- For Gigabit Ethernet, you can only turn on or off auto-negotiation. You cannot set the speed or duplex for Gigabit modules.
- The **speed** parameter is currently used on WAN ports to inform the software of the speed of the interface. However, this information is known for CSU/DSU-based interfaces. Consequently, the **port set speed** command is not used for Channelized T1, E1, and T3 ports, and Clear Channel T3 and E3 ports.

Examples

To configure port **et.1.5** to 10 Mbps and half duplex:

```
rs(config)# port set et.1.5 speed 10mbps duplex half
```

To turn off auto-negotiation for the Gigabit port **gi.4.2**:

```
rs(config)# port set gi.4.2 auto-negotiation off
```

To set the Layer 2 hash mode for all ports to the **m0** hash algorithm:

```
rs(config)# port set all-ports hash-mode m0
```

To set the speed for a HSSI PPPWAN port located on port 1 of slot 3:

```
rs(config)# port set hs.3.1 wan-encapsulation ppp speed 45000000
```

To set an internal clock source (25.92 Mhz) for a HSSI PPPWAN port located on port 1 of slot 3:

```
rs(config)# port set hs.3.1 wan-encapsulation ppp speed 45000000 clock  
internal-clock-25mh
```

To set the speed for a serial Frame RelayWAN port located at port 4 of slot 2, VC 100:

```
rs(config)# port set se.2.4.100 wan-encapsulation frame-relay speed  
1500000
```

To increase the Interframe Gap for port **et.1.1** by 400 nanoseconds (10 * 40ns):

```
rs(config)# port set ifg et.1.1 ifg 10
```

port set cablelength

Mode

Configure

Format

```
port set <port-list> cablelength <length> [wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

Description

For T1 interfaces, the **port set cablelength** command is used to configure the short-haul mode of operation (also known as the DSU mode) and the length of the cable used. The default **cablelength** for T1 interfaces is 133 feet.

For T3 interfaces, this **port set cablelength** command is used to configure the length of the cable used. The default **cablelength** for T3 interfaces is 244 feet.

For Clear Channel T3 and E3 interfaces, the default is 244 feet.

Parameter	Value	Meaning
set	<port-list>	Sets port parameters for the specified port(s) (see Section 1.4 , "<port-list> Syntax.").
cablelength	<length>	The length (in feet) of the cable connecting the T1/T3 interface to the telecommunications network terminating equipment. For Channelized T1, this is a value in the range 1 to 5000 feet; the default is 224 feet. For channelized T3 and Clear Channel T3/E3 interfaces, this is a value in the range 1 to 450 feet. The default is 224 feet.

Restrictions

The **port set cablelength** command is only supported for Channelized T1 and Channelized T3 physical interfaces (that is, t1.*.*, no channel permitted, and t3.*.*, no T1 channel permitted), and Clear Channel T3 and E3 interfaces.

For T1 interfaces, the **port set cablelength** command is mutually exclusive with the **port set lbo** command. Any ports that have not had the long-haul cable characteristics nor the cable length explicitly configured will use a default cable length of 133 feet.

Examples

To specify a 50 foot cable on the second T3 interface in slot 10:

```
rs(config)# port set t3.10.2 cablelength 50
```

port set clock-source

Mode

Configure

Format

```
port set <port-list> clock-source {internal|loop} [wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

Description

The **port set clock-source** command is used to select local or network clock sources for the transmit interface. Usually, the network clock is used for interfaces as these are more accurate than the internal clock. For back-to-back operation, at least one RS must be configured for **internal** timing. Use of the **internal** clock when connected to the public telephone network may result in network *slips* and loss of *data-unreliable* network operation.

For back-to-back operation, at least one end must be configured for **internal** timing.

Use of the **internal** clock when connected to the public telephone network may result in network ‘slips’ and loss of data/ unreliable network operation.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
clock-source		Used to set the transmit timing source.
	internal	Use the free-running clock generated internally to the module for the transmit interface.
	loop	Use the clock recovered from the receiver for the transmit interface. This is the default for Channelized T1 and E1 interfaces and for Channelized T3 interfaces, Clear Channel T3/E3 interfaces.

Restrictions

This command applies to Channelized T1, Channelized E1, or Channelized T3 ports, or a Clear Channel T3 or E3 interface. That is, port-types: t1.*.*, e1.*.*, t3.*.*[*] and e3.*.*.



Note T1 channels within a Channelized T3 are separately clocked.

Examples

To select the network (loop timing) for the fourth T1 interface in slot 3:

```
rs(config)# port set t1.3.4 clock-source loop
```


port set crc

Mode

Configure

Format

```
port set <port-list> crc {16-bit | 32-bit} [wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

Description

This command is used to select the use of either the 16 or 32 bit CRCs, as specified in ISO 3309, for Channelized T1, E1 or T3 interfaces, or a Clear Channel T3 or E3 interface. Most equipment uses 16 bit CRCs. However, for links that use large-length packets, or are likely to have burst errors longer than 16 bits, the 32-bit CRC may be a better choice.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
crc		Used to set the datalink CRC type.
	16-bit	Use the 16-bit CRC. This is the default.
	32-bit	Use the 32-bit CRC.

Restrictions

This command applies to Channelized T1, Channelized E1 or Channelized T3, or a Clear Channel T3 or E3 ports.

There is no automatic negotiation of this parameter. Consequently, both ends of the link must be configured to use the same CRC algorithm. Failure to do this will result in no communication between the nodes.

Examples

To set the fourth T1 within the third T3 in slot 12 to use a 32-bit CRC:

```
rs(config)# port set t3.12.3:4 crc 32-bit
```

port set fdl

Mode

Configure

Format

```
port set <port-list> fdl {ansi | bellcore | none}
```

Description

This command is used to enable the one-second generation and processing of performance reports using the FDL on a T1 link configured for ESF.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
fdl		Used to set the FDL parameters for T1 links using ESF framing.
	ansi	The FDL messages are generated and processed according to the ANSI-T1.403. This is the default.
	bellcore	The FDL messages are generated and processed using the AT&T PUB 54016 message format.
	none	No performance parameters are generated or processed by the RS.

Restrictions

- The FDL is only available on T1 links using ESF framing.
- The ports listed in <port-list> must refer to a complete Channelized T1 stream, either a physical port (t1.*.*), or a T1 channel within a Channelized T3 port (t3.*.*.*).

Examples

To enable ANSI messages on the first T1 in slot 7:

```
rs(config)# port set t1.7.1 fdl ansi
```



Note The channel number is not required. This command applies to the whole T1 stream.

To enable AT&T messages on the 20th T1 in the fourth T3 in slot 11:

```
rs(config)# port set t3.11.4:20 fdl bellcore
```

port set framing

Mode

Configure

Format

Channelized T1 interfaces:

```
port set <port-list> framing sf|esf|sf-japan|esf-japan|{none wan-encapsulation  
frame-relay|ppp| cisco-hdlc}
```

Channelized E1 interfaces:

```
port set <port-list> framing crc4|nocrc4|none {wan-encapsulation frame-relay|ppp|  
cisco-hdlc}
```

Channelized T3 and Clear Channel T3 interfaces:

```
port set <port-list> framing c-bit|m23 [wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

Clear Channel E3 interfaces:

```
port set <port-list> framing g751|g832 [wan-encapsulation frame-relay|ppp|cisco-hdlc]
```

Description

The **port set framing** command is used to select the framing format on a Channelized T1, E1 or T3 interface, or Clear Channel T3 or E3 port. There are different qualifiers to the parameter for Channelized T1, E1, and T3 and Clear Channel T3 and E3 lines.

The **port set framing none** command is used to select no framing on a port. That is, the line is used as a continuous bit-stream. There is no structure to the data, and it is not possible to extract multiple bit-streams.



Note If you use the **framing none** command, you must also include **wan-encapsulation <type>** with the command.

For Channelized T1 and E1 ports, specifying **port set <port-list> framing none** allows the use of the port without channelization. (That is, the port(s) specified in <port-list> do not need a ‘:<channel>’ added to the port name.) When other framing types are used for Channelized T1 and E1 ports, a set of channels is implicitly created for use in **port set <port-list>** commands. So, after a **port set t1.3.2 framing none** command, it is illegal to specify a port as **t1.3.2:1**, for example. However, after any other **port set <port-list> framing** command, the channelized form must be used to refer to individual data pipes. (Note that commands that refer to the whole Channelized T1 or Channelized E1 port never use a channel specifier.)



Note The commands that refer to the whole Channelized T1 or Channelized E1 port never use a channel specifier.

For Channelized T3 ports, all the T1/E1 channels are always implicitly created, since **framing none** is not supported.

For each of the interfaces:

Parameter	Value	Meaning
set	<i><port-list></i>	The list of ports to which the command is to be applied (see Section 1.4, "<port-list> Syntax.").
wan-encapsulation		Sets the encapsulation for the WAN port to frame-relay, ppp or cisco-hdlc. See Section 1.5, "Use of wan-encapsulation." for details on the use of wan-encapsulation . This is mandatory if you specify framing none on Channelized T1 and E1 interfaces.
	frame-relay	Frame Relay encapsulation.
	ppp	PPP encapsulation.
	cisco-hdlc	Cisco HDLC encapsulation

For Channelized T1 interfaces only:

Parameter	Value	Meaning
framing		Specifies the type of framing to use for Channelized T1.
	sf	Select the SuperFrame (SF) format, also known as D4.
	esf	Select the Extended SuperFrame (ESF) format. This is the default for Channelized T1 ports, and T1 streams within Channelized T3 ports.
	sf-japan	Select the Japanese variant of the SuperFrame (SF) format.
	esf-japan	Select the Japanese variant of the Extended SuperFrame format.
	none	No framing is used on the port, and no performance parameters are generated or processed by the T1 links. Ports configured in this way are also known as unframed or unstructured. The interface is treated as a continuous stream of bits, with no delimiter. T1 ports configured in this mode cannot support any channelization.

For Channelized E1 interfaces only:

Parameter	Value	Meaning
framing		Specifies the type of framing to use for Channelized E1.
	crc4	Select the CRC4 format for E1, as specified in G.704. This is the default for Channelized E1 ports.

Parameter	Value	Meaning
	nocrc4	Do not use the CRC4 framing. When nocrc4 is specified, you can set the <i>Si</i> bits in the frame using the port set <port-list> international-bits command.
	none	No framing is used on the port, and no performance parameters are generated or processed by the E1 links. Ports configured in this way are also known as unframed or unstructured. The interface is treated as a continuous stream of bits, with no delimiter. E1 ports configured in this mode cannot support any channelization.

For Channelized T3 and Clear Channel T3 interfaces:

Parameter	Value	Meaning
framing		Specifies the type of framing to use for Channelized T3 and Clear Channel T3.
	c-bit	Select C-bit parity framing. This is the default.
	m23	Select M23, also known as asynchronous framing.

For Clear Channel E3 interfaces only:

Parameter	Value	Meaning
framing		Specifies the type of framing to use for Clear Channel E3.
	g751	Select g751 framing. This is the default.
	g832	Select g832 framing.

Restrictions

- This command applies to Channelized T1, Channelized E1 and Channelized T3 ports, or Clear Channel T3 and E3 ports.
- The ports listed in *<port-list>* must refer to a Channelized T3 interface, a complete T1 or E1 pipe (a physical T1 or E1 port), a T1/E1 channel within a Channelized T3 port, or a Clear Channel T3/E3 pipe.
- **port set framing none** is not supported on the Channelized T3 interface, or on a T1/E1 channel in a Channelized T3 interface.

Examples

To set the third T3 in the second slot to use M23 framing:

```
rs(config)# port set t3.2.3 framing m23
```

To set the 15th T1 in the above T3 to use SF framing:

```
rs(config)# port set t3.2.3:15 framing sf
```

To set the first Channelized E1 port in the third slot to be unstructured:

```
rs(config)# port set e1.3.1 framing none wan-encapsulation ppp
```

port set idle-code

Mode
Configure

Format

port set <port-list> **idle-code** <value>

Description

Sets the value to be used in unassigned timeslots within a Channelized T1 or E1 frame.

Often a carrier specifies that unused timeslots within a Channelized T1 or E1 frame must be filled with a specific pattern. Use the **port set** <port-list> **idle-code** <value> to configure this pattern.

For a port configured for 56Kbps operation (see **port set** <port-list> **speed-56** command), the least significant 7 bits of the value are used as the idle code.

In most cases, the carrier either doesn't care, or requires that the timeslots be filled with an all-ones pattern (the default).

Parameter	Value	Meaning
set	<port-list>	Sets the idle-code for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
idle-code	<value>	A decimal or hexadecimal number, whose value is placed in each unused timeslot of the specified port. Hexadecimal values should be specified in the standard C style, 0xnn. The default value is 0xff .

Restrictions

- The **port set idle-code** command applies to Channelized T1, Channelized E1 and Channelized T3 ports.
- The ports listed in <port-list> must refer to a complete Channelized T1 or E1 pipe, either a physical port or a Channelized T1 or E1 channel within a Channelized T3 port (that is, t1.*.*, e1.*.* and t3.*.*.*).



Note For a Multi-rate WAN module, the port number is ignored and any idle code specified is applied to all four ports. However, you must still specify a port number.

Examples

To set the third T1 port in slot 6 to use an idle-code of 0x55:

```
rs(config)# port set t1.6.3 idle-code 0x55
```

To set the 12th T1 in the second T3 in slot 14 to 0xAA:

```
rs(config)# port set t3.14.2:12 idle-code 0xAA
```

port set impedance

Mode
Configure

Format

port set <port-list> impedance 75ohm | 120ohm

Description

This command sets the impedance of a port or ports.
The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
impedance		Specify to set the line impedance for an E1 interface. The default is 120 ohms.
	75ohm	Specify to set the line impedance for a 75 ohm unbalanced interface with BNC connectors.
	120ohm	Specify to set the line impedance for a 120 ohm balanced interface with RJ-45 connectors.

Restrictions

- This command applies to Channelized E1 ports only. That is, the port type must be e1.*.* (no channel specifier allowed).
- There is no way for the software to determine the correct interface settings. Incorrect settings will probably result in greater packet loss, or at worst no communication.

Examples

To set the line impedance on the fourth Channelized E1 port in slot 5 to 75ohm unbalanced:

```
rs(config)# port set e1.5.4 impedance 75ohm
```

port set international-bits

Mode

Configure

Format

```
port set <port-list> international-bits 0 | 1
```

Description

This command sets the international (Si) bits in the G.704 frame for E1 streams.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
international-bits		Use this option to set the Si bit. The default is 1 for nocrc4 framing.
	0	Sets the Si bit to 0.
	1	Sets the Si bit to 1.

Restrictions

- This command only applies to framed E1 streams on a physical E1 port – physical E1 interfaces (e1.*.* – no channel specifier allowed).
- The international/Si bits are only available when the Channelized E1 is configured for **nocrc4** operation. (See **set port <port-list> framing** command.)

Examples

To set the international bits to zero on the first Channelized E1 port in slot 2:

```
rs(config)# port set e1.2.1 international-bits 0
```

port set invert-data

Mode
Configure

Format

port set <port-list> invert-data

Description

The **port set invert-data** command is a method of ensuring ones-density when using communications links that don't provide any other alternative. For example, 64kbps timeslots on a T1 link that don't support B8ZS (see **port set line-coding**). Because HDLC always guarantees to transmit a zero at least once in every seven bits, inverting the data results in a one at least once in every seven bits.



Note Both ends of the datalink must support (and be configured for) this mode of operation – there is no way to negotiate this.

If inverted data is no longer required, you must negate this command.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
invert-data		Used to set HDLC data to be inverted on the line. The default is not to invert the data.

Restrictions

This command applies to Channelized T1, Channelized E1 and Channelized T3 ports, or Clear Channel T3 or E3 ports.

Examples

To set the 10th channel in the second T1 in slot 5 to use inverted data:

```
rs(config)# port set t1.5.2:10 invert-data
```

port set lbo

Mode

Configure

Format

```
port set <port-list> lbo {0db | -7.5db | -15db | -22.5db}
```

Description

The **port set lbo** command is used to configure the line build-out for the T1 interface when operating in the long-haul mode (also known as the CSU mode).

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
lbo		Used to configure the long-haul cable characteristics for a Channelized T1 interface.
	0db	0 dB line loss.
	-7.5db	-7.5 dB line loss.
	-15db	-15 dB line loss.
	-22.5db	-22.5 dB line loss.

Restrictions

- The **port set lbo** command is only supported for T1 physical interfaces (that is, t1.*.*, no channel permitted).
- The **port set lbo** command is mutually exclusive with the **port set cablelength** command. Any ports that have not had the long-haul cable characteristics nor the cable length configurations applied use a default cable length of 133 feet.

Examples

To set a line build-out of -7.5db on the third T1 in slot 12:

```
rs(config)# port set t1.12.3 lbo -7.5db
```

port set line-coding

Mode

Configure

Format

```
port set <port-list> line-coding {ami|b8zs|hdb3}
```

Description

The **port set line-coding** command is used to set the line coding for a T1 or E1 interface. (T3 and E3 interfaces only support one type of line coding, B3ZS). The **port set line-coding** command is already used by the ATM interface on the RS.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
line-coding		Select the line encoding for T1 and E1 physical lines and T1/E1 channels within a T3 port.
	ami	This is the simplest form of line encoding, and can be selected for both T1 and E1 ports. It does not provide any mechanism for enforcing the (required) minimum number of ones on a line. This format is not often used today.
	b8zs	This is the default line encoding for T1 lines and Clear Channel and channelized T3. It provides the adequate <i>ones-density</i> requirements. This encoding is not supported on E1 lines.
	hdb3	This is the default line encoding for E1 lines and Clear Channel E3. It provides the adequate ones-density requirements. This encoding is not supported on T1 lines.

Restrictions

- The **port set line-coding** command is only supported on Channelized T1, Channelized E1 and Channelized T3 ports.
- The ports listed in <port-list> must refer to a complete Channelized T1 or Channelized E1 pipe, either a physical port or a Channelized T1/E1 channel within a Channelized T3 port.

Examples

To set the line coding to AMI on the first T1 in slot 11:

```
rs(config)# port set t1.11.1 line-coding ami
```

port set national-bits

Mode

Configure

Format

For Channelized E1 interfaces:

```
port set <port-list> national-bits <num/hex>
```

For Clear Channel E3 interfaces:

```
port set <port-list> national-bits 1|0 [wan-encapsulation frame-relay|ppp| cisco-hdlc]
```

Description

This command is used to set the ‘national’ (*Sa*) bits (*Sa4* through *Sa8* bits) in time-slot 0 of the G.704 frame for a Channelized E1 stream, or to enable national bits in a Clear Channel E3 stream.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
national-bits	<num/hex>	- Use <i>num</i> to set the value using a decimal number. The range is 0 to 31. - Use <i>hex</i> to set the value using a hexadecimal number. The range is 0x00 to 0x1f. When this number is converted to binary, the most significant bit is <i>Sa4</i>, and the least significant bit is <i>Sa8</i>. The default is 0x1f, all national bits set to 1.
1 0		Enables or disables national bits in a Clear Channel E3 stream. The default is 0 = disabled; 1 = enabled.

Restrictions

This command applies to framed E1 streams on physical Channelized E1 ports only – physical E1 interfaces (e1.*.* - no channel specifier allowed), or a Clear Channel E3 stream.

Examples

To set the national bits to 0x15 on the third Channelized E1 in slot 9:

```
rs(config)# port set e1.9.3 national-bits 0x15
```


port set remote-loopback-enable

Mode

Configure

Format

```
port set <port-list> remote-loopback-enable {enable | disable} [wan-encapsulation  
frame-relay|ppp|cisco-hdlc]
```

Description

The **port set remote-loopback-enable** command specifies that the T1 port enters the loopback mode when it receives a loopback code on the line. This parameter does not effect loopbacks activated using the FDL capability of the ESF frame.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
remote-loopback-enable		Used to allow remote loopback requests.
	enable	Processes remote-loopback-inband requests initiated from the remote side. This is the default.
	disable	Ignores remote-loopback-inband requests initiated from the remote side.

Restrictions

- The **port set remote-loopback-enable** command is only available on Channelized T1 ports and Clear Channel T3 ports.
- For Channelized T1, the ports listed in <port-list> must refer to a complete T1 stream, either a physical port (t1.*.*) or a T1 channel within a Channelized T3 port (t3.*.*).

Examples

To enable remote payload loopbacks on the 11th T1 stream within the third T3 of slot 6:

```
rs(config)# port set t3.6.3:11 remote-loopback-enable enable
```

port set scrambling-mode

Mode
Configure

Format

port set <port-list> scrambling-mode enabled|disabled [wan-encapsulation frame-relay|ppp|cisco-hdlc]

Description

The **port set scrambling-mode** command ensure that inadvertent user codes do not cause alarm or loop up conditions Clear Channel T3/E3 equipment.



Caution If you want to use scrambling, then you must enable scrambling at both ends of the link, otherwise all data will be lost.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
scrambling-mode		Used to ensure that inadvertent user codes do not cause alarm or loop up conditions on Fiber SDH equipment.
	enabled	Data is scrambled and then unscrambled.
	disabled	Data is not scrambled. This is the default.

Restrictions

The **port set scrambling-mode** command is available only on Clear Channel T3 and E3 links.

Examples

To enable scrambling mode on the first T3 of slot 2:

```
rs(config)# port set t3.2.1 scrambling-mode enabled
```

port set speed-56 | speed-64

Mode

Configure

Format

```
port set <port-list> {speed-56 | speed-64}
```

Description

The **port set {speed-56 | speed-64}** command is used to specify the speed of the timeslots within a channel. **speed-56** is usually used when communicating over (or interworking with) a T1 line that does not support clear-channel-capability (CCC). Bit 8 of each octet is not used for data and is forced to a **1**. This is one scheme used to guarantee ones-density.

This command is usually used for communicating over older T1 infrastructure, it is also necessary when interworking with such equipment remotely. For example, across an international link where one side of the link uses older equipment, and the other side uses newer equipment.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the port parameters for the specified port(s) (see Section 1.4, "<port-list> Syntax.").
speed-56		Use only the least significant seven bits of each timeslot.
speed-64		Use all of the bits of each timeslot. This is the default.

Restrictions

- This command applies to Channelized T1, Channelized E1 and Channelized T3 ports.
- The ports listed in <port-list> must refer to a channel within a Channelized T1 or E1 port (t1.*.*:* or e1.*.*:*), or a T1 or E1 line within a Channelized T3 (t3.*.*:*).

Examples

To set the timeslots in the sixth channel of the second T1 in slot 9 for 56kbps operation:

```
rs(config)# port set t1.9.2:6 speed-56
```

port set timeslots

Mode

Configure

Format

```
port set <port-list> timeslots {<start-slot>[-<end-slot>][, ...]} wan-encapsulation  
frame-relay|ppp|cisco-hdlc
```

Description

The **port set timeslots** command is used to select specific timeslots (or a range of timeslots) from a T1 or E1 frame. Timeslots cannot concurrently be used in more than one channel.

The following table describes the parameters of the command.

Parameter	Value	Meaning
set	<port-list>	Sets the timeslots for the specified port(s) (see Section 1.4, "<port-list> Syntax."). For Channelized T1 and E1, a specific channel number must be specified - you cannot enter a range or a wildcard for the channel number. For example t1.3.(1-2):3 is valid, whereas, t1.3.2:(1-4) is invalid. For Channelized T3, normal use of ranges and wildcarding applies.
timeslots		A comma-separated list of timeslots, or range of timeslots.
	<start-slot>	The comma-separated list of timeslots, or start timeslot for the range.
	<end-slot>	(Optional) The end timeslot for the range.
wan-encapsulation		Sets the encapsulation for the WAN port to frame-relay, ppp or cisco-hdlc. See Section 1.5, "Use of wan-encapsulation." for details on the use of wan-encapsulation.
	frame-relay	Sets the encapsulation to Frame Relay.
	ppp	Sets the encapsulation to PPP.
	cisco-hdlc	Sets the encapsulation to Cisco HDLC.



Note The parameter(s) to this command are a comma separated list of timeslot ranges. A timeslot range can be a single timeslot number, or a range of timeslots, separated by a hyphen. Where a range is given, it specifies all time-slots within the two numbers, inclusive.

The one exception is that for Channelized E1, time-slot 16 cannot be specified directly – the **ts16** command must be used and specified with the **timeslots** command.

There is no default for this command. It is mandatory to specify the timeslots for a channel.

Restrictions

- The **port set timeslots** command applies to Channelized T1, Channelized E1 and Channelized T3 ports.
- You must specify all timeslots in the same command line, and you must enter the **wan-encapsulation** *<type>* as part of that command. Therefore, you cannot add timeslots to a port using a second command. If you need to change the timeslot assignment for a port, you must negate the command, and its associated commands, then repeat them using the new timeslot assignment.
- The ports listed in *<port-list>* must refer to a channel within a Channelized T1 or E1 port (t1.*.*:* or e1.*.*:*), or a T1 or E1 line within a Channelized T3 (t3.*.*:*)).

Examples

To specify the timeslots in the 19th T1 link of the second T3 port of slot 12:

```
rs(config)# port set t3.12.2:19 timeslots 1-6,13-18
```

port set ts16

Mode

Configure

Format

```
port set <port-list> ts16 wan-encapsulation frame-relay|ppp|cisco-hdlc
```

Description

The **port set** <port-list> **ts16** command selects the use of timeslot 16 on a framed Channelized E1 interface. Usually, time-slot 16 is used for signalling purposes (either CAS or CCS). Consequently, using a **timeslots** range of **1-17** does *not* select time-slot 16.

The use and restrictions of this command are the same as the **port set** <port-list> **timeslots** command.

The default is that time-slot 16 is *not* used for data.

Parameter	Value	Meaning
set	<port-list>	The list of ports to which the command is to be applied (see Section 1.4, "<port-list> Syntax.").
ts16		Specifies that timeslot 16 is to be used for data.
wan-encapsulation		Sets the encapsulation for the WAN port to frame-relay, ppp or cisco-hdlc. See Section 1.5, "Use of wan-encapsulation." for details on the use of wan-encapsulation.
	frame-relay	Sets the encapsulation to Frame Relay.
	ppp	Sets the encapsulation to PPP.
	cisco-hdlc	Sets the encapsulation to Cisco HDLC.

Restrictions

This command applies to Channelized E1 ports only.

The ports listed in <port-list> must refer to a channel within a Channelized E1 port (**e1.*.*:***).



Note

If you want to use timeslot 16 with other timeslots, you must specify **ts16** in the same command line as the **port set** <port-list> **timeslots** command, and you must enter the **wan-encapsulation** <type> as part of that command. Therefore, you cannot add timeslots to a port using a second command. If you need to change the timeslot assignment for a port, you must negate the command, and its associated commands, then repeat them using the new timeslot assignment.

Examples

To use timeslots 12-18, including timeslot 16 on channel five of the second Channelized E1 interface in slot 7:

```
rs(config)# port set e1.7.2:5 timeslots 12-18 ts16 wan-encapsulation ppp
```

port show 8021p

Mode
Enable

Format

port show 8021p <port-list> | all-ports

Description

The **port show 8021p** command displays whether 802.1p encapsulation is enabled or disabled on a port or list of ports. The 802.1p standard provides the ability to classify traffic into eight priority categories or class of services. This classification scheme is based upon MAC frame information and is used for Quality of Service (QoS) for VLANs. The following table describes the parameters of the command.

Parameter	Value	Meaning
8021p	<port-list>	Specifies the ports for which you want to display the description (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the description for all the RS ports.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To display 802.1p encapsulation status for port **et.2.1**:

rs# port show 8021p et.2.1		
Port	802.1p	Status
----	-----	
et.2.1		Disabled

port show autonegotiation

Mode

Enable

Format

port show autonegotiation *<port-list>* | all-ports

Description

The **port show autonegotiation** command displays auto-negotiation information. This command displays port number, administration status, current status, remote signaling, fault advertised, and fault received.

Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode, and flow control scheme to communicate with each other.

The following table describes the parameters of the command.

Parameter	Value	Meaning
autonegotiation	<i><port-list></i>	Specifies the ports for which you want to display the auto-negotiation information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the auto-negotiation information for all the RS ports.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To display auto-negotiation information for port **et.2.1**:

rs# port show MAU et.2.1						
Admin Port	Current Status	Remote Status	Fault Signalling	Fault Advertised	Received	
-----	-----	-----	-----	-----	-----	
et.2.1	disabled	other	not detected	n/a	n/a	

port show autonegotiation-capabilities

Mode
Enable

Format

port show autonegotiation-capabilities <port-list> | all-ports

Description

The **port show autonegotiation-capabilities** command displays auto-negotiation capabilities. This command displays a list of port capabilities, advertised capabilities, and any received capabilities from another port. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode, and flow control scheme to communicate with each other.

Parameter	Value	Meaning
autonegotiation-capabilities	<port-list>	Specifies the ports for which you want to display the auto-negotiation capabilities (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the auto-negotiation capabilities for all the RS ports.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To display auto-negotiation capabilities for port **et.2.1**:

```
rs# port show autonegotiation-capabilities et.2.1
```

Port	Capability	Advertised	Received
-----	-----	-----	-----
et.2.1	other	other	
	10 baseT	10 baseT	
	10 baseT FD	10 baseT FD	
	100 baseT4	100 baseT4	
	100 baseTX	100 baseTX	
	100 baseTX FD	100 baseTX FD	
	100 baseT2	100 baseT2	
	100 baseT2 FD	100 baseT2 FD	
	Pause	Pause	
	Asymmetric Pause	Asymmetric Pause	
	Symmetric Pause	Symmetric Pause	
	Asym-Sym Pause	Asym-Sym Pause	
	1000 baseX	1000 baseX	
	1000 baseX FD	1000 baseX FD	
	1000 baseT	1000 baseT	
	1000 baseT FD	1000 baseT FD	

port show bmon

Mode
Enable

Format

port show bmon [config] [detail] [port <port list>] [stats]

Description

The **port show bmon** command lets you display broadcast monitoring information for RS ports.
The following table describes the parameters of the command.

Parameter	Value	Meaning
bmon		Displays broadcast monitor information.
	config	Displays configuration information for broadcast monitoring.
	detail	Displays all information for broadcast monitoring.
	port <port list>	Specifies the ports for which you want to display information (see Section 1.4, "<port-list> Syntax.").
	stats	Displays statistics information for broadcast monitoring.

**Note** If no parameters are specified, the current states of all ports are displayed.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To display the state of ports with broadcast monitoring:

```
rs# port show bmon

Port: et.1.1 State: On

Port: et.6.8 State: ShutDn Expire: 39 (sec)

Port: et.7.8 State: On
```

The above example shows three ports, with the port et.6.8 shut down for 39 seconds.

To display broadcast monitoring configuration values set for the ports:

```
rs# port show bmon config

Port: et.1.1 Rate (Kpps): 10 Burst (sec): 1 Shutdown (sec):300
Port: et.6.8 Rate (Kpps): 10 Burst (sec): 5 Shutdown (sec):60
Port: et.7.8 Rate (Kpps): 2 Burst (sec): 2 Shutdown (sec):60
```

In the above example, port **et.1.1** has been configured with default values.

To display broadcast monitoring statistics for the ports:

```
rs# port show bmon stats

Port: et.1.1 Current Broadcast Rate (Kpps): 0.000
Port: et.6.8 Burst at port shutdown (Kpps): 10.032
ShutDn Count: 2
Port: et.7.8 Current Broadcast Rate (Kpps): 0.000
```

In the above example, the current broadcast traffic on **et.1.1** and **et.7.8** is zero. The port **et.6.8** is currently shut down and it shows a burst of 10.032K packets per second at its shut down. This port has been shut down twice because of excessive broadcast traffic.

To show broadcast monitoring details for the ports:

```
rs# port show bmon detail

Port: et.1.1 Rate (Kpps): 10 Burst (sec): 1 Shutdown (sec):300
State: On
Current Broadcast Rate (Kpps): 0.000

Port: et.6.8 Rate (Kpps): 10 Burst (sec): 5 Shutdown (sec):60
State: ShutDn Expire: 39 (sec)
Burst at port shutdown (Kpps): 10.032
ShutDn Count: 2

Port: et.7.8 Rate (Kpps): 2 Burst (sec): 2 Shutdown (sec):60
State: On
Current Broadcast Rate (Kpps): 0.000
```

The above example shows configuration, state, and statistics information.

port show bridging-status

Mode
Enable

Format

port show bridging-status <port-list> | all-ports

Description

The **port show bridging-status** command lets you display bridging-status information for RS ports. The following table describes the parameters of the command.

Parameter	Value	Meaning
bridging-status	<port-list>	Specifies the ports for which you want to display the bridging-status information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the bridging-status information for all the RS ports.

Restrictions

This command applies to all ports, with the exception of ATM and CMTS ports.

Example

To display the bridging status for all available ports:

rs# port show bridging-status all-ports				
Port	Mgmt Status	phy-state	link-state	Bridging Mode
----	-----	-----	-----	-----
et.4.1	No Action	Disabled	Link Down	Address
et.4.2	No Action	Disabled	Link Down	Address
et.4.3	No Action	Forwarding	Link Up	Address
et.4.4	No Action	Disabled	Link Down	Address
et.4.5	No Action	Disabled	Link Down	Address
et.4.6	No Action	Forwarding	Link Up	Address
et.4.7	No Action	Disabled	Link Down	Address
et.4.8	No Action	Disabled	Link Down	Address

port show description

Mode

Enable

Format

port show description <port-list> | all-ports

Description

The **port show description** command lets you display the user defined description for RS ports. The description is defined using the **port description** command.

The following table describes the parameters of the command.

Parameter	Value	Meaning
description	<port-list>	Specifies the ports for which you want to display the description (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the description for all the RS ports.

Restrictions

This command applies to all ports, with the exception of ATM and CMTS ports.

Example

To display the description for all available ports:

rs# port show description et.2.1	
Port Name	Description
-----	-----
et.2.1	vlan1-2

port show dsx-stats

Mode
Enable

Format

port show dsx-stats <port-list> interval <number>

Description

The **port show dsx-stats** command displays accumulated values for error events, performance parameters, and failure states associated with WAN links.

The following table describes the parameters of the command.

Parameter	Value	Meaning
dsx-stats	<port-list>	Specifies the ports for which you want to display the description (see Section 1.4, "<port-list> Syntax.").
	interval	Statistics are collected in 15-minute intervals, and a total of 96 intervals are accumulated (24 hours) before overwriting the collection buffer. The interval parameter allows the statistics to be displayed that were collected during a particular multiple of 15-minute intervals within the last 24 hours. If interval is not specified, statistics are displayed for the latest 15-minute interval.



Note Depending on the interface (T1, E1, T3, or E3), different output parameters are displayed.

Restrictions

Can be used only on channelized WAN ports of type T1/E1 and T3 and Clear Channel T3 and E3.

Example

To display statical values collected for port **t1.2.3** during 32 15-minute intervals (480 minutes),

```
rs# port show dsx-stats t1.2.3 interval 32

Total Data (480 minute interval):
  0 Line Code Violations,    0 Path Code Violations
  0 Slip Secs,    0 Fr Loss Secs,    900 Line Err Secs,    0 Degraded Mins
  0 Errored Secs,    0 Bursty Err Secs,    900 Severely Err Secs,    900 Unavail Secs
```

The following table explains the output of the **port show dsx-stats** command:

Table 49-13Display Field Description

FIELD	DESCRIPTION
Total Data	Number of minutes over which the displayed data was collected.
Line Code Violations	Number of Line Coding Violations (LCV) that have occurred during the specified interval. A Line Coding Violation is either a Bipolar Violation (BPV) or an Excessive Zeroes Error Event (EXZ).
Path Code Violations	Number of Path Coding Violations (PCV) that have occurred during the specified interval. A Path Coding Violation is a frame synchronization bit error in the D4 and E1-noCRC formats or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Number of seconds within the interval in which one or more Controlled Slip (CS) Error Events have occurred. A Controlled Slip Error Event is the replication or deletion of the payload bits of a DS1 frame. A Controlled Slip may occur when there is a difference between the timing of a synchronous receiving terminal and the received signal. A Controlled Slip does not cause an Out of Frame defect.
Fr Loss Secs	Number of seconds within the interval in which one or more Loss of Frame failures have occurred. For T1 links, the Loss of Frame failure is issued when an OOF or LOS defect has persisted for T seconds, where, $2 \leq T \leq 10$. The Loss of Frame is cleared when there have been no OOF or LOS defects during a period of T seconds, where $0 \leq T \leq 20$.
Line Err Secs	Number of seconds within the interval in which one or more Line Coding Violation error events were detected.
Degraded Mins	The number of minutes within the interval in which the estimated error rate exceeds 10^{-6} but does not exceed 10^{-3}. Degraded Minutes are determined by collecting all of the Available Seconds, removing any Severely Errored Seconds, grouping the result in 60-second long groups, and then counting a 60-second long group (1 minute) as degraded if the cumulative errors during that minute exceed 10^{-6}.

Table 49-13 Display Field Description (Continued)

FIELD	DESCRIPTION
Errored Secs	Number of seconds within the interval in which one or more Path Coding Violations, Out of Frame defects, Controlled Slip events, or detected AIS defects have occurred. Errored Seconds (ES) applies to ESF and E1-CRC.
Bursty Err Secs	Number of seconds within the interval with fewer than 320 but more than one Path Coding Violations, no Severely Errored Frame defects, and no detected incoming AIS defects. Controlled Slips are not included within this counter. This parameter is not incremented during an Unavailable Second.
Severely Err Secs	Number of seconds within the interval in which one of the following has occurred: ESF – A second with 320 or more Path Coding Violations, one or more Out of Frame defects, or a detected AIS defect. E1-CRC – A second with 832 or more Path Coding Violations or one or more Out of Frame defects. E1-noCRC – A second with 2,048 or more Line Coding Violations. D4 – A second with Framing Error events, OOF defects, or 1,544 or more Line Coding Violations. Controlled Slips are not included in this parameter, and the counter is not incremented during Unavailable Seconds.
Unavail Secs	Number of seconds within the interval in which the interface is unavailable. A DS1 interface is said to be unavailable from the onset of ten contiguous SESs or the onset of a condition leading to a failure. Once unavailable, and no failure is present, the DS1 interface becomes available at the onset of ten contiguous seconds with no SESs. if the failure clearing is less than or equal to 10. With respect to DS1 error counts, all counters are incremented while the DS1 interface is considered available. If the interface is considered unavailable, only the Unavailable Seconds counter is incremented.

Table 49-13 Display Field Description (Continued)

FIELD	DESCRIPTION
C-bit Coding Violations	For C-bit parity DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors occurring in the accumulation interval.
P-bit Errored Seconds	A P-bit Errored Second (PES) is a second with one or more PCVs, one or more Out of Frame defects, or a detected incoming AIS. This is not incremented when UASs are counted.
P-bit Severely Errored Seconds	A P-bit Severely Errored Second (PSES) is a second with 44 or more PCVs, one or more out of frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
C-bit Errored Seconds	A C-bit Errored Second (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This is not incremented when UASs are counted.
C-bit Severely Errored Seconds	A C-bit Severely Errored Second (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This is not incremented when UASs are counted.
P-bit Coding Violations	P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
Severely Errored Framing Second	A Severely Errored Framing Second (SEFS) is a second with one or more out of frame defects or a detected AIS defect.
BIP Coding Violations	For B3ZS (HDB3)-coded signals, is the occurrence of a pulse of the same polarity as the previous pulse without being part of the zero substitution code, B3ZS (HDB3). A bipolar violation error event may also include other error patterns such as: three (four) or more consecutive zeros and incorrect polarity.

port show hash-mode

Mode
Enable

Format

port show hash-mode <port-list> | all-ports

Description

The **port show description** command lets you display the user defined description for RS ports. The description is defined using the **port description** command.

Parameter	Value	Meaning
hash-mode	<port-list>	Specifies the ports for which you want to display the hash mode (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the hash mode for all the RS ports.

Restrictions

This command applies to all ports.

Example

To display the hash mode for all available ports (port **et.1.2** is set to hash mode m3):

```
rs# port show hash-mode all-ports

L2 Port Hash Mode (assume a MAC address = 0011:2233:4455)
-----
Port et.1.1           Mode-2    0011_3322_4455
Port et.1.2           Mode-3    1100_2233_4455
Port et.1.3           Mode-2    0011_3322_4455
Port et.1.4           Mode-2    0011_3322_4455
Port et.1.5           Mode-2    0011_3322_4455
Port et.1.6           Mode-2    0011_3322_4455
Port et.1.7           Mode-2    0011_3322_4455
Port et.1.8           Mode-2    0011_3322_4455
Port t1.2.1           Mode-2    0011_3322_4455
Port t1.2.2           Mode-2    0011_3322_4455
Port t1.2.3           Mode-2    0011_3322_4455
Port t1.2.4           Mode-2    0011_3322_4455
Port t3.3.1           Mode-2    0011_3322_4455
Port t3.3.2           Mode-2    0011_3322_4455
```

port show MAU

Mode
Enable

Format

port show MAU <port-list> | all-ports

Description

The **port show MAU** command displays Media Access Control (MAC) information. This command displays

- Port number
- Media and default media type
- Jack type
- Operational status
- Support level.

The following table describes the parameters of the command.

Parameter	Value	Meaning
MAU	<port-list>	Specifies the ports for which you want to display the MAC information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the MAC information for all the RS ports.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To display MAC information for port **et.2.1**:

rs# port show MAU et.2.1						
Port	MUA Type	Default Type	Jack Type	Status	Supported	
-----	-----	-----	-----	-----	---	
et.2.1	100 BaseFX HD	100 BaseFX HD	fiber SC	operational	no	

port show MAU-statistics

Mode
Enable

Format

port show MAU-statistics <port-list> | all-ports

Description

The **port show MAU-statistics** command displays Media Access Control (MAC) statistics. This command displays:

- Port number
- Media availability
- Media availability state exits totals
- Jabber (excessively long frames) state
- Jabbering state enters totals
- False carriers totals

The following table describes the parameters of the command.

Parameter	Value	Meaning
MAU-statistics	<port-list>	Specifies the ports for which you want to display the MAC statistics (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the MAC statistics for all the RS ports.

Restrictions

This command applies to Ethernet and Gigabit Ethernet ports only.

Example

To display MAC statistics for port **et.2.1**:

rs# port show MAU-statistics et.2.1						
Media Avail.	Jabber	Jabbering	False			
Port	Media Avail.	State Exits	State	State	Enters	Carriers
-----	-----	-----	-----	-----	-----	-----
et.2.1	not available	0	other	0		0

port show mirroring-status

Mode

Enable

Format

```
port show mirroring-status <port> | all-ports | all-acls
```

Description

The **port show mirroring-status** command shows the following port mirroring status information for the specified ports:

- Port mirroring enable/disable
- Mirrored ports
- Mirroring mode

The following table describes the parameters of the command.

Parameter	Value	Meaning
mirroring-status	<port>	Specifies the ports for which you want to display port mirroring status (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays port mirroring status for all the ports.
	all-acls	The all-acls keyword displays port mirroring status for all the flow mirroring rules.

Restrictions

This command applies to Ethernet, Gigabit Ethernet, HSSI and Serial ports only.

Examples

To display the port mirroring status for port **gi.2.2**:

rs# port show mirroring-status gi.2.2		
Target Port	Monitor Port	Monitor Index
-----	-----	-----
gi.2.2	gi.2.1	4128

port show mtu

Mode
Enable

Format

port show mtu <port-list>|all-ports

Description

The **port show mtu** command lets you display the MTU for RS ports. The MTU is defined using the **port set mtu** command.

Parameter	Value	Meaning
mtu	<port-list>	Specifies the ports for which you want to display the MTU (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the MTU for all the RS ports.

Restrictions

None.

Example

To display the MTU for all available ports:

rs# port show mtu all-ports		
	MTU	MRU
gi.1.1	1500	1500
gi.1.2	1500	1500
se.2.1	1500	1500
se.2.2	1500	1500
se.2.3	1500	1500
se.2.4	1500	1500

port show per-vlan-stats

Mode

Enable

Format

```
port show per-vlan-stats [port <port> {vid <number> | vlan <string>}] [vid <number> port <port>] [vlan <string> port <port>]
```

Description

Use the **port show per-vlan-stats** command to display the amount of inbound and outbound layer-2 traffic (in terms of octets and frames) passing through a particular port belonging to a VLAN.

Parameter	Value	Meaning
port	<port>	Specifies the port for which statistics are displayed (see Section 1.4, "<port-list> Syntax."). Individual inbound and outbound counters are displayed for each VLAN for which this port is a member.
vid	<number>	Specifies the VLAN by ID number for which statistics on a particular port within that VLAN are displayed.
vlan	<string>	Specifies the VLAN by name for which statistics on a particular port within that VLAN are displayed.

Restrictions

Available only for VLANs consisting of 10/100 and Gigabit Ethernet ports.

Port within VLAN from which statistics are gathered must first be enabled to collect statistics by using the **port enable per-vlan-stats** command.

This feature does not display statistics for VLANs that are in L4 Bridging mode. Additionally, if a VLAN is moved in and out of L4 Bridging mode while **per-vlan-stats** is enabled on any of its ports, the statistics for those ports may be inaccurate

Example

The following example displays statistics for port et.11.4:

```
rs# port show per-vlan-stats vlan vlan11 port et.11.2
Traffic Statistics for Port et.11.2, VLAN vlan11 (VLAN ID 2):
Inbound
  Octets:                1,872 octets
  Frames:                 24 frames

Outbound
  Octets:                2,864 octets
  Frames:                 38 frames
```

The output of the command displays the inbound and outbound octets and frames for port **et.11.2**, which belongs to VLAN **vlan11**.

In the following example, information is displayed for each VLAN for which port **et.10.4** is a member:

```
RS# port show per-vlan-stats port et.10.4
Traffic Statistics for Port et.10.4, VLAN red (VLAN ID 2):
Inbound
  Octets:                107,196,271 octets
  Frames:                 134,940 frames

Outbound
  Octets:                105,965,469 octets
  Frames:                 133,549 frames

Traffic Statistics for Port et.10.4, VLAN blue (VLAN ID 3):
Inbound
  Octets:                354,072,575 octets
  Frames:                 446,763 frames

Outbound
  Octets:                347,463,892 octets
  Frames:                 435,218 frames

Traffic Statistics for Port et.10.4, VLAN green (VLAN ID 4):
Inbound
  Octets:                104,199,749 octets
  Frames:                 130,972 frames

Outbound
  Octets:                103,111,034 octets
  Frames:                 129,616 frames

RS#
```

port show phy-errors

Mode

Enable

Format

```
port show phy-errors <port list> | all-ports [interval <seconds>]
```

Description

The **port show phy-errors** command measures and displays potential physical layer errors. You can use this command to relate a performance issue on a network segment with a possible physical problem on that segment.

The following table describes the parameters of the command.

Parameter	Value	Meaning
phy-errors	<port list>	Specifies the ports for which you want potential physical layer errors shown (see Section 1.4, "<port-list> Syntax.").
	all-ports	Specify all-ports to display physical layer errors for all ports.
interval	<seconds>	Specifies the interval, in seconds, for the measurement of errors. Specify a value between 1-10. The default is 1 second.

This command returns the same information as the **statistics show phy-errors** command.

Restrictions

You *cannot* use this command to show physical layer errors for WAN ports or ports on the following line cards:

- POS OC-12
- ATM OC-12
- Serial line cards
- CMTS line cards

This command provides a reasonable estimate of potential degradation problems with the physical medium and is not intended to be a substitute for bit error rate testing of the physical line.

Example

To display potential physical layer errors for the port **et.2.1**:

```
rs# port show phy-errors et.2.1

Port: et.2.1
-----
Physical Error Stats
-----
RX frames Okay                100
Correlated Layer 1 Errors      10
Average bytes per frame        64
Errors gathered since 2000-11-01 11:22:4
Error stats cleared 2000-11-01 11:12:4
```

The display shows:

- The number of frames successfully received.
- The number of *suspected* physical layer errors.
- The average number of bytes per frame.
- The time when error statistics measurement and collection began and the time when the statistics were last cleared with the **port clear phy-errors** command.

port show port-status

Mode

Enable

Format

```
port show port-status <port-list/SmartTRUNK-list> | all-ports | all-SmartTRUNKs
```

Description

The **port show port-status** command lets you display port-status information for RS ports or SmartTRUNKs. The following table describes the parameters of the command.

Parameter	Value	Meaning
port-status	<port-list/SmartTRUNK-list>	Specifies the LAN/WAN ports or SmartTRUNKs for which you want to display status information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the description for all the RS ports.
	all-SmartTRUNKs	The all-SmartTRUNKs keyword displays information for all SmartTRUNKs.

Restrictions

This command does not show Virtual Circuit (VC) information. To see the state of sub-interfaces, you need to use the appropriate facility command, such as the **frame-relay show stats** command.

Example

To display the port status for all ports on an Ethernet line card in slot 1:

```
rs# port show port-status et.1.*
```

Flags: M - Mirroring enabled S - SmartTRUNK port

Port	Port Type	Duplex	Speed	Negotiation	Link State	Admin State	Flags
----	-----	-----	-----	-----	-----	-----	-----
et.1.1	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.2	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.3	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.4	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.5	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.6	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.7	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	
et.1.8	10/100-Mbit Ethernet	Half	10 Mbits	Manual	Up	Up	

port show pvst-info

Mode

Enable

Format

```
port show pvst-info <port-list> | all-ports spanning-tree <string>
```

Description

The **port show pvst-info** command lets you display spanning tree information for a particular spanning tree. The following table describes the parameters of the command.

Parameter	Value	Meaning
pvst-info	<port-list>	Specifies the ports for which you want to display Spanning-Tree information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the Spanning-Tree information for all the RS ports.
spanning-tree	<string>	Specifies the name of the spanning tree for which you want to display information.

Restrictions

This command applies to all ports, with the exception of ATM and CMTS ports.

Example

To display the spanning tree information for spanning tree **stp1** on port **et.2.1**:

rs# port show pvst-info et.2.1 spanning-tree stp1						
Port	Priority	Cost	STP	State	Designated-Bridge	Designated Port
----	-----	----	---	----	-----	-----
et.2.1	000	00100	Enabled	Learning	8000:000306030600	0 001

port show serial-link-info

Mode
Enable

Format

```
port show serial-link-info <port-list> | all-ports [brief|all]
```

Description

The **port show serial-link-info** command displays the Channelized T1, E1 and T3 line settings, including the channel configuration where applicable. It also displays the HSSI, Serial and Clear Channel T3 and E3 line settings.



Note For Channelized ports, use the asterisk (*) as a wild character to request the display of all the channels, if any, that are configured on the specified physical line (for example, t1.2.3:*)).

Parameter	Value	Meaning
serial-link-info	<port-list>	The list of ports to which the command is to be applied (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the line settings for all the RS ports.
brief		Displays a reduced set of the information fields described in Table 49-14 . Specifically, only those fields indicated with †. This is the default.
all		Displays the entire set of the information fields described in Table 49-14 . If you are running BERT tests, then you must use this keyword to view the results.

Restrictions

This command applies to the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3
- Clear Channel T3 and Clear Channel E3

Examples

To display the full information for logical channel 1 of the second Channelized T1 link in slot 4:

```
rs# port show serial-link-info t1.4.2:1 all
T1 Slot 4 Port 2:      Channelized
  Module Revision:      1.0
  T1 WIC Version:       1.0
  LB0:                  -7.5db
  Clock source:         Loop
  Framing:              ESF
  Line coding:          B8ZS
  Loopback:             none
  Idle code:            0xff (255)
  FDL enable:           ANSI
  Remote loopback enable: enabled
  BERT state:           Stopped
  BERT status:          no sync
  BERT start time:      Mon Oct 16 09:59:27 2000
  BERT end time:        Mon Oct 16 09:59:27 2000
  BERT time remaining:  00H 00M 00S
  BERT pattern:         2^20-QRSS
  BERT interval (minutes): 60
  BERT sync count:      0
  BERT total errors:     0
  BERT total mb:        0
  BERT errors since sync: 0
  BERT kb since sync:   0
Total Data (Last 24 hour interval):
  0 Line Code Violations,  0 Path Code Violations
  0 Slip Secs,  0 Fr Loss Secs,  0 Line Err Secs,  0 Degraded Mins
  0 Errored Secs,  0 Bursty Err Secs,  0 Severely Err Secs,
0 Unavail Secs
Total Data (Last 15 minute interval):
  0 Line Code Violations,  0 Path Code Violations
  0 Slip Secs,  0 Fr Loss Secs,  0 Line Err Secs,  0 Degraded Mins
  0 Errored Secs,  0 Bursty Err Secs,  0 Severely Err Secs,
0 Unavail Secs
Data in current interval (0 Seconds Elapsed):
  0 Line Code Violations,  0 Path Code Violations
  0 Slip Secs,  0 Fr Loss Secs,  0 Line Err Secs,  0 Degraded Mins
  0 Errored Secs,  0 Bursty Err Secs,  0 Severely Err Secs,
0 Unavail Secs
Channel 1:              Up
  CRC:                  16-Bit
  Invert data:          Not invert data
  Timeslot speed:       56Kbps
  Timeslot(s) selected: 1-24
  Alarm state:          No alarms detected
```

To display brief information for logical channel 1 of the first Channelized E1 link in slot 3:

```
rs# port show serial-link-info e1.3.1:1 brief
E1 Slot 3 Port 1:      Channelized
Module Revision:      1.0
E1 WIC Version:       1.0
Impedance:            120ohm
Clock source:         Loop
Framing:              CRC4
Line coding:          HDB3.
Loopback:             none
Idle code:            0xff (255).
National (Sa) bits:   0x1f (31)
Channel 1:            Up
CRC:                  16-Bit.
Invert data:          Not invert data.
Timeslot speed:       64Kbps
Timeslot(s) selected: 1-5,ts16
Alarm state:          Receiver has loss of signal
```

Table 49-14 describes the fields displayed by the **port show serial-link-info** command.



Note Only those fields indicated with † are displayed when the **brief** parameter is used

Table 49-14 Display Field Descriptions

FIELD	DESCRIPTION
XX Slot <slot> Port <port> : <port-state> †	Identifies the interface (where XX is T1, E1 or T3 or E3, <slot> is the slot number and <port> is the port number). The <port-state> is: - Channelized, for ports with framing. - One of the following, for Channelized ports with no framing (that is, framing none), or Clear Channel T3 or E3 ports: - Up - Down - Administratively down - Locally looped - Remotely looped - Network looped
Module Revision: †	The revision number of the module.
XX WIC Version: †	The WIC version number (where XX is T1, E1, T3 or E3). This applies only to a Multi-rate WAN module.

Table 49-14Display Field Descriptions (Continued)

FIELD	DESCRIPTION
Channel <i><number></i> : <i><state></i> †	Identifies the number (<i><number></i>) of the channel and indicates the channel state (<i><state></i>). The possible channel states are: • Up • Down • Administratively down • Locally looped • Remotely looped • Network looped
Alarm state: †	Any alarms detected by the line controller. The possible alarms that can be reported are: • Transmitter is sending remote alarm • Transmitter is sending AIS • Receiver has loss of signal • Receiver is getting AIS • Receiver has loss of frame • Receiver has remote alarm • Receiver has no alarms • No alarms detected

Table 49-14Display Field Descriptions (Continued)

FIELD	DESCRIPTION
Framing: †	The possible framing types according to the line type are: • for Channelized T1: - SF - ESF - SF-Japan - ESF-Japan - None • for Channelized E1: - CRC4 - CRC4: interworking OK This means that CRC4 framing is being both transmitted and received correctly. - CRC4: interworking with no-CRC4 This means that CRC4 framing is being transmitted, but is interworking with the other end that is not using CRC4 framing (see <i>G.706, Annex B</i>). - NOCRC4 - None • for Channelized T3: - CBIT - M23
Framing: (continued)	• for Clear Channel T3: - CBIT - M23 • for Clear Channel E3: - G751 - G832

Table 49-14 Display Field Descriptions (Continued)

FIELD	DESCRIPTION
Line coding: †	The possible line coding types according to the line type are: • for Channelized T1: - AMI - Channelized B8ZS • for Channelized E1: - AMI - HDB3 • for Channelized T3: - B3ZS • for Clear Channel T3: - B3ZS • for Clear Channel E3: - HDB3
CRC: †	The possible CRC values are: • 16-bit • 32-bit
Clock source: †	The possible clock sources for the line are: • Internal • Loop
Cable length: †	This applies only to a short-haul T1 line or a T3 line. The value is displayed in feet.
LBO: †	This applies only to a long haul T1 line. The possible values are: • 0db • -7.5db • -15db • -22.5db
Idle code: †	This value is displayed in both hex and decimal.
Impedance: †	This field is only specific to an E1 line. The possible values are: • 75 ohm (unbalanced) • 120 ohm (balanced)
Invert data: †	This only applies to communication links for which there is no other alternative of ensuring ones-density. For example, when a 64K DS0 in a T1 line does not support B8ZS framing. The possible values are: • Invert data • Not invert data

Table 49-14Display Field Descriptions (Continued)

FIELD	DESCRIPTION
National (Sa) bits: †	For Channelized E1 interfaces the possible values are 0 to 31 displayed in both hex and decimal. For Clear Channel E3 enabled or disabled is displayed
International (Si) bits: †	For Channelized E1 interfaces, international-bits is only displayed if the E1 framing is set to NOCRC4.
Timeslot speed: †	This displays the speed of the timeslots within a channel. The possible values are: • 56Kbps • 64Kbps.
Timeslot(s) selected: †	This displays the timeslot(s) selected in the form of <i>start-slot[-end-slot][,...]</i> This applies only to channelized lines. Note that for E1 interfaces, timeslot 16 is displayed as ts16.
Loopback: †	For Channelized T1 interfaces which include DS1 streams in a Channelized T3 trunk the possible values are: • Local • Network-line • Network-payload • Remote-line-fdl ansi • Remote-line-fdl bellcore • Remote-line-inband • Remote-payload-fdl-ansi • None For Channelized E1 interfaces the possible values are: • Local • Network-line • Network-payload • None

Table 49-14 Display Field Descriptions (Continued)

FIELD	DESCRIPTION
Loopback: (continued)	For Channelized T3 interfaces the possible values are: • Local • Network-line • Network-payload • Remote • None For Clear Channel T3 interfaces the possible values are: • Local • Network-line • Remote-line-feac • None For Clear Channel E3 interfaces the possible values are: • Local • Network-line • None
Remote loopback receive: †	For Channelized T1 or Clear Channel T3 interfaces, indicates whether or not to process remote-loopback-inband requests initiated from the remote side.
Scrambling Mode: (Clear Channel T3 and E3)	Indicates whether or not scrambling mode is enabled: • Scrambling Enabled • Scrambling Disabled
BERT state: †	The possible states of the BERT testing feature are: • Running • Stopped
BERT pattern:	The selected BERT pattern, which is displayed if BERT testing is enabled. The possible values are: • 0s • 1s • 2^11 • 2^15 • 2^20-0153 • 2^20-QRSS • 2^23 • alt-0-1

Table 49-14 Display Field Descriptions (Continued)

FIELD	DESCRIPTION
The following information is displayed if BERT testing is enabled.	
BERT status:	• Test status, that is Sync or No Sync.
BERT start time:	• BERT testing start time.
BERT end time:	• BERT testing end time if BERT testing is finished otherwise displays running.
BERT sync count:	• Number of times the sync pattern from No Sync to Sync has been detected.
BERT interval (minutes):	• BERT test duration in minutes.
BERT time remaining:	• Time remaining on the BERT test in minutes.
BERT total errors:	• Number of bit errors encountered since the start of the BERT test.
BERT total mb:	• Number of Mbits received including errored bits since the start of the BERT test.
BERT errors since sync:	• Number of bit errors since the last sync pattern was detected.
BERT kb since sync:	• Number of Kbits received including errored bits since the last sync pattern was detected.
FDL enable: †	FDL is only available on Channelized T1 links using ESF framing. The possible values are: • ANSI • Bellcore • None
FEAC code received is	Denotes whether or not a FEAC code is being received. The possible values are: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpts. Failures (NSA) • No code is being received.

Table 49-14 Display Field Descriptions (Continued)

FIELD	DESCRIPTION
Data in current interval (XX seconds elapsed)	Displays the current accumulation period which is a value in the range 1 to 900 seconds in four intervals. In addition, the current 24-hour accumulation period as well as the previous 15-minute accumulation period is displayed. Consequently, up to 96 15-minute accumulation periods can be kept. The 24-hour accumulation period is implemented as a First In Last Out (FILO) buffer. As such, when the FILO is full the next 15-minute accumulation period becomes the 1st entry in the buffer thereby requiring all the other entries to shift one entry which results in the last entry (that is, the oldest 15-minute accumulation period) being discarded.
Line Code Violations (Channelized T1, E1 and T3)	Line Code Violations (LCV) reflects a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs). A BPV error event for an AMI-coded signal is the occurrence of a pulse of the same polarity as the previous pulse. A BPV error event for a B8ZS- or HDB3- coded signal is the occurrence of a pulse of the same polarity as the previous pulse without being a part of the zero substitution code. An Excessive Zeroes error event for an AMI coded signal is the occurrence of more than fifteen contiguous zeroes. For a B8ZS coded signal, the defect occurs when more than seven contiguous zeroes are detected. For E1 with AMI line coding, line code violations exclude Excessive Zeroes.
Path Coding Violations (Channelized T1 and E1 only)	A Path Coding Violation (PCV) error event is a frame synchronization bit error in the SF and E1-noCRC formats, or a CRC or frame synchronization bit error in the ESF and E1-CRC formats.
Framing Loss Seconds (Channelized T1 only)	A Framing Loss Seconds indicates the number of seconds an out of frame error is detected.
Line Errored Seconds (Channelized T1, E1 and T3)	A Line Errored Seconds (LES) is a second in which one or more code violations occurred or one or more LOS defects.
Controlled Slip Seconds (Channelized T1 and E1 only)	A Controlled Slip Second (CSS) is a one-second interval containing one or more controlled slips. This is not incremented during an Unavailable Second. A Controlled Slip (CS) is the replication or deletion of the payload bits of a DS1 frame. A Controlled Slip may be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal. A Controlled Slip does not cause an Out of Frame defect.
Errored Seconds (Channelized T1, E1 only)	For ESF and E1-CRC links an Errored Second (ES) is a second with one or more Path Code Violation OR one or more Out of Frame defects OR one or more Controlled Slip events OR a detected AIS defect. For SF and E1-noCRC links, the presence of Bipolar Violations also triggers an Errored Second. This is not incremented during an Unavailable Second.
Bursty Errored Seconds (Channelized T1 only)	A Bursty Errored Second (BES) is a second with fewer than 320 and more than 1 Path Coding Violation error events, no Severely Errored Frame defects and no detected incoming AIS defects. Controlled slips are not included in this parameter. This is not incremented during an Unavailable Second. It applies to ESF signals only.

Table 49-14 Display Field Descriptions (Continued)

FIELD	DESCRIPTION
Severely Errored Seconds (Channelized T1, E1 only)	A Severely Errored Second (SES) for ESF signals is a second with 320 or more Path Code Violation Error Events OR one or more Out of Frame defects OR a detected AIS defect. For E1 CRC signals, a Severely Errored Second is a second with 832 or more Path Code Violation error events OR one or more Out of Frame defects. For E1-noCRC signals, a Severely Errored Second is a 2048 LCVs or more. For SF signals, a Severely Errored Second is a count of one-second intervals with Framing Error events, or an OOF defect, or 1544 LCVs or more. Controlled slips are not included in this parameter. This is not incremented during an Unavailable Second.
Degraded Minutes (Channelized T1, E1 only)	A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information refer to RFC-2495.
P-bit Coding Violations (T3 only)	For a DS3, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violations (Channelized T3 only)	For C-bit parity DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors occurring in the accumulation interval.
P-bit Errored Seconds (Channelized T3 only)	A P-bit Errored Second (PES) is a second with one or more PCVs OR one or more Out of Frame defects OR a detected incoming AIS. This gauge is not incremented when UASs are counted.
P-bit Severely Errored Seconds (Channelized T3 only)	A P-bit Severely Errored Second (PSES) is a second with 44 or more PCVs, one or more out of frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Errored Framing Second (Channelized T3 only)	A Severely Errored Framing Second (SEFS) is a second with one or more out of frame defects or a detected AIS defect.
Unavailable Seconds (Channelized T3 only)	Unavailable Seconds (UAS) are calculated by counting the number of seconds that the interface is unavailable. For more information, refer to RFCs 2495 and 2496.
C-bit Errored Seconds (Channelized T3 only)	A C-bit Errored Second (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Seconds (Channelized T3 only)	A C-bit Severely Errored Second (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

port show stp-info

Mode

Enable

Format

port show stp-info *<port-list>* | all-ports

Description

The **port show stp-info** command lets you display spanning tree information for RS ports.

The following table describes the parameters of the command.

Parameter	Value	Meaning
stp-info	<i><port-list/SmartTRUNK-list></i>	Specifies the ports for which you want to display Spanning-Tree information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the Spanning-Tree information for all the RS ports.

Restrictions

None.

Example

To display the spanning tree information for all available ports:

rs# port show stp-info all-ports						
Port	Priority	Cost	STP	State	Designated-Bridge	Designated Port
-----	-----	----	---	-----	-----	-----
et.1.1	128	00100	Enabled	Listening	8000:00e063111111	80 01
et.1.2	128	00100	Enabled	Listening	8000:00e063111111	80 02
et.1.3	128	00100	Enabled	Listening	8000:00e063111111	80 03
et.1.4	128	00100	Enabled	Listening	8000:00e063111111	80 04
et.1.5	128	00100	Enabled	Listening	8000:00e063111111	80 05
et.1.6	128	00100	Enabled	Listening	8000:00e063111111	80 06
et.1.7	128	00100	Enabled	Listening	8000:00e063111111	80 07
et.1.8	128	00100	Enabled	Listening	8000:00e063111111	80 08

port show vlan-info

Mode
Enable

Format

port show vlan-info <port-list> | all-ports

Description

The **port show vlan-info** command lets you display VLAN information about RS ports.

The following table describes the parameters of the command.

Parameter	Value	Meaning
vlan-info	<port-list>	Specifies the ports for which you want to display VLAN information (see Section 1.4, "<port-list> Syntax.").
	all-ports	The all-ports keyword displays the VLAN information for all the RS ports.

Restrictions

None

Example

To display the VLAN information for all available ports:

rs# port show vlan-info all-ports				
Port	Access Type	IP VLANs	IPX VLANs	Bridging VLANs
-----	-----	-----	-----	-----
et.4.1	access	DEFAULT	DEFAULT	DEFAULT
et.4.2	access	DEFAULT	DEFAULT	DEFAULT
et.4.3	access	DEFAULT	DEFAULT	DEFAULT
et.4.4	access	DEFAULT	DEFAULT	DEFAULT
et.4.5	access	DEFAULT	DEFAULT	DEFAULT
et.4.6	access	DEFAULT	DEFAULT	DEFAULT
et.4.7	access	DEFAULT	DEFAULT	DEFAULT
et.4.8	access	DEFAULT	DEFAULT	DEFAULT

port testport

Mode

Configure

Format

```
port testport <port-list> {monitor | break-out} [line-coding {ami | b8zs|hdb3}]
```

Description

The **port testport** command is used to configure the testports on the Channelized T3 interface. This command is supported only on the RS 32000 and RS 38000.

The following table describes the parameters of the command.

Parameter	Value	Meaning
testport	<port-list>	The list of ports to which the command is to be applied (see Section 1.4, "<port-list> Syntax.").
monitor		In this mode, an external analyzer may be connected to the test port allowing transparent monitoring of data on the specified T1/E1 channel.
break-out		In this mode, the specified T1/E1 channel will be removed from service which allows for external test equipment to verify the operation of the specified T1/E1 channel. This mode is mainly intended for support of external BERT equipment.
line-coding		This specifies the line coding for the T1 line. This parameter is identical to the port set <port-list> line-coding command, including defaults. You can specify one of the following keywords:
	ami	Alternate Mark Inversion
	b8zs	Bipolar 8 Zero Substitution
	hdb3	High Density Bipolar 3

Restrictions

This command is supported only on the RS 32000 and RS 38000, and only on Channelized T3 ports, and is not supported on the RS 8000/8600.

Examples

To set the cable length to 50 feet for the first T3 test port of slot 2:

```
rs(config)# port testport t3.2.1 line-coding b8zs
```


50 PORT MIRRORING COMMAND

port mirroring

Mode

Configure

Format

```
port mirroring monitor-port <port number> target-port <port number>|target-profile <acl name>
```

Description

The **port mirroring** command allows you to monitor via a single port the activity of a port on an RS or the traffic that is specified by an ACL.

Parameter	Value	Meaning
monitor-port	<port number>	The port you will use to monitor activity.
target-port	<port number>	The port for which you want to monitor activity. You can specify any single port.
target-profile	<acl name>	The name of the ACL that specifies the profile of the traffic that you want to monitor. The ACL must be a previously created IP ACL. The ACL may contain either permit or deny keywords. The port mirroring command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS.

Restrictions

Only one target port may be defined for a given RS, and only one monitor port may be defined. Also, Riverstone recommends that you monitor Gigabit ports through other Gigabit ports—you would almost certainly experience speed-inconsistency-related problems monitoring a Gigabit port through a 10Base-T or 100Base-TX port.

Known Problems

- Packets that are lost due to CRC and BUFFER_OVERFLOW errors are not mirrored to the monitor-port.
- In the example below, routed packets from source A to destination B on link 2 are seen as leaving src mac of RS when port 1.2 is being monitored.



Examples

To mirror traffic on ethernet ports et.2.2 to port et1.2:

```
rs(config)# port mirroring monitor-port et.1.2 target-port et.2.2
```

After configuring et.1.2 as a monitor-port, et.1.2 is unusable for any other function in the system. This is indicated by a LINK_DOWN message. However, et.1.2 is capable of transmitting TX packets and its LED will be lit while in operation.

To mirror traffic that is specified by the profile in the ACL “101” to port et1.2:

```
rs(config)# port mirroring monitor-port et.1.2 target-profile 101
```


51 PPP COMMANDS

The following commands allow you to define Point-to-Point Protocol (PPP) service profiles, and specify and monitor PPP High-Speed Serial Interface (HSSI) and standard serial ports.

51.1 COMMAND SUMMARY

The following table lists the PPP commands. The sections following the table describe the command syntax.

ppp add-to-mlp <i><mlp></i> port <i><port list></i>
ppp apply service <i><service name></i> ports <i><port list></i>
ppp clear stats-counter [packet-drop-qdepth-counter] [max-packet-enqueued-counter] [packet-drop-red-counter] [rmon] ports <i><port list></i>
ppp create-mlp <i><mlp list></i> slot <i><number></i>
ppp define service <i><service name></i> [bridging enable disable] [high-priority-queue-depth <i><number></i>] [ip enable disable] [ipx enable disable] [lcp-echo on off] [lcp-magic on off] [low-priority-queue-depth <i><number></i>] [max-configure <i><number></i>] [max-failure <i><number></i>] [max-terminate <i><number></i>] [med-priority-queue-depth <i><number></i>] [red on off] [red-maxTh-high-prio-traffic <i><number></i>] [red-maxTh-low-prio-traffic <i><number></i>] [red-maxTh-med-prio-traffic <i><number></i>] [red-minTh-high-prio-traffic <i><number></i>] [red-minTh-low-prio-traffic <i><number></i>] [red-minTh-med-prio-traffic <i><number></i>] [retry-interval <i><number></i>] [rmon on off] [iso enable disable]
ppp restart lcp-ncp ports <i><port list></i>
ppp set mlp-encaps-format ports <i><port list></i> [format short-format]
ppp set mlp-frag-size ports <i><port list></i> [size <i><size></i>]
ppp set mlp-fragq-depth ports <i><port list></i> qdepth <i><number-of-packets></i>
ppp set mlp-orderq-depth ports <i><port list></i> qdepth <i><number-of-packets></i>
ppp set mlp-preserv-pkt-order ports <i><port list></i>
ppp set payload-compress [max-histories 0 1] [type stac] ports <i><port list></i>

ppp set payload-encrypt [type des-bis] transmit-key <key> receive-key <key> ports <port list>
ppp set peer-addr <IP address> <IPX address> ports <port>
ppp set ppp-encaps-bgd ports <port list>
ppp show mlp <mlp list> all-ports
ppp show service <service name> all
ppp show stats port <port> [bridge-ncp] [ip-ncp] [osi-ncp] [link-status] [summary]

ppp add-to-mlp

Mode

Configure

Format

ppp add-to-mlp *<mlp>* **port** *<port list>*

Description

The **ppp add-to-mlp** command adds one or more PPP ports to a previously defined MLP bundle.

Parameter	Value	Meaning
add-to-mlp	<i><mlp></i>	The name of the previously defined MLP bundle.
port	<i><port list></i>	The WAN port(s) you want to add to the MLP bundle.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

MLP bundles cannot be created across multiple line cards.

Example

To add the port “hs.3.1” to the MLP bundle “mp.1”:

```
rs(config)# ppp add-to-mlp mp.1 port hs.3.1
```

ppp apply service

Mode

Configure

Format

ppp apply service *<service name>* **ports** *<port list>*

Description

Issuing the **ppp apply service ports** command applies a previously defined service profile to a given PPP WAN port.

Parameter	Value	Meaning
service	<i><service name></i>	The name of the previously defined service you apply to the given port(s) or interfaces.
ports	<i><port list></i>	The port(s) to which you apply the pre-defined service profile. You can specify a single port or a comma-separated list of ports.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To apply the service “s1” to slot 2, serial ports 1 and 2:

```
rs(config)# ppp apply service s1 ports se.2.1,se.2.2
```

ppp clear stats-counter

Mode

Enable

Format

```
ppp clear stats-counter [packet-drop-qdepth-counter] [max-packet-enqueued-counter]
[packet-drop-red-counter] [rmon] ports <port list>
```

Description

The **ppp clear stats-counter** command specifies a statistic counter to reset to zero. There are statistic counters on each PPP WAN and channelized T1/T3 port. Use the **ppp clear stats-counter** to clear the counter for individual WAN ports or for a group of ports.

Parameter	Value	Meaning
packet-drop-qdepth-counter		Specify this optional parameter to reset the frame drop counter to zero
max-packet-enqueued-counter		Specify this optional parameter to reset the max enqueuedframes counter to zero.
packet-drop-red-counter		Specify this optional parameter to reset the packet drop counter to zero.
rmon		Specify this optional parameter to reset the rmon counter to zero.
ports	<port list>	The WAN port(s) to be cleared.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To clear the frame drop counter to zero on WAN port hs.3.1:

```
rs# ppp clear frame-drop-qdepth-counter ports hs.3.1
```

ppp create-mlp

Mode
Configure

Format

ppp create-mlp *<mlp list>* **slot** *<number>*

Description

The **ppp create-mlp** command creates one or more MLP bundles.

Parameter	Value	Meaning
create-mlp	<i><mlp list></i>	The name(s) of the MLP bundles you want to create. You can specify a single bundle or a comma-separated list of MLP bundles.
slot	<i><number></i>	The slot number for the MLP bundle(s).

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.
MLP bundles cannot be created across multiple line cards.

Example

To create the MLP bundle “mp.1” for slot 1:

```
rs(config)# ppp create-mlp mp.1 slot 1
```

ppp define service

Mode

Configure

Format

```
ppp define service <service name> [bridging enable | disable] [high-priority-queue-depth <number>] [ip enable | disable] [ipx enable | disable] [lcp-echo on | off] [lcp-magic on | off] [low-priority-queue-depth <number>] [max-configure <number>] [max-failure <number>] [max-terminate <number>] [med-priority-queue-depth <number>] [red on | off] [red-maxTh-high-prio-traffic <number>] [red-maxTh-low-prio-traffic <number>] [red-maxTh-med-prio-traffic <number>] [red-minTh-high-prio-traffic <number>] [red-minTh-low-prio-traffic <number>] [red-minTh-med-prio-traffic <number>] [retry-interval <number>] [rmon on | off] [iso enable | disable]
```

Description

The **ppp define service** command specifies the following attributes for a newly created service profile:

- Activate and deactivate bridging, IP, and/or IPX for PPP WAN ports. If you do not specify any bridging, IP, or IPX protocols for PPP WAN ports, they are all activated by default. If you specify a bridging, IP, or IPX protocol, you must also explicitly define the behavior of the other two (i.e., **enabled** or **disabled**).
- The allowable PPP queue depth for high-, low-, and medium-priority items.
- Enable and disable the sending of LCP Echo Request messages. LCP Echo Requests and their corresponding LCP Echo Responses determine if a link to a peer is down.
- Enable and disable the use of LCP magic numbers. Magic numbers are used to help detect loopback conditions.
- The maximum allowable number of unanswered/improperly answered configuration requests before determining that the connection to the peer is lost.
- The maximum allowable number of negative-acknowledgment responses for a given interface before declaring an inability to converge.
- The maximum allowable unacknowledged terminate requests before determining that the peer is unable to respond.
- Activate or deactivate Random Early Discard (RED) for PPP ports.
- The maximum and minimum threshold values for RED high-, low-, and medium-priority traffic.



Note

In general, Riverstone recommends that the maximum threshold values be less than or equal to the respective high-, low-, or medium-priority queue depth. The minimum threshold values should be one-third of the respective maximum threshold.

- The number of seconds that will pass before a subsequent “resending” of the configuration request will be transmitted.
- Activate and deactivate RMON for PPP WAN ports. Before you can view RMON statistics such as ethernet statistics and history for PPP WAN ports, RMON has to be activated.

Parameter	Value	Meaning
service	<i><service name></i>	The name you assign to the newly created service profile.
bridging	enable	Specifying the enable keyword activates bridging for PPP WAN ports.
	disable	Specifying the disable keyword deactivates bridging for PPP WAN ports.
high-priority-queue-depth	<i><number></i>	The number of items allowed in the PPP queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 to 100 item range. The default value is 20.
ip	enable	Specifying the enable keyword activates IP for PPP WAN ports.
	disable	Specifying the disable keyword deactivates IP for PPP WAN ports.
ipx	enable	Specifying the enable keyword activates IPX for PPP WAN ports.
	disable	Specifying the disable keyword deactivates IPX for PPP WAN ports.
lcp-echo	on	Specifying the on keyword enables the sending of LCP Echo Request messages. The sending of LCP Echo Requests is enabled by default.
	off	Specifying the off keyword disables the sending of LCP Echo Request messages.
lcp-magic	on	Specifying the on keyword enables the use of LCP magic numbers.
	off	Specifying the off keyword disables the use of LCP magic numbers. The use of LCP magic numbers is enabled by default.
low-priority-queue-depth	<i><number></i>	The number of items allowed in the PPP queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 to 100 item range. The default value is 20.
max-configure	<i><number></i>	The maximum allowable number of unanswered requests. You can specify any number greater than or equal to 1. The default value is 10.

Parameter	Value	Meaning
max-failure	<i><number></i>	The maximum allowable number of negative-acknowledgment transmissions. You can specify any number greater than or equal to 1. The default value is 5.
max-terminate	<i><number></i>	The maximum allowable number of unanswered or improperly answered connection-termination requests before declaring the link to a peer lost. You can specify any number greater than or equal to 1. The default value is 2.
med-priority-queue-depth	<i><number></i>	The number of items allowed in the PPP queue. You can specify a number between 1 and 65,535. Riverstone recommends a value within the 5 to 100 item range. The default value is 20.
red	on	Specifying the on keyword enables RED for PPP WAN ports.
	off	Specifying the off keyword disables RED for PPP WAN ports.
red-maxTh-high-prio-traffic	<i><number></i>	The maximum allowable threshold for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-maxTh-low-prio-traffic	<i><number></i>	The maximum allowable threshold for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-maxTh-med-prio-traffic	<i><number></i>	The maximum allowable threshold for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.
red-minTh-high-prio-traffic	<i><number></i>	The minimum allowable threshold for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
red-minTh-low-prio-traffic	<i><number></i>	The minimum allowable threshold for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
red-minTh-med-prio-traffic	<i><number></i>	The minimum allowable threshold for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.
retry-interval	<i><number></i>	The number of seconds between subsequent configuration request transmissions (the interval). You can specify any number greater than or equal to 1. The default value is 30.
rmon	on	Specifying the on keyword enables RMON for PPP WAN ports.

Parameter	Value	Meaning
	off	Specifying the off keyword disables RMON for PPP WAN ports.
iso	enable	Use this option to enable the ISO protocol.
	disable	Use this option to disable the ISO protocol.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

Create a service profile named “pppserv4” with the following attributes:

- Bridging enabled
- IP and IPX enabled
- LCP Echo Requests disabled
- LCP magic numbers disabled
- RED disabled
- A retry interval of 20 seconds
- RMON enabled

Enter the following command line in the Configure mode:

```
rs(config)# ppp define service pppserv4 bridging enable ip enable ipx enable  
lcp-echo off lcp-magic off red off retry-interval 20 rmon on
```

ppp restart lcp-ncp

Mode

Enable

Format

ppp restart lcp-ncp ports *<port list>*

Description

The **ppp restart lcp-ncp** command resets and restarts the LCP/NCP negotiation process for PPP WAN and channelized T1/T3 ports.

Parameter	Value	Meaning
ports	<i><port list></i>	The ports on which you re-establish LCP/NCP negotiation.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To restart LCP/NCP negotiation on serial ports 1 and 2 of slot 4:

```
rs# ppp restart lcp-ncp ports se.4.1,se.4.2
```

ppp set mlp-encaps-format

Mode

Configure

Format

ppp set mlp-encaps-format **ports** *<port list>* [**format** **short-format**]

Description

The **ppp set mlp-encaps-format** command specifies the encapsulation format for MLP bundles. If this command is not configured, long format encapsulation is used for MLP bundles.

Parameter	Value	Meaning
ports	<i><port list></i>	The MLP port(s) to which you want to apply the encapsulation format
format	short-format	Specifies the use of short format for MLP encapsulation.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

MLP bundles cannot be created across multiple line cards.

Example

To specify short format encapsulation for the MLP bundles “mp.1” and “mp.4-7”:

```
rs(config)# ppp set mlp-encaps-format ports mp.1,mp.4-7 format  
short-format
```

ppp set mlp-frag-size

Mode

Configure

Format

```
ppp set mlp-frag-size ports <port list> [size <size>]
```

Description

The **ppp set mlp-frag-size** command sets the frame size under which no fragmentation is needed for transmission on the MLP bundle. The default size is 1500 bytes. Any frames that are less than the value set by the **ppp set mlp-frag-size** command are not fragmented. Any frames that are over the value are fragmented for transmission on the MLP bundle.

Parameter	Value	Meaning
ports	<port list>	The MLP port(s) to which the frame size applies.
size	<size>	The size of the frame, in bytes, that is fragmented by MLP. The value can be between 64 and 1500, inclusive. The default value is 1500.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

MLP bundles cannot be created across multiple line cards.

Example

To specify that frames of 200 bytes or more are fragmented on the MLP bundles “mp.1” and “mp.4-7”:

```
rs(config)# ppp set mlp-frag-size ports mp.1,mp.4-7 size 200
```

ppp set mlp-fragq-depth

Mode

Configure

Format

ppp set mlp-fragq-depth **ports** *<port list>* **qdepth** *<number-of-packets>*

Description

The **ppp set mlp-fragq-depth** command sets the depth of the queue used by MLP to hold packet fragments for reassembly.

Parameter	Value	Meaning
ports	<i><port list></i>	The MLP port(s) to which the queue depth applies.
qdepth	<i><number-of-packets></i>	The depth of the queue, in packets, to hold unassembled packet fragments. The value can be between 100 and 4000, inclusive. The default value is 1000.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

MLP bundles cannot be created across multiple line cards.

Example

To specify a queue depth of 2500 packets to hold fragments for reassembly on the MLP bundles “mp.1”:

```
rs(config)# ppp set mlp-fragq-depth ports mp.1 size 2500
```

ppp set mlp-orderq-depth

Mode

Configure

Format

ppp set mlp-orderq-depth **ports** *<port list>* **qdepth** *<number-of-packets>*

Description

The **ppp set mlp-orderq-depth** command sets the depth of the queue used by MLP to hold MLP packets for preserving the packet order.

Parameter	Value	Meaning
ports	<i><port list></i>	The MLP port(s) to which the queue depth applies.
qdepth	<i><number-of-packets></i>	The depth of the queue, in packets, to hold MLP packets. The value can be between 100 and 4000, inclusive. The default value is 1000.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

MLP bundles cannot be created across multiple line cards.

Example

To specify a queue depth of 2500 packets to hold packets for reordering on the MLP bundles “mp.1”:

```
rs(config)# ppp set mlp-orderq-depth ports mp.1 size 2500
```

ppp set mlp-preserv-pkt-order

Mode

Configure

Format

ppp set mlp-preserv-pkt-order ports *<port list>*

Description

The **ppp set mlp-preserv-pkt-order** command enables the MLP module to preserve the packet order.

Parameter	Value	Meaning
ports	<i><port list></i>	The MLP port(s) to which the queue depth applies.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

MLP bundles cannot be created across multiple line cards.

Example

To enable the MLP module to preserve the packet order on the MLP bundles “mp.1”:

```
rs(config)# ppp set mlp-preserv-pkt-order ports mp.1
```


ppp set payload-compress

Mode

Configure

Format

```
ppp set payload-compress [max-histories <number>] [type stac] ports <port list>
```

Description

The **ppp set payload-compress** command enables Stacker payload compression. Enable compression on a single port, an entire multilink PPP (MLP) bundle, or on individual ports that are members of a multilink PPP bundle. If this command is not configured, payload compression is not enabled.

Parameter	Value	Meaning
max-histories	<number>	Specifies the maximum number of compression history buffers to be kept. You can specify either 0 or 1. Specifying 0 disables the keeping of any histories and each packet is individually compressed. Specifying 1 allows a history buffer to be kept, which may result in better compression. The default value is 1.
type stac		Specifies the Stacker (STAC LZS) compression algorithm. This is the default.
ports	<port list>	The port(s) on which you want to enable payload compression. Specify a single port or a comma-separated list of ports.

Restrictions

Usage is restricted to PPP WAN.

MLP bundles cannot be created across multiple line cards.

Example

To enable LZS Stac payload compression on slot 4, on serial port 2:

```
rs(config)# ppp set payload-compress port se.4.2
```

ppp set payload-encrypt

Mode

Configure

Format

ppp set payload-encrypt [**type des-bis**] **transmit-key** <key> **receive-key** <key> **ports** <port list>

Description

The **ppp set payload-encrypt** command enables the encryption of packets using the DES-bis algorithm. Enable encryption on a single port, an entire multilink PPP (MLP) bundle, or on individual ports that are members of an MLP bundle. If this command is not configured, payload encryption is not enabled.

Parameter	Value	Meaning
type	des-bis	Specifies the DES-bis encryption algorithm. This is the default.
transmit-key	<key>	Specifies a 16-digit hexadecimal number for the encoding and decoding of the packets. The keys are themselves encrypted and stored in the active and startup configurations.
receive-key	<key>	Specifies a 16-digit hexadecimal number for the encoding and decoding of the packets. The keys are themselves encrypted and stored in the active and startup configurations.
ports	<port list>	The port(s) on which you want to enable payload encryption. Specify a single port or a comma-separated list of ports.

Restrictions

Usage is restricted to PPP WAN.

MLP bundles cannot be created across multiple line cards.

Example

To enable DES-bis payload encryption on slot 4, on serial port 2:

```
rs(config)# ppp set payload-encrypt transmit-key 0x123456789abcdef0  
receive-key 0xfedcba9876543210 port se.4.2
```

ppp set peer-addr

Mode

Configure

Format

ppp set peer-addr *<IP address>* **ports** *<port>*

Description

Issuing the **ppp set peer-addr** command sets the peer address if it can't be resolved by IPCP or IPXCP.

Parameter	Value	Meaning
peer-addr	<i><IP address></i>	The IP or IPX address you wish to use.
ports	<i><port></i>	The port to which you wish to assign the address.

Restrictions

Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.

Example

To assign an ip address 10.1.1.1/16 to slot 2, serial port 1:

```
rs(config)# ppp set peer-addr ip-addr 10.1.1.1/16 ports se.2.1
```

ppp set ppp-encaps-bgd

Mode

Configure

Format

ppp set ppp-encaps-bgd ports *<port list>*

Description

Issuing the **ppp set ppp-encaps-bgd** command configures the use of ethernet bridged format encapsulation on a given port.

Parameter	Value	Meaning
ports	<i><port list></i>	The port(s) on which you use ethernet bridged encapsulation. Specify a single port or a comma-separated list of ports.

Restrictions

- Usage is restricted to PPP WAN and channelized T1/T3, unframed T1/E1, and Clear Channel T3/E3 ports.
- PoS ports that will be trunk ports must be configured for bridged encapsulation with this command. If you want to negate this command on a PoS port, make sure that the port is an access port and not a trunk port.

Example

To force the bridged encapsulation to slot 2, serial port 1 and slot 3, PoS port 1:

```
rs(config)# ppp set ppp-encaps-bgd ports se.2.1,so.3.1
```

ppp show mlp

Mode

Enable

Format

ppp show mlp *<mlp list>* | **all-ports**

Description

The **ppp show mlp** command displays information about one or more MLP bundles.

Parameter	Value	Meaning
mlp	<i><mlp list></i>	The name(s) of the MLP bundles to display. Specify a single bundle or a comma-separated list of MLP bundles.
	all-ports	Displays information on all MLP ports.

Restrictions

None.

Example

To display the PPP ports for mp.1:

```
rs# ppp show mlp mp.1
mp.1:
  Slot: 4
  PPP ports: se.4.1, se.4.3
```

ppp show service

Mode

Enable

Format

ppp show service *<service name>* | **all**

Description

The **ppp show service** command displays one or all of the available PPP service profiles.

Parameter	Value	Meaning
service	<i><service name></i>	The name of the service profile to display.
	all	Displays all of the available PPP service profiles.

Restrictions

None.

Example

To display the available PPP service profiles named “profile_4”:

```
rs# ppp show service profile_4
```

ppp show stats

Mode

Enable

Format

ppp show stats port *<port>* [**bridge-ncp**] [**ip-ncp**] [**link-status**] [**summary**]

Description

The **ppp show stats** command displays parameters for bridge NCP, IP NCP, and link-status on PPP WAN ports, as well as statistics for channelized T1/T3 ports. You can specify one, two, or three of the available parameter types.

Parameter	Value	Meaning
port	<i><port></i>	The PPP WAN port for which you wish to view bridge NCP, IP NCP, and/or link-status parameters.
bridge-ncp		Specifies that you view bridging NCP parameters for the given port.
ip-ncp		Specifies that you view IP NCP parameters for the given port.
osi-ncp		Displays OSI NCP status.
link-status		Specifies that you view link-status parameters for the given port.
summary		Specifies that you view summarized display.

Restrictions

None.

Example

To display the available link-status and IP NCP parameters for the PPPWAN interface located at slot 4, port 1 :

```
rs# ppp show stats port se.4.1 ip-ncp link-status
```


52 PVST COMMANDS

The **pvst** commands let you display and change settings for a VLAN spanning tree.

52.1 COMMAND SUMMARY

The following table lists the **pvst** commands. The sections following the table describe the command syntax.

<code>pvst create spanningtree vlan-name <string></code>
<code>pvst enable port <port-list> spanning-tree <string></code>
<code>pvst set bridging [forward-delay <num>] [hello-time <num>] [max-age <num>] [priority <num>] spanning-tree <string></code>
<code>pvst set port <port-list> priority <num> port-cost <num> spanning-tree <string></code>
<code>pvst show bridging-info spanning-tree <string></code>

pvst create spanningtree

Mode

Configure

Format

```
pvst create spanningtree vlan-name <string>
```

Description

The **pvst create spanningtree** command creates a spanning tree instance for a particular VLAN.

Parameter	Value	Meaning
vlan-name	<string>	The name of the VLAN for which a new instance of spanning tree is to be created.

Restrictions

None.

pvst enable port spanning-tree

Mode

Configure

Format

```
pvst enable port <port-list> spanning-tree <string>
```

Description

The **pvst enable port** command enables STP on the specified port for the specified spanning tree.

Parameter	Value	Meaning
port	<port-list>	The ports on which you are enabling STP. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8).
spanning-tree	<string>	The name of the spanning-tree instance. This name is the same as the VLAN name.



Note For default VLAN, use **stp** commands.

Restrictions

For PVST, the spanning tree instance must have previously been created.

pvst set bridging spanning-tree

Mode

Configure

Format

```
pvst set bridging [forward-delay <num>] [hello-time <num>] [max-age <num>]  
[priority <num>] spanning-tree <string>
```

Description

The **pvst set bridging spanning-tree** command lets you configure the following STP parameters for a particular VLAN:

- Bridging priority
- Hello time
- Maximum age
- Forward delay

Parameter	Value	Meaning
forward-delay	<num>	Sets the STP forward delay for the RS. The forward delay is measured in seconds. Specify a number from 4– 30. The default is 15.
hello-time	<num>	Sets the STP hello time for the RS. The hello time is measured in seconds. Specify a number from 1– 10. The default is 2.
max-age	<num>	Sets the STP maximum age for the RS. Specify a number from 6–40. The default is 20.
priority	<num>	Sets the STP bridging priority for the RS. Specify a number from 0 – 65535. The default is 32768.
spanning-tree	<string>	The name of the spanning-tree instance. This name is the same as the VLAN name.



Note For default VLAN, use **stp** commands.

Restrictions

For PVST, the spanning tree instance must have previously been created.

Examples

To set the bridging priority of Spanning Tree for VLAN ip1 to 1:

```
rs(config)# pvst set bridging priority 1 spanning-tree ip1
```

pvst set port spanning-tree

Mode
Configure

Format

pvst set port <port-list> priority <num> port-cost <num> spanning-tree <string>

Description

The **pvst set port** command sets the STP priority and port cost for individual ports for a particular VLAN.

Parameter	Value	Meaning
port	<port-list>	The port(s) for which you are setting STP parameters. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8).
priority	<num>	The priority you are assigning to the port(s). Specify a number from 0– 255. The default is 128.
port-cost	<num>	The STP cost you are assigning to the port(s). Specify a number from 1– 65535. The default depends on the port speed: 1 for Gigabit (100-Mbps) ports, 10 for 100-Mbps ports, and 100 for 10-Mbps ports.
spanning-tree	<string>	The name of the spanning-tree instance. This name is the same as the VLAN name.

**Note** For default VLAN, use **stp** commands.

Restrictions

For PVST, the spanning tree instance must have previously been created.

pvst show bridging-info spanning-tree

Mode

Enable

Format

```
pvst show bridging-info spanning-tree <string>
```

Description

The **pvst show bridging-info** command displays STP bridging information for a particular VLAN.

Parameter	Value	Meaning
spanning-tree	<string>	The name of the spanning-tree instance. This name is the same as the VLAN name.

Restrictions

For PVST, the spanning tree instance must have previously been created.

53 QOS COMMANDS

The **qos** commands define and display Quality of Service (QoS) parameters. Use the command to classify Layer 2, Layer 3, and Layer 4 traffic into the following priorities:

- Control
- High
- Medium
- Low

By assigning priorities to network traffic, you can ensure that critical traffic will reach its destination even if the exit ports for the traffic are experiencing greater than maximum utilization. Use the **qos set l2**, **qos set ip**, and **qos set ipx** commands to assign priorities for Layer-2, IP, and IPX traffic respectively.

53.1 COMMAND SUMMARY

The following table lists the **qos** commands. The sections following the table describe the command syntax for each command.

<code>qos apply priority-map <string> ports <port list></code>
<code>qos create priority-map <string> <num> control low med high</code>
<code>qos create one-p-overwrite-map <string> <num></code>
<code>qos overwrite tos-precedence-overwrite list <port list> <interface name> with [IEEE802dot1p] [tos-overwrite-map <string>]</code>
<code>qos overwrite tos-byte-rewrite list <port list> <interface name> with tos-byte-rewrite-map <string></code>
<code>qos overwrite one-p-priority list <ifnames port list> with [tos-precedence] [IEEE8022dot1p-overwrite-map <string>]</code>
<code>qos precedence ip [sip <num>] [dip <num>] [srcport <num>] [dstport <num>] [tos <num>] [protocol <num>] [intf <num>]</code>
<code>qos precedence ipx [srcnet <num>] [srcnode <num>] [srcport <num>] [dstnet <num>] [dstnode <num>] [dstport <num>] [intf <num>]</code>
<code>qos priority-map off</code>
<code>qos set ip <name> <priority> <srcaddr/mask> any <dstaddr/mask> any <srcport> any <dstport> any <tos> <interface-list> any <protocol></code>

qos set ip-acl <string> acl <string> priority low medium high control list <name/ipaddr> tos-mask <num> tos-precedence-rewrite <num> tos-rewrite <num>
qos set ipx <name> <priority> <srcnet> any <srcmask> any <srcport> any <dstnet> any <dstmask> any <dstport> <interface-list> any
qos set l2 name <name> source-mac <MACaddr> dest-mac <MACaddr> vlan <vlanID> in-port-list <port-list> priority control high medium low <trunk-priority>
qos set queuing-policy weighted-fair port <port list> all-ports
qos set weighted-fair control <percentage> high <percentage> medium <percentage> low <percentage> port <port list> all-ports
qos show ip
qos show ipx
qos show l2 all-destination all-flow ports <port-list> vlan <vlanID> source-mac <MACaddr> dest-mac <MACaddr>
qos show one-p-priority-overwrite-with-tos interface
qos show one-p-priority-overwrite-with-map <string> all
qos show precedence ip ipx
qos show priority-map <string> all
qos show tos-precedence-overwrite-with-1p ports interfaces
qos show tos-precedence-overwrite-with-map <string> all
qos show tos-byte-overwrite <string> all
qos show wfq port <port list> all-ports
qos show wred [input output] [port <port list> all-ports]
qos wred input output [exponential-weighting-constant <num>] [mark-prob-denominator <num>][max-queue-threshold <percent>] [min-queue-threshold <percent>] [port <port list> all-ports] [queue control high medium low]

qos apply priority-map

Mode

Configure

Format

qos apply priority-map *<string>* ports *<port list>*

Description

The **qos apply priority-map** command allows you apply a previously defined priority map to a port or multiple ports. A priority map associates certain 802.1p tag values inside the frame to an internal priority queue. Use the **qos create priority-map** command to first create a priority map. By default, the RS maps the number to the four internal priorities as follows:

- 0 or 1 = low
- 2 or 3 = medium
- 4 or 5 = high
- 6 or 7 = control.

Parameter	Value	Meaning
priority-map	<i><string></i>	Specifies the name of the map. Specify a string 25 characters or less.
port	<i><port list></i>	Specifies the port(s) to which you want to apply the priority map.

Restrictions

None.

Example

The following command applies the priority map *map1* to port so.2.1:

```
rs(config)# qos apply priority-map 'map1' port so.2.1
```

qos create priority-map

Mode

Configure

Format

```
qos create priority-map <string> <num> control | low | med | high
```

Description

The **qos create priority-map** command lets you map 802.1p tags from a frame to one of the four internal priority queue classes: **control**, **low**, **medium**, and **high**. Internal priority queue classes are used to prioritize flows during traffic congestion. The flows with the higher priority are given precedence over flow with a lower priority. The internal priority class **control** receives the highest precedence, while **low** receives the lowest precedence. With this command, you can set a particular 802.1p priority tag to map to a specific internal priority queue. By default, the RS maps the number to the four internal priorities as follows:

- 0 or 1 = low
- 2 or 3 = medium
- 4 or 5 = high
- 6 or 7 = control.

Restrictions

Parameter	Value	Meaning
priority-map	<string>	Specifies the name of the map. Specify a string 25 characters or less.
	<num>	Specifies the 802.1p priority tag that you want to map. The range of <num> is between 0 and 7.
queue	control high medium low	Specifies the internal priority queue. Specify either the control , high , medium , or low queue.

None.

Example

The following command creates a priority map *map1* that maps the 802.1p tags 0 and 1 to low, 2 and 3 to medium, 4 and 5 to high, and 6 and 7 to control queue:

```
rs(config)# qos create priority-map 'map1' 0 low 1 low 2 medium 3  
medium 4 high 5 high 6 control 7 control
```

qos create one-p-overwrite-map

Mode
Configure

Format

qos create one-p-overwrite-map <string> <num>

Description

The **qos create one-p-overwrite-map** command remaps ToS precedence.

Parameter	Value	Meaning
one-p-overwrite-map	<string>	This is the name of the map. Specify a string 25 characters or less.
	<num>	Use this to specify 802.1p ToS precedence. <num> is a list. The list is from 0 to 7. Use the list to remap 802.1p ToS precedence. By default, the mapping is as follows: • 0 • 1 • 2 • 3 • 4 • 5 • 6 • 7

Restrictions

None.

Example

The following command remaps precedence as follows:

- 0 goes to 1
- 1 goes to 3
- 2 goes to 4
- 3 goes to 2
- 4 goes to 6
- 5 goes to 7
- 6 goes to 8
- 7 goes to 5

```
rs(config)# one-p-overwrite-map 1,3,4,2,6,7,8,5
```

qos overwrite tos-precedence-overwrite

Mode
Configure

Format

qos overwrite tos-precedence-overwrite list <port list> | <interface name> with [IEEE802dot1p]
| [tos-overwrite-map <string>]

Description

The **qos overwrite tos-precedence-overwrite** command allows you to overwrite the ToS precedence bits within the ToS field.

Parameter	Value	Meaning
list	<port list> <interface name>	Specifies the port(s) or interface name(s) to be overwritten.
IEEE802dot1p		Overwrites the precedence bits of the ToS field with the IEEE802.1p priority bits.
tos-overwrite-map	<string>	Overwrites the precedence bits of the TOS field with a value according to an existing map. Specify the name of the map.

Restrictions

None.

Example

The following command overwrites the ToS precedence bits with the IEEE802.1p priority bits for port et.2.1:

```
rs(config)# qos overwrite tos-precedence-overwrite list et.2.1  
with IEEE802dot1p
```

qos overwrite tos-byte-rewrite

Mode
Configure

Format

qos overwrite tos-byte-rewrite list <port list> | <interface name> with tos-byte-rewrite-map <string>

Description

The **qos overwrite tos-byte-rewrite** command allows you to overwrite the whole ToS field.

Parameter	Value	Meaning
list	<port list> <interface name>	Specifies the port(s) or interface name(s) to be overwritten.
tos-byte-rewrite-map	<string>	Overwrites the whole ToS field with a value according to an existing map. Specify in <string> the name of the map.

Restrictions

None.

Example

The following command overwrites the ToS field with the ToS field value of map *map1* for interface *int2*:

```
rs(config)# qos overwrite tos-byte-rewrite list int2 with
tos-byte-rewrite-map map1
```


qos overwrite one-p-priority

Mode

Configure

Format

qos overwrite one-p-priority list <ifnames | port list> with [tos-precedence] | [IEEE802dot1p-overwrite-map <string>]

Description

The **qos overwrite one-p-priority** command allows you to overwrite the ToS .

Parameter	Value	Meaning
list	<ifnames port list>	Specifies the port(s) or interface name(s) to be overwritten.
IEEE802dot1p-overwrite-map	<string>	Overwrites the whole ToS field with a value according to an existing map. Specify in <string> the name of the map.

Restrictions

None.

Example

The following command overwrites the ToS field with the ToS field values of *map1* for interface *int1*:

```
rs(config)# qos overwrite one-p-priority list int1 with  
IEEE802dot1p-overwrite-map map1
```

qos precedence ip

Mode

Configure

Format

```
qos precedence ip [sip <num>] [dip <num>] [srcport <num>] [destport <num>] [tos <num>]  
[protocol <num>] [intf <num>]
```

Description

The **qos precedence ip** command lets you set the QoS precedence for various flow fields in IP traffic. You can set a precedence from 1 to 7 for the following IP fields:

- IP source address
- IP destination address
- Source TCP or UDP port
- Destination TCP or UDP port
- Type of Service (TOS) for the packet
- Protocol (TCP or UDP)
- Incoming interface

Precedence 1 is the highest priority. IP interfaces or flow fields within IP packets that have a precedence of 1 are given first priority. The default priorities are as follows:

- destination port (1)
- destination address (2)
- source port (3)
- source IP address (4)
- TOS (5)
- interface (6)
- protocol (7).

Parameter	Value	Meaning
sip	<num>	Specifies the precedence of the source address field in IP flows. Specify a precedence from 1 to 7.
dip	<num>	Specifies the precedence of the destination address field in IP flows. Specify a precedence from 1 to 7.
srcport	<num>	Specifies the precedence of the source port field in IP flows. Specify a precedence from 1 to 7.
dstport	<num>	Specifies the precedence of the destination port field in IP flows. Specify a precedence from 1 to 7.

Parameter	Value	Meaning
tos	<num>	Specifies the precedence of the TOS field in IP flows. Specify a precedence from 1 to 7.
protocol	<num>	Specifies the precedence of the transport layer protocol name field in IP flows. Specify a precedence from 1 to 7.
intf	<num>	Specifies the precedence of the IP interface based on the interface's name. Specify a precedence from 1 to 7.

Restrictions

None.

Examples

To change the precedence for fields within IP flows from the default precedences listed above:

```
rs(config)# qos precedence ip sip 3 dip 1 srcport 2 destport 4 tos 5 protocol  
6 intf 7
```

qos precedence ipx

Mode
Configure

Format

```
qos precedence ipx [srcnet <num>] [srcnode <num>] [srcport <num>] [dstnet <num>] [dstnode <num>] [dstport <num>] [intf <num>]
```

Description

The **qos precedence ipx** command lets you set the precedence for the following fields in IPX flows:

- Source network
- Source port
- Source node
- Destination network
- Destination node
- Destination port
- Incoming interface

You can set the precedence of the following fields from 1 to 7. Precedence 1 has the highest priority and 7 has the lowest. The default priorities are as follows:

- Destination network – 1
- Source network – 2
- Destination node – 3
- Source node – 4
- Destination port – 5
- Source port – 6
- Interface – 7

Parameter	Value	Meaning
srcnet	<num>	Specifies the precedence of the source network field in IPX flows. Specify a precedence from 1 to 7.
srcport	<num>	Specifies the precedence of the source port field in IPX flows. Specify a precedence from 1 to 7.
srcnode	<num>	Specifies the precedence of the source node field in IPX flows. Specify a precedence from 1 to 7.
dstnet	<num>	Specifies the precedence of the destination network field in IPX flows. Specify a precedence from 1 to 7.

Parameter	Value	Meaning
dstnode	<num>	Specifies the precedence of the destination node field in IPX flows. Specify a precedence from 1 to 7.
dstport	<num>	Specifies the precedence of the destination port field in IPX flows. Specify a precedence from 1 to 7.
intf	<num>	Specifies the precedence of the IPX interface based on the interface's name. Specify a precedence from 1 to 7.

Restrictions

None.

Examples

To change the precedence for fields within IPX flows from the default precedences listed above:

```
rs(config)# qos precedence ipx srcnet 1 srcnode 2 srcport dstnet 3  
srcport 4 dstnode 5 dstport 6 intf 7
```

qos priority-map off

Mode

Configure

Format

```
qos priority-map off
```

Description

The **qos priority-map off** command allows you disable any priority maps applied on a port using the **qos apply priority-map** command. By default, the RS maps the number to the four internal priorities as follows:

- 0 or 1 = Low
- 2 or 3 = Medium
- 4 or 5 = High
- 6 or 7 = Control

Restrictions

None.

Example

The following command disables all priority mapping:

```
rs(config)# qos priority-map off
```

qos set ip

Mode

Configure

Format

```
qos set ip <name> <priority> [<srcaddr/mask> | any] [<dstaddr/mask> | any] [<srcport> | any]
[<dstport> | any] [<tos> | any] [<port list> | <interface-list> | any] [<protocol> | any]
[<tos-mask> | any] [<tos-precedence-rewrite> | any] [<tos-rewrite> | any]
```

Description

The **qos set ip** command sets the priority for an IP flow based on the following fields in the flow:

- Flow name
- Source IP address and network mask
- Destination IP address and network mask
- Source port
- Destination port
- TOS
- Layer 4 bridging port list or interface list
- Transport layer protocol (TCP or UDP)

You can set the priority of each field to control, low, medium, or high. The default is low.

Parameter	Value	Meaning
ip	<name>	Specifies the IP flow name.
	<priority>	Specifies the priority you are assigning to the flow parameters you specified from the list above. You can specify one of the following priorities:
	control	Assigns control priority to the IP flow parameters you have specified. This is the highest priority.
	high	Assigns high priority to the IP flow parameters you have specified.
	medium	Assigns medium priority to the IP flow parameters you have specified.
	low	Assigns low priority to the IP flow parameters you have specified. This is the default.

Parameter	Value	Meaning
	<srcaddr/mask> any	Specifies the source IP address and network mask for which you are assigning a priority. You can specify the mask using the traditional IP address format, 255.255.0.0, or the CIDR format, /16. If you specify any instead of a network mask, the RS assumes a wildcard <i>don't care</i> condition. If you do not specify a mask, then the RS assumes a mask of 255.255.255.255. You cannot substitute the mask with the any keyword. The keyword any is for the entire <srcaddr/mask> pair.
	<dstaddr/mask> any	Specifies the destination IP address and network mask for which you are assigning a priority. The same requirements and restrictions for <srcaddr/mask> apply to <dstaddr/mask>. If you specify any instead of a network mask, the RS assumes a wildcard <i>don't care</i> condition. If you do not specify a mask, then the RS assumes a mask of 255.255.255.255. You cannot substitute the mask with the any keyword. The keyword any is for the entire <dstaddr/mask> pair.
	<srcport> any	Specifies the source TCP or UDP port for which you are assigning a priority. Specify a port number from 1 to 65535 or any to allow any value.
	<dstport> any	Specifies the destination TCP or UDP port for which you are assigning a priority. Specify a port number from 1 to 65535 or any to allow any value.
	<tos> any	Specifies the TOS for which you are assigning a priority. Specify a number from 0 to 255 or any to allow any value.
	<port list> <interface-list> any	Specifies one or more Layer 4 bridging ports or one or more IP interface names for which you are assigning priority. If you specify a list, delimit the interface names with commas. Specify any to allow any IP interface name.
	<protocol> any	Specifies the transport layer protocol for which you are assigning priority. You can specify one of the following values:
	tcp	Assigns the priority parameters to the TCP protocol.
	udp	Assigns the priority parameters to the UDP protocol.
	any	Assigns the priority parameters to both the TCP and UDP protocols.
	<tos-mask>	Specifies the mask that is used for the TOS byte. Specify a number from 1 to 255 or any to specify any TOS value. The default is 30.

Parameter	Value	Meaning
	<i><tos-precedence-rewrite></i>	Rewrites the precedence portion of the TOS field with a new value. Specify a number from 0-7 or any to specify any TOS value.
	<i><tos-rewrite></i>	Rewrites the entire TOS field with a new value. Specify a number from 0-31 or any to specify any TOS value.
I		

**Note**

If you set **any** for the TOS precedence rewrite and specify a value for *<tos-rewrite>*, then the precedence portion of the TOS field remains the same as in the packet, but the rest of the TOS field is rewritten. If you specify values for both *<tos-precedence-rewrite>* and *<tos-rewrite>*, then the precedence portion of the TOS field is rewritten to the new *<tos-precedence-rewrite>* number and the rest of the TOS field is rewritten to the new *<tos-rewrite>* number.

Restrictions

None.

Examples

The following command creates a flow called *flow1*. This flow provides a template for an IP packet with the IP address 1.1.1.1, network mask 255.255.0.0, destination address 2.2.2.2, and implied destination mask 255.255.255.255. The flow includes source TCP/UDP port 3010, destination port 3000, a TOS of 15, the interfaces *mls1* and *mls2*, and the TCP protocol as transport layer. This flow has the highest priority, control.

```
rs(config)# qos set ip flow1 control 1.1.1.1/255.255.0.0 2.2.2.2 3010 3000 15
mls1,mls2 tcp
```

qos set ip-acl

Mode

Configure

Format

```
qos set ip-acl <string> acl <string> priority <1Q priority>|low | medium | high||control  
list <name/ipaddr> [tos-mask <num>][tos-precedence-rewrite <num>] [tos-rewrite <num>]
```

Description

The **qos set ip-acl** command sets the priority for an IP flow based on a predefined ACL policy. This command is essentially a shortcut for using the **qos set ip** command with a particular ACL policy. Since the ACL policy contains the following information, do not specify the information already inherent in the ACL policy.

- Flow name
- Source IP address and network mask
- Destination IP address and network mask
- Source port
- Destination port
- TOS
- Layer 4 bridging port list or interface list
- Transport layer protocol (TCP or UDP)

Parameter	Value	Meaning
ip-acl	<string>	Set a priority for an IP flow using a predefined ACL. Specify a character string to identify the QoS profile.
acl	<string>	Specify ACL(s) for matching IP flows.
priority		Specifies the 802.1Q priority value or a keyword that specifies the internal priority. Specify one of the following:
	<1Q priority>	802.1Q priority value. Specify a value between 0-7.
	high	High priority.
	medium	Medium priority.
	low	Low priority. This is the default.
	control	Control priority.

Parameter	Value	Meaning
list	<name/port_list> any	Interface name or port list for L4 bridging VLAN. Specify any to enable L4 bridging VLAN on all interfaces.
tos-mask	<tos-mask> any	Specifies the mask that is used for the TOS byte. Specify a number from 1-255 or any to specify any TOS value. The default is 30.
tos-precedence-rewrite	<tos-precedence-rewrite> any	Rewrites the precedence portion of the TOS field with a new value. Specify a number from 0 to 7 or any to specify any TOS value.
tos-rewrite	<tos-rewrite> any	Rewrites the entire TOS field with a new value. Specify a number from 0 to 31 or any to specify any TOS value.

**Note**

If you set **any** for the TOS precedence rewrite and specify a value for <tos-rewrite>, then the precedence portion of the TOS field remains the same as in the packet, but the rest of the TOS field is rewritten. If you specify values for both <tos-precedence-rewrite> and <tos-rewrite>, then the precedence portion of the TOS field is rewritten to the new <tos-precedence-rewrite> number and the rest of the TOS field is rewritten to the new <tos-rewrite> number.

Restrictions

None.

Examples

The following command uses an ACL called *ipacl2* to set the priority for the IP flow *ipflow2*.

```
rs(config)# qos set ip-acl ipacl2 priority high list ipflow2
```

qos set ipx

Mode

Configure

Format

```
qos set ipx <name> <priority> [<srcnet> | any] [<srcmask> | any] [<srcport> | any] [<dstnet> | any]
[<dstmask> | any] [<dstport> | any] [<port list> | <interface-list> | any]
```

Description

The **qos set ipx** command lets you set the priority for an IPX flow based on the following fields in the flow:

- Flow name
- Source network
- Source network mask
- Source port
- Destination network
- Destination network mask
- Destination port
- Layer 4 bridging port or interface list

You can set the priority of each field to control, low, medium, or high. The default is low.

Parameter	Value	Meaning
ipx	<name>	Specifies the IPX flow name.
	<priority>	Specifies the priority you are assigning to the flow. You can specify one of the following priorities:
	control	Assigns control priority to the IPX flow specified. This is the highest priority.
	high	Assigns high priority to the IPX flow specified.
	medium	Assigns medium priority to the IPX flow specified.
	low	Assigns low priority to the IPX flow specified. This is the default.
	<srcnet> any	Specifies the IPX source network and node address. Specify in the following format: <netaddr> . <macaddr>. For example, a1b2c3d4.aa:bb:cc:dd:ee:ff . If any is specified instead of .<macaddr>, the RS assumes a wildcard value. All MAC addresses are then valid.

Parameter	Value	Meaning
	<srcmask> any	Specify the IPX source network mask. Specify the mask in hexadecimal. If you do not specify a mask value and instead use the value any , the RS sets the mask to FFFFFFFF.
	<srcport> any	Specify a port number from 1 to 65535 or any to allow any value.
	<dstnet> any	Specify the IPX destination network and node address. The same requirements and restrictions for <dstaddr> apply to <srcaddr>.
	<dstmask> any	This is the IPX destination network mask. Specify the mask in hexadecimal or any to allow any value.
	<dstport> any	Specify a port number from 1 to 65535 or any to allow any value.
	<port list> <interface-list> any	Specify one or more Layer 4 bridging ports or one or more IPX interface names for which you are assigning priority. If you specify a list, delimit the interface names with commas. Specify any to allow any IPX interface name.

Restrictions

None.

Examples

The following command creates an IPX flow called *abc*. This flow gives a high priority to IPX traffic on interface *mls1* from network 12345678.00:01:00:00:00:00, mask 0000ff00, port 55 to network 22222222.02:00:00:00:00:00, mask 0000ff00, port 65.

```
rs(config)# qos set ipx abc high 12345678.00:01:00:00:00:00
0000ff00 55 22222222.02:00:00:00:00:00 0000ff00 65 mls1
```

qos set l2

Mode

Configure

Format

```
qos set l2 name <name> source-mac <MACaddr> source-mac-mask <MACaddr> dest-mac <MACaddr>
dest-mac-mask <MACaddr> vlan <vlanID> in-port-list <port-list> priority control | high |
medium | low | <trunk-priority>
```

Description

The **qos set l2** command sets QoS priority for Layer 2 flows. Set a priority for a flow based on the following fields in the flow:

- L2 flow name
- Source MAC address
- Destination MAC address
- VLAN ID
- Incoming port(s)

You can set the priority in one of the following ways:

- The flow is assigned a priority within the RS. In this case specify a priority of control, low, medium, or high. The default is low.
- The flow is assigned a priority within the RS and in addition, if the exit ports are VLAN trunk ports the flow is assigned an 802.1Q priority. In this case specify a number from 0 to 7. The RS maps the number to the four internal priorities as follows:
 - 0 or 1 = Low
 - 2 or 3 = Medium
 - 4 or 5 = High
 - 6 or 7 = Control

Parameter	Value	Meaning
name	<name>	Specify the L2 flow name.
source-mac	<MACaddr> any	This is the L2 source MAC address used to create a flow priority entry. Specify the MAC address in either of the following formats: xx:xx:xx:xx:xx:xx xxxxxx:xxxxxx Specify any to allow any MAC address as the L2 source MAC address.
source-mac-mask	<MACaddr>	Specify the source MAC mask address.

Parameter	Value	Meaning
dest-mac	<MACaddr> any	Specify the L2 destination MAC address used to create either a destination priority entry (without a source-mac defined) or a flow priority entry (with a source-mac defined.) Specify any to allow any MAC address as the L2 destination MAC address.
dest-mac-mask	<MACaddr>	Specify the destination MAC mask address.
vlan	<vlanID> any	Specifies the VLAN number. Specify any to allow any VLAN.
in-port-list	<port-list>	Specify the RS ports for which you are setting priority for this flow. The priority applies when the L2 packet enters the RS on one of the specified ports. The priority does not apply to exit ports.
 Note When a qos l2 flow priority entry is defined, the ports defined in the in-port-list must have flow-based bridging enabled on them.		
priority	control high medium low <trunk-priority>	This sets the priority for the flow. Specify one of the following priorities:
	control	Assigns control priority to the IP flow specified. This is the highest priority.
	high	Assigns high priority to the IP flow specified.
	medium	Assigns medium priority to the IP flow specified.
	low	Assigns low priority to the IP flow specified. This is the default.
	<trunk-priority>	Assigns an 802.1Q VLAN trunk priority when the exit port is a VLAN trunk port. The RS maps the number to the four internal priorities as follows: • 0 = Low • 1, 2, or 3 = Medium • 4, 5, or 6 = High • 7 = Control

Restrictions

None.

qos set queuing-policy

Mode
Configure

Format

qos set queuing-policy weighted-fair port <port list> | all-ports

Description

The **qos set queuing-policy** command overrides the default queuing policy (strict priority) in favor of weighted-fair queuing on specific ports or on all ports. Only one type of queuing policy can be active at a time for a port.

Parameter	Value	Meaning
queuing-policy	weighted-fair	Sets the queuing policy to weighted-fair.
port	<port list> all-ports	Specify the ethernet ports or WAN modules and ports on which weighted-fair queuing apply. Use all-ports to apply weighted fair queuing to all ports.

Restrictions

None.

Examples

To set the queuing policy back to strict priority, enter the following command:

```
rs(config)# qos set queuing-policy weighted-fair port et.1.*
```


qos set weighted-fair

Mode

Configure

Format

```
qos set weighted-fair control <percentage> high <percentage> medium <percentage> low  
<percentage> port <port list> | all-ports
```

Description

The **qos set weighted-fair** command sets the percentage of RS bandwidth allocated to the priority when the port uses weighted-fair queuing. The percentages apply to specific ports or to all ports. Make sure the total percentages for all four priorities equals 100.

Parameter	Value	Meaning
control	<percentage>	Specify the percentage of RS bandwidth allocated to the control priority. The range for <percentage> is 1 to 100. The default is 25.
high	<percentage>	Specify the percentage of RS bandwidth allocated to the high priority. The range for <percentage> is 1 to 100. The default is 25.
medium	<percentage>	Specify the percentage of RS bandwidth allocated to the medium priority. The range for <percentage> is 1 to 100. The default is 25.
low	<percentage>	Specify the percentage of RS bandwidth allocated to the low priority. The range for <percentage> is 1 to 100. The default is 25.
port	<port list> all-ports	Specifies the ethernet ports or WAN modules and ports on which the defined percentages apply. Specify all-ports to apply the percentages to all ports.

Restrictions

The total percentages for all four QoS levels must equal 100%.

qos show ip

Mode

Enable

Format

qos show ip

Description

The **qos show ip** command lets you display QoS information for IP flows.

Restrictions

None.

qos show ipx

Mode

Enable

Format

```
qos show ipx
```

Description

The **qos show ipx** command lets you display QoS information for IPX flows.

Restrictions

None.

qos show l2

Mode

Enable

Format

```
qos show l2 all-destination all-flow ports <port-list> vlan <vlanID> source-mac <MACaddr>
dest-mac <MACaddr>
```

Description

The **qos show l2** command lets you display QoS information for L2 flows. You can filter the display according to the following:

- Destinations
- Flows
- Ports
- VLANs
- Source MAC addresses
- Destination MAC addresses
- Priority

Parameter	Value	Meaning
l2	all-destination	Shows all the L2 destination priorities.
	all-flow	Shows all the L2 flow priorities.
ports	<port-list>	Shows L2 priority information for specific ports.
vlan	<vlanID>	Shows L2 priority information for specific VLANs.
source-mac	<MACaddr>	Shows L2 priority information for specific source MAC addresses.
dest-mac	<MACaddr>	Shows L2 priority information for specific destination MAC addresses.

Restrictions

None.

qos show one-p-priority-overwrite-with-tos

Mode

Enable

Format

```
qos show one-p-priority-overwrite-with-tos interfaces | ports
```

Description

The **qos show one-p-priority-overwrite-with-tos** command displays the interfaces or ports that were previously configured with 802.1p and now are configured with a new ToS value.

Parameter	Value	Meaning
interfaces ports		Specify interfaces to display all interfaces that are reconfigured. Specify ports to display all ports that are reconfigured.

Restrictions

None.

qos show one-p-priority-overwrite-with-map

Mode

Enable

Format

qos show one-p-priority-overwrite-with-map <string> | all

Description

The **qos show one-p-priority-overwrite-with-tos** command displays a previously created map.

Parameter	Value	Meaning
one-p-priority-overwrite-with-map	<string>	Specify the name of a map to display.
all		Specify all to display all the maps that were created.

Restrictions

None.

qos show precedence

Mode

Enable

Format

```
qos show precedence ip | ipx
```

Description

The **qos show precedence** command lets you display the precedence values for all fields in a flow:

- IP flows consist of the following fields:
 - Destination Port
 - Destination Address
 - Source Port
 - Source Ip Address
 - Tos
 - Interface
 - Protocol
- IPX flows consist of the following fields:
 - Destination Network
 - Source Network
 - Destination Node
 - Source Node
 - Destination Port
 - Source Port
 - Interface

Parameter	Value	Meaning
precedence	ip	Displays the precedence values for IP flows.
	ipx	Displays the precedence values for IPX flows.

Restrictions

None.

qos show priority-map

Mode

Enable

Format

```
qos show priority-map <string> | all
```

Description

The **qos show priority-map** command displays the priority mapping that is configured on a port. The command shows how each 802.1p tag value is mapped to a specific internal priority queue.

Parameter	Value	Meaning
priority-map	<string>	Specify the name of the priority map.
	all	Displays all priority maps.

Restrictions

None.

qos show tos-precedence-overwrite-with-1p

Mode

Enable

Format

```
qos show tos-precedence-overwrite-with-1p ports | interfaces
```

Description

The **qos show tos-precedence-overwrite-with-1p** command displays the ports or interfaces has TOS precedence bits that were overwritten with IEEE 802.1p priority.

Parameter	Value	Meaning
ports		Show ports on which the TOS precedence bits have been rewritten with IEEE 802.1p priority.
interfaces		Show interfaces on which the TOS precedence bits have been rewritten with IEEE 802.1p priority.

Restrictions

None.

qos show

tos-precedence-overwrite-with-map

Mode

Enable

Format

qos show tos-precedence-overwrite-with-map <string> | all

Description

The **qos show tos-precedence-overwrite-with-map** command displays priority maps used to overwrite TOS precedence.

Parameter	Value	Meaning
tos-precedence-overwrite-with-map	<string>	Specifies the name of the priority map.
all		Displays all priority maps.

Restrictions

None.

qos show tos-byte-overwrite

Mode

Enable

Format

qos show tos-byte-overwrite <string> | all

Description

The **qos show tos-byte-overwrite** command displays priority maps used to overwrite TOS bytes.

Parameter	Value	Meaning
tos-byte-overwrite	<string>	Specify the name of the priority map.
all		Displays all priority maps.

Restrictions

None.

qos show wfq

Mode

Enable

Format

qos show wfq [port <port list> | all-ports] [input <slot num> | all-modules]

Description

The **qos show wfq** command displays the bandwidth for each port allocated with weighted-fair queuing.

Parameter	Value	Meaning
port	<port list> all-ports	Displays bandwidth allocated for each port. Specify a list of ethernet or WAN ports. Specify all-ports to display bandwidth for all ports.
input	<slot num> all-modules	Displays bandwidth allocated for each slot. Specify a list of occupied slots. Specify all-modules to display bandwidth for all modules.

Restrictions

None.

qos show wred

Mode

Enable

Format

```
qos show wred [input|output] [port <port list> | all-ports]
```

Description

The **qos show wred** command displays WRED information for a certain port or all ports. You can display WRED parameter information according to the following:

- Input ports
- Output ports
- All ports

Parameter	Value	Meaning
input		Displays WRED parameters for input ports.
output		Displays WRED parameters for output ports.
port	<port list> all-ports	Displays WRED parameters for each port. Specify all-ports to display parameters for all ports.

Restrictions

None.

qos wred

Mode

Configure

Format

```
qos wred input|output [exponential-weighting-constant <num>] [mark-prob-denominator
<num>] [max-queue-threshold <percent>] [min-queue-threshold <percent>] [port <port list> |
all-ports] [queue control | high | medium | low]
```

Description

The **qos wred** command is used to set the parameters for Weighted Random Early Detection (WRED) and to apply them to either input or output queues on specific ports.

WRED is a dynamic process for controlling congestion on RS ports and the segments of the network associated with the WRED enabled ports. The WRED process consists of setting a *minimum queue threshold* (min-threshold) and a *maximum queue threshold* (max-threshold) on any of the four queues (low, medium, high, and control) belonging to a port. Associated with these thresholds is an *average queue size*, which is dynamically calculated as the instantaneous average buffer depth. If the average queue size is below the min-threshold, no packets are discarded. However, if the average queue size rises above the min-threshold, WRED uses a *packet-marking probability* algorithm to randomly mark packets for discard. As the average queue size increases toward the max-threshold, the probability of packet drop also increases. Eventually, if the average queue size exceeds the max-threshold, the probability of packet drop becomes 1 (100% of packets are dropped). This increase in the probability of packet drop increases in a linear fashion from 0 to 1 (0% dropped to 100% dropped). Notice that the probability of packet drop roughly depends on bandwidth, i.e.; the more packets sent by a particular connection, the greater the probability that packets will be dropped from that connection.

Parameter	Value	Meaning
input output	<string>	Specifies whether WRED is applied to an input or output queue.
exponential-weighting-constant	<num>	Determines how fast the average queue size changes with changes in actual queue size. Specify a number between 0 (fastest) and 3 (slowest) for input queues (default is 1). Specify a number between 0 and 7 for output queues (default is 3).
mark-prob-denominator	<num>	Used to determine the probability with which a packet is dropped when average queue size is between min-threshold and max-threshold. The lower this value is set, the higher the probability of packet drop. Specify a value between 0 and 7 for input queues (default is 1). Specify a value between 0 and 14 for output queues (default is 3).

Parameter	Value	Meaning
max-queue-threshold	<percent>	Sets the maximum queue threshold. When the average queue size reaches this threshold, all packets are dropped. Threshold is in percent of queue. Specify a value between 10 and 100 (the default is 50% for output queues).
min-queue-threshold	<percent>	Sets the minimum queue threshold. When the average queue size rises above this threshold, packets begin to drop. Threshold is in percent of queue. Specify a value between 0 and 100 (the default is 25% for output queues).
port	<port list> all-ports	Specifies the port on which the WRED algorithm is applied. Specify all-ports to apply WRED to all ports.
queue	control high medium low	Specifies which queue to apply the WRED algorithm. Specify control, high, medium, or low queue.

Restrictions

WRED's full capabilities to reduce congestion are best used with TCP (and other connection-oriented protocols). As TCP traffic increases on a WRED port, and the average queue size rises above the min-threshold, some TCP packets begin to drop. Each TCP source interprets dropped packets as an indication of congestion. As a result, each TCP source that has experienced a dropped packet reduces its window, the average queue size decreases, and congestion is alleviated.

Although connection-less protocols do not have the response capability of TCP to sense congestion. Nevertheless, WRED's technique of dropping packets based on rising probability assures that those connections that are sending the most packets or using the most bandwidth will be more likely to have their packets dropped than lower bandwidth connections. This provides at least some assurance of equality of throughput on a WRED port for connection-less protocols.

Examples

The following command sets WRED on port et.2.1's high input queue, sets the queue weight to 2, min-threshold to 10% of total queue size, max-threshold to 70% of total queue size, and the probability denominator to 0 (higher probability of packets being dropped):

```
rs(config)# qos wred input exponential-weighting-constant 2
mark-prob-denominator 0 min-queue-threshold 10 max-queue-threshold 70 port
et.2.1 queue high
```


54 RADIUS COMMANDS

The **radius** commands let you secure access to the RS using the Remote Authentication Dial-In User Service (RADIUS) protocol. When a user logs in to the RS or tries to access Enable mode, he or she is prompted for a password. If RADIUS authentication is enabled on the RS, it will contact a RADIUS server to verify the user. If the user is verified, he or she is granted access to the RS.

54.1 COMMAND SUMMARY

The following table lists the **radius** commands. The sections following the table describe the command syntax.

<code>radius accounting command level <level></code>
<code>radius accounting shell start stop all</code>
<code>radius accounting snmp active startup</code>
<code>radius accounting system fatal error warning info</code>
<code>radius authentication login enable</code>
<code>radius enable</code>
<code>radius set deadtime <minutes></code>
<code>radius set key <string></code>
<code>radius set last-resort password succeed deny</code>
<code>radius set retries <number></code>
<code>radius set server <IPaddr> [acct-port <acct-port-no>] [auth-port <auth-port-no>]</code>
<code>radius set source <ipaddr> <interface></code>
<code>radius set timeout <seconds></code>
<code>radius show stats all</code>

radius accounting command level

Mode

Configure

Format

radius accounting command level *<level>*

Description

The **radius accounting command level** command allows you specify the types of commands that are logged to the RADIUS server. The user ID and timestamp are also logged.

Parameter	Value	Meaning
level	<i><level></i>	Specifies the type(s) of commands that are logged to the RADIUS server. Enter one of the following values:
	5	Log Configure commands.
	10	Log all Configure and Enable commands.
	15	Log all Configure, Enable, and User commands.

Restrictions

None.

Example

To cause Configure, Enable, and User mode commands to be logged on the RADIUS server:

```
rs(config)# radius accounting command level 15
```

radius accounting shell

Mode

Configure

Format

```
radius accounting shell start|stop|all
```

Description

The **radius accounting shell** command allows you to track shell usage on the RS. It causes an entry to be logged on the RADIUS server when a shell is started or stopped. You can specify that an entry be logged when a shell is started, when a shell is stopped, or when a shell is either started or stopped.

Parameter	Value	Meaning
shell	start	Logs an entry when a shell is started.
	stop	Logs an entry when a shell is stopped.
	all	Logs an entry when a shell is either started or stopped.

Restrictions

None.

Example

To cause an entry to be logged on the RADIUS server when a shell is either started or stopped on the RS:

```
radius accounting shell all
```

radius accounting snmp

Mode

Configure

Format

```
radius accounting snmp active|startup
```

Description

The **radius accounting snmp** command allows you to track changes made to the active or startup configuration through SNMP. It causes an entry to be logged on the RADIUS server whenever a change is made to the ACL configuration. You can specify that an entry be logged to the active or startup configuration.

Parameter	Value	Meaning
snmp	active	Logs an entry when a change is made to the active configuration.
	startup	Logs an entry when a change is made to the startup configuration.

Restrictions

None.

Example

To cause an entry to be logged on the RADIUS server whenever an ACL configuration change is made via SNMP to the active configuration:

```
rs(config)# radius accounting snmp active
```

radius accounting system

Mode

Configure

Format

```
radius accounting system fatal|error|warning|info
```

Description

The `radius accounting system` command allows you to specify the types of messages that are logged on the RADIUS server.

Parameter	Value	Meaning
<code>fatal</code>		Logs only fatal messages.
<code>error</code>		Logs fatal messages and error messages.
<code>warning</code>		Logs fatal messages, error messages, and warning messages.
<code>info</code>		Logs all messages, including informational messages.

Restrictions

None.

Example

To log only fatal and error messages on the RADIUS server:

```
rs(config)# radius accounting system error
```

radius authentication

Mode

Configure

Purpose

Causes RADIUS authentication to be performed at the RS login prompt and/or when the user tries to access Enable mode.

Format

```
radius authentication login|enable
```

Description

The **radius authentication** command allows you to specify when RADIUS authentication is performed: when a user logs in to the RS and/or tries to access Enable mode.

Parameter	Value	Meaning
login		Authenticates users at the RS login prompt.
enable		Authenticates users when they try to access Enable mode.

Restrictions

None.

Example

To perform RADIUS authentication at the RS login prompt:

```
radius authentication login
```

radius enable

Mode

Configure

Format

radius enable

Description

The **radius enable** command causes RADIUS authentication to be activated on the RS. RADIUS authentication is disabled by default on the RS.

You set RADIUS-related parameters with the **radius set** or **radius accounting** commands, then use the **radius enable** command to activate RADIUS authentication.

Restrictions

None.

Example

The following commands set RADIUS-related parameters on the RS. The commands are then activated with the **radius enable** command:

```
radius set server 207.135.89.15
radius set timeout 30
radius authentication login
radius accounting shell all
radius enable
```

radius set deadline

Mode
Configure

Format

radius set deadline <minutes>

Description

The **radius set deadline** command allows you to set the length of time that a RADIUS server is ignored after it has failed. This command sets a global value that is applicable to all configured RADIUS servers. You can set a deadline value for a specific server with the **radius set server** command.



Note The deadline value set for a specific server with the **radius set server** command takes precedence over the value specified with the **radius set deadline** command.

Parameter	Value	Meaning
deadline	<minutes>	Number of minutes that any RADIUS server is ignored after it has failed. Specify a value between 0 and 1440. The default is 0 minutes.

Restrictions

None.

Example

The following commands configure three RADIUS servers. The RS will ignore hosts 137.72.5.41 and 137.72.5.25 for 10 minutes if either server fails, and it will ignore host 137.72.5.9 for 2 minutes if that server fails.

```
radius set server 137.72.5.9 deadline 2
radius set server 137.72.5.41
radius set server 137.72.5.25
radius set deadline 10
```


radius set key

Mode

Configure

Format

radius set key *<string>*

Description

The **radius set key** command allows you to set the authentication key for RADIUS servers. This command sets a global key that is applicable to all configured RADIUS servers. You can set a key for a specific server with the **radius set server** command.



Note

The key set for a specific server with the **radius set server** command takes precedence over the key specified with the **radius set key** command.

Parameter	Value	Meaning
key	<i><string></i>	Authentication key to be shared with a configured RADIUS server. Specify a string up to 128 characters.

Restrictions

None.

Example

The following commands configure three RADIUS servers. The RS will use the authentication key 'pome4' for hosts 137.72.5.41 and 137.72.5.25, and the key 'b456' for host 137.72.5.9.

```
radius set server 137.72.5.9 key b456
radius set server 137.72.5.41
radius set server 137.72.5.25
radius set key pome4
```

radius set last-resort

Mode

Configure

Format

```
radius set last-resort password|succeed|deny
```

Description

The **radius set last-resort** command allows you to specify what the RS does if the RADIUS server does not reply by a given time. If this command is not specified, the RS tries the next configured authentication method (including TACACS+ configuration commands). Otherwise, if the RADIUS server does not reply within the configured timeout period for the configured number of retries, user authentication will fail.

Parameter	Value	Meaning
last-resort		The action to take if a RADIUS server does not reply within the configured timeout.
	password	The password set with system set password command is used. This keyword is <i>recommended</i> for optimal security, however, note that you must set a password with the system set password command.
	succeed	Access to the RS is granted.
	deny	Access to the RS is denied.

Restrictions

None.

Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are RADIUS servers, and the RS should wait no more than 30 seconds for a response from one of these servers. If a response from a RADIUS server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the RS **system set password** command.

```
radius set server 137.72.5.9
radius set server 137.72.5.41
radius set timeout 30
radius set last-resort password
```

radius set retries

Mode
Configure

Format

radius set retries <number>

Description

The **radius set retries** command allows you to set the maximum number of times that the RS will try to contact a RADIUS server for authentication and accounting. This command sets a global value that is applicable to all configured RADIUS servers. You can set a retries value for a specific server with the radius set server command.



Note The retries value set for a specific server with the **radius set server** command takes precedence over the retries specified with the **radius set retries** command.

Parameter	Value	Meaning
retries	<number>	The maximum number of times that the RS will try to contact a RADIUS server. Specify a value between 1 and 10. The default is 3 times.

Restrictions

None.

Example

The following commands configure three RADIUS servers. The RS will try up to four times for a response from hosts 137.72.5.41 and 137.72.5.25, but will try up to six times for a response from host 137.72.5.9.

```
radius set server 137.72.5.9 retries 6
radius set server 137.72.5.41
radius set server 137.72.5.25
radius set retries 4
```

radius set server

Mode

Configure

Format

```
radius set server <IPaddr> [acct-port <acct-port-no>] [auth-port <auth-port-no>] [timeout
<seconds>] [retries <number>] [deadtime <minutes>] [key <string>] [source
<ipaddr>|<interface>]
```

Description

The **radius set server** command allows you to identify a RADIUS server and configure parameters for the server. These parameters include the port numbers for accounting and authentication, how long to wait for the server to authenticate the user, and number of times to try contacting the server for authentication. You can configure up to five RADIUS servers for use with the RS. Specify one server per **radius set server** command.

Parameter	Value	Meaning
server	<IPaddr>	Is the IP address of a RADIUS server. You can enter up to five RADIUS servers. Enter one server per radius set server command.
acct-port	<acct-port-no>	Port number to use for accounting for this RADIUS server. Specify a value between 0-65535. Specify 0 to disable accounting on this RADIUS server. The default is port 1813.
auth-port	<auth-port-no>	Port number to use for authentication for this RADIUS server. Specify a value between 0-65535. Specify 0 to disable authentication on this RADIUS server. The default is port 1812.
timeout	<seconds>	The maximum time (in seconds) to wait for this RADIUS server to reply. Specify a value between 1-30. If this parameter is not defined, the global timeout value defined with the radius set timeout command is used. If a radius set timeout value is not configured, the default is 3 seconds.
retries	<number>	The number of times to try contacting this RADIUS server. Specify a value between 1-10. If this parameter is not defined, the global retries values defined with the radius set retries command is used. If a radius set retries value is not configured, the default is 3 times.
deadtime	<minutes>	Number of times that this RADIUS server is ignored after it has failed. Specify a value between 0-1440. If this parameter is not defined, the global deadtime value defined with the radius set deadtime command is used. If a radius set deadtime value is not configured, the default is 0 minutes.

Parameter	Value	Meaning
key	<string>	Authentication key to be shared with this RADIUS server. Specify a string up to 128 characters. If this parameter is not defined, the global key defined with the radius set key command is used.
source	<ipaddr> <interface>	IP address or name of the interface to use with this server.

Restrictions

None.

Example

The following commands configure hosts 137.72.5.9 and 137.72.5.41 as RADIUS servers, each with different operating parameters.

```
radius set server 137.72.5.9 timeout 30 retries 4
radius set server 137.72.5.41 timeout 20 retries 6 deadtime 5
```

radius set source

Mode
Configure

Format

radius set source <ipaddr> | <interface>

Description

The **radius set source** command allows you to set a source IP address or interface to use with a RADIUS server. This command sets a global value that is applicable to all configured RADIUS servers. You can set a source value for a specific server with the **radius set server** command.

**Note** The source value set for a specific server with the **radius set server** command takes precedence over the source specified with the **radius set source** command.

Parameter	Value	Meaning
source	<ipaddr> <interface>	IP address or the name of the interface to use with the RADIUS server.

Restrictions

None.

Example

The following commands configure three RADIUS servers. The RS will use the IP address 101.100.100.102 for hosts 137.72.5.41 and 137.72.5.25, but will use 10.10.10.10 for host 137.72.5.9.

```
radius set server 137.72.5.9 source 10.10.10.10
radius set server 137.72.5.41
radius set server 137.72.5.25
radius set source 101.100.100.102
```

radius set timeout

Mode

Configure

Format

radius set timeout <seconds>

Description

The **radius set timeout** command allows you to set how long to wait for the RADIUS server to authenticate the user. This command sets a global value that is applicable to all configured RADIUS servers. You can set a timeout value for a specific server with the **radius set server** command.



Note The timeout value set for a specific server with the **radius set server** command takes precedence over the timeout specified with the **radius set timeout** command.

Parameter	Value	Meaning
timeout	<seconds>	The maximum time (in seconds) to wait for a RADIUS server to reply. Specify a value between 1 and 30. The default is 3 seconds.

Restrictions

None.

Example

The following commands configure three RADIUS servers. The RS will wait no more than 10 seconds for a response from hosts 137.72.5.41 and 137.72.5.25, but will wait up to 30 seconds for a response from host 137.72.5.9.

```
radius set server 137.72.5.9 timeout 30
radius set server 137.72.5.41
radius set server 137.72.5.25
radius set timeout 10
```

radius show

Mode

Enable

Format

```
radius show stats|all
```

Description

The **radius show** command displays statistics and configuration parameters related to RADIUS configuration on the RS. The statistics displayed include:

- accepts: Number of times each server responded and validated the user successfully.
- rejects: Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied.
- challenges: Number of times each server requested additional information for user authentication.
- timeouts: Number of times each server did not respond.

Parameter	Value	Meaning
stats		Displays the accepts, rejects, and timeouts for each RADIUS server.
all		Displays the configuration parameters set with the radius set command, in addition to the accepts, rejects, and timeouts for each RADIUS server.

Restrictions

None.

Example

To display configuration parameters and RADIUS server statistics:

```
rs# radius show all
RADIUS                                status:                                ❶
RADIUS last resort:                   System Password                        ❷
Default RADIUS timeout (seconds):     3                                ❸
Default RADIUS retries:               3                                ❹
Default RADIUS deadtime (minutes):    0                                ❺
Default RADIUS source IP address:     Let system decide                    ❻

RADIUS servers listed in order of priority:

Server:                               ❼
Authentication Port: 1645
Accounting Port: 1646
Timeout (seconds): 20
Retries: <Default>
Deadtime (minutes): <Default>
Source IP: <Default>

Server: 192.168.1.78
Authentication Port: 1812
Accounting Port: 1813
Timeout (seconds): 5
Retries: 5
Deadtime (minutes): 5
Source IP: 176.141.101.141

Server: 192.168.2.33
Authentication Port: 1812
Accounting Port: 1813
Timeout (seconds): <Default>
Retries: <Default>
Deadtime (minutes): <Default>
Source IP: <Default>

RADIUS server statistics:

❽      ❾      ❿      ⓫      ⓬
Host      Accepts  Rejects  Challenges  Timeouts
10.50.7.45      0         0         0         0
192.168.1.78    0         0         0         0
192.168.2.33    0         0         0         0
```

Legend:

- Shows “ACTIVE” if RADIUS has been enabled with the **radius enable** command.
- Action to be taken if there is no response from the RADIUS server, as configured with the **radius set last-resort** command. If this command is not configured, the action shown is “None set.”
- Value set with the **radius set timeout** command. Default is 3 seconds.
- Value set with the **radius set retries** command. Default is 3 retries.
- Value set with the **radius set deadtime** command. Default is 0 minutes.

6. IP address set with the **radius set source** command. “Let system decide” means that no source IP address is configured with this command and the RS performs a lookup in its routing table to set the source IP address for client requests.
7. Shows server-specific parameter values for each configured RADIUS server. Server-specific parameters are configured with the **radius set server** command. “<Default>” means that the default value is used for the particular parameter.
8. IP address of RADIUS server.
9. Number of times server responded and successfully validated the user.
10. Number of times server responded and denied the user access, either because the user was not known or the wrong password was supplied.
11. Number of times server requested additional information for authentication.
12. Number of times server did not respond before the timeout expired.

55 RARPD COMMANDS

The **rarpd** commands let you configure and display information about Reverse Address Resolution Protocol (RARP) on the RS.

55.1 COMMAND SUMMARY

The following table lists the `rarpd` commands. The sections following the table describe the command syntax.

<code>rarpd add hardware-address <mac-address> ip-address <IPaddr></code>
<code>rarpd set interface <name> all</code>
<code>rarpd show interface mappings</code>

rarpd add

Mode

Configure

Purpose

Maps a MAC address to an IP address.

Format

```
rarp add hardware-address <mac-address> ip-address <IPaddr>
```

Description

The **rarpd add** command allows you to map a MAC address to an IP address for use with RARP. When a host makes a RARP request on the RS, and its MAC address has been mapped to an IP address with the **rarpd add** command, the RARP server on the RS responds with the IP address that corresponds to the host's MAC address.

Parameter	Value	Meaning
hardware-address	<mac-address>	Is a MAC address in the form xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx.
ip-address	<IPaddr>	Is the IP address to be mapped to the MAC address.

Restrictions

None

Example

To map MAC address 00:C0:4F:65:18:E0 to IP address 10.10.10.10:

```
rs(config)# rarpd add hardware-address 00:C0:4F:65:18:E0 ip-address 10.10.10.10
```

rarpd set interface

Mode

Configure

Format

```
rarpd set interface <name>|all
```

Description

The **rarpd set interface** command allows you to specify to which interfaces the RS' RARP server responds when sent RARP requests. You can specify individual interfaces or all interfaces.

Parameter	Value	Meaning
interface	<name>	Is the name of an interface.
	all	Causes the RARP server to respond to RARP requests from all interfaces.

Restrictions

None.

Example

To cause the RS' RARP server to respond to RARP requests from interface int1:

```
rs(config)# rarpd set interface int1
```

rarpd show

Mode

Enable

Format

rarpd show interface|mappings

Description

The **rarpd show** command displays information about the configuration of the RS' RARP server. You can list the MAC-to-IP address mappings or the interfaces to which the RS responds to RARP requests.

Parameter	Value	Meaning
show	interface	Lists the interfaces to which the RS responds to RARP requests.
	mappings	Displays the list of MAC-to-IP address mappings that was set with the rarp add command.

Restrictions

None.

Example

To display the RARP server's list of MAC-to-IP address mappings:

```
rs(config)# rarpd show mappings
```

56 RATE-LIMIT COMMAND

Use the **rate-limit** commands to define rate limits and apply them to IP interfaces.

56.1 COMMAND SUMMARY

The following table lists the **rate-limit** commands. The sections following the table describe the command syntax.

<code>rate-limit <name> aggregate acl <acl list> rate [drop-packets no-action lower-priority lower-priority-except-control tos-precedence-rewrite <num> tos-precedence-rewrite-lower-priority <num>] [allocate-resources-during-apply allocate-resources-during-traffic]</code>
<code>rate-limit <name> apply interface [<interface> all] [port <port>]</code>
<code>rate-limit disable master-rlbit <num> port-rewrite <num></code>
<code>rate-limit enable master-rlbit <num> port-rewrite <num></code>
<code>rate-limit <name> flow-aggregate acl <acl list> rate <rate> exceed-action <action> [sequence <number>] [min-bandwidth <min-bw>] [distribute-among <number-of-flows>]</code>
<code>rate-limit <name> input acl <acl list> rate <number> exceed-action <action> [sequence <number>]</code>
<code>rate-limit <name> port-level input port <port list> rate <num> [drop-packets no-action lower-priority lower-priority-except-control tos-precedence-rewrite <num> tos-precedence-rewrite-lower-priority <num>]</code>
<code>rate-limit <name> port-level slot <num> ignore-control-priority</code>
<code>rate-limit <name> port-level output port <port list> rate <num> drop-packets</code>
<code>rate-limit show [all] [policy-type flow-policies flow-aggregate-policies aggregate-policies portlevel-policies all] [policy-name <name>] [interface <interface>] [port-level port <port list> all-port] [port-level policy-name <name>] [rate-limiting-mode]</code>

rate-limit aggregate acl

Mode

Configure

Format

```
rate-limit <name> aggregate acl <acl list> rate [drop-packets | no-action | lower-priority |
lower-priority-except-control | tos-precedence-rewrite <num> |
tos-precedence-rewrite-lower-priority <num>] [allocate-resources-during-apply |
allocate-resources-during-traffic]
```

Description

Use the **rate-limit aggregate acl** command to specify the rate limiting policy for an *aggregation* of flows (all flows using the same ACLs). This rate limiting policy affects the whole aggregation and not individual flows. Enable aggregate rate limiting on individual line cards with the **system enable aggregate-rate-limiting** command.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limit.
acl	<acl list>	Specify the ACLs associated with the flows that will be rate limited.
	all	Specify all to include all the ACLs.
rate	<num>	Specify the rate limit, in bps, for the flow. The range for <num> is 3000 to 1000000000.
drop-packets		This optional parameter specifies that if the rate-limit is exceeded, the packets will be dropped.
no-action		This optional parameter specifies that if the rate-limit is exceeded, no action will be taken.
lower-priority		This optional parameter specifies that if the rate-limit is exceeded, the packet's priority is lowered.
lower-priority-except-control		This optional parameter specifies that if the rate-limit is exceeded, the packet's priority is lowered, except control packets.
tos-rewrite	<num>	Specify this option to rewrite the ToS byte when the rate limit is exceeded. The range for <num> is 0 to 255.
tos-rewrite-lower-priority <num>		Specify this option to rewrite the ToS byte and lower the priority when the rate limit is exceeded. The range for <num> is 0 to 255.

Parameter	Value	Meaning
tos-precedence-rewrite	<num>	This optional parameter specifies that if the rate-limit is exceeded, ToS precedence in the packet header will be rewritten to the value specified in <num>. The range for this value is 0 to 7.
tos-precedence-rewrite-lower-priority	<num>	This optional parameter specifies that if the rate-limit is exceeded, ToS precedence in the packet header will be rewritten to the value specified in <num>. The range for this value is 0 to 7.
allocate-resources-during-apply		This optional parameter allocates resources to the policy when it is applied to an interface.
allocate-resources-during-traffic		This optional parameter allocates resources to the policy when actual traffic flow is present.
time-select	<num>	Use this parameter to specify a time <i>slice</i> for a given rate limit policy. The range for <num> is 0 to 10. The default value is chosen by the software based on the specified rate.

Restrictions

None.

Example

To define an aggregate rate limiting policy based on the ACL *engacl*:

```
rs(config)# rate-limit eng aggregate acl engacl rate 10000000 drop-packets
allocate-resources-during-apply
```

rate-limit apply

Mode
Configure

Format

rate-limit <name> apply interface [<interface> | all] [port <port>]

Description

Use the **rate-limit apply** command to apply a previously-defined rate limiting policy to an IP interface or a port.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limiting policy.
interface	<interface>	The name of the interface.
	all	The keyword all applies the policy to all interfaces.
port	<port>	Specifies a single port.

Restrictions

None.

Example

To apply the rate limiting policy *engacl* to the interface *ip16*:

```
rs(config)# rate-limit engacl apply interface ip16
```

rate-limit disable

Mode

Configure

Format

```
rate-limit disable master-rlbit <num> | port-rewrite <num>
```

Description

Use the **rate-limit disable** command to disable rate limiting features on channels.

Parameter	Value	Meaning
master-rlbit	<num>	Specify to disable the master RL bit on a channel. The range for <num> is 1 to 32.
port-rewrite	<num>	Specify to disable port rewrite on a channel. The range for <num> is 1 to 32.

Restrictions

None.

Example

To disable port rewrite on channel 2:

```
rs(config)# rate-limit disable port-rewrite 2
```

rate-limit enable

Mode

Configure

Format

rate-limit enable master-rlbit <num> | port-rewrite <num>

Description

Use the **rate-limit enable** command to enable rate limiting features on channels.

Parameter	Value	Meaning
master-rlbit	<num>	Specify to enable master RL bit on a channel. The range for <num> is 1 to 32.
port-rewrite	<num>	Specify to enable port rewrite on a channel. The range for <num> is 1 to 32.

Restrictions

None.

Example

To enable master RL bit on channel 29:

```
rs(config)# rate-limit enable master-rlbit 29
```

rate-limit flow-aggregate

Mode

Configure

Format

```
rate-limit <name> flow-aggregate acl <acl list> rate <rate> exceed-action <action> [sequence <number>] [min-bandwidth <min-bw> | distribute-among <number-of-flows>]
```

Description

Use the **rate-limit flow-aggregate** command to specify software-based aggregate rate limiting.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limiting policy. The maximum length for <name> is 30 bytes.
acl	<acl list>	The ACL that defines a rate limiting policy. The rate-limit flow-aggregate command disregards the permit/deny keywords in the ACL rule definition. However, it does look at all parameters in the ACL rule.
rate	<rate>	The rate limit, in bps, for an aggregation of flows. The range for <rate> is 3000 to 1000000000.
exceed-action	<action>	The action taken if the rate limit is exceeded.
	drop-packets	Drop packets.
	set-priority-low	Sets the packet priority to low.
	set-priority-medium	Sets the packet priority to medium.
	set-priority-high	Sets the packet priority to high.
sequence	<number>	The sequence number for this policy. The range for <number> is 1 to 65535.
min-bandwidth	<min-bw>	The minimum bandwidth for each flow. The range for <min-bw> is 3000 to 1000000000.
distribute-among	<number-of-flows>	The number of flows among which freed bandwidth is distributed. The range for <number-of-flows> is 1 to 10. The default is 1.

Restrictions

None.

Example

The following example defines a rate limit profile *client1* for traffic from the 10.10.10.0 network. Packets will be dropped if the rate limit of 10 million bps is exceeded, and each flow will have a minimum bandwidth of 10,000 bps.

```
rs(config)# acl 100 permit ip 10.10.10.0/24 any  
rs(config)# rate-limit client1 flow-aggregate acl 100 rate  
100000000 exceed-action drop-packets min-bandwidth  
rs(config)# rate-limit apply client1 interface in1
```

rate-limit input acl

Mode

Configure

Format

```
rate-limit <name> input acl <acl list> rate <number> exceed-action <action> [sequence <number>]
```

Description

Use the **rate-limit input** command to specify a policy for per-flow rate limiting.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limiting policy. The maximum length for <name> is 30 bytes.
input acl	<acl list>	The ACLs defined in the per-flow rate limiting policy. The rate-limit input command disregards the permit/deny keywords in the ACL rule definition. However, the command does look at all parameters in the ACL rule.
rate	<number>	The rate limit, in bps, for the flow. The range of <number> is 3000 to 1000000000.
exceed-action	<action>	The action taken if the rate limit is exceeded.
	drop-packets	Drop packets.
	set-priority-low	Sets the packet priority to low.
	set-priority-medium	Sets the packet priority to medium.
	set-priority-high	Sets the packet priority to high.
sequence	<number>	The sequence number for this profile. The range of <number> is 1 to 65535.

Restrictions

None.

Example

The following command defines the rate limit policy *client1* for ACL *100*. The policy causes packets to be dropped if the rate limit of 10 million bps is exceeded.

```
rs(config)# rate-limit client1 input acl 100 rate 10000000  
exceed-action drop-packets
```


rate-limit port-level input

Mode

Configure

Format

```
rate-limit <name> port-level input port <port list> rate <num> [drop-packets | no-action |
lower-priority | lower-priority-except-control | tos-rewrite <num> | tos-precedence-rewrite
<num> | tos-rewrite-lower-priority <num> | tos-precedence-rewrite-lower-priority <num> |
time-select <num>]
```

Description

Use the **rate-limit port-level input** command to specify a rate limiting policy on a per-port basis. This policy only affects incoming traffic on the port. The policy applies to a specific port and not an aggregation of flows.



Note Enable port-level rate limiting on a per-line card basis with the **system enable aggregate-rate-limiting** command.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limit.
port	<port list>	Specify the ports on which to apply the rate-limiting policy.
	all-ports	Enables the rate-limiting policy on all ports.
rate	<num>	Specify the rate limit, in bps, for the flow. The range of <num> is 3000 to 1000000000.
drop-packets		This optional parameter specifies that if the rate-limit is exceeded, packets are dropped.
no-action		This optional parameter specifies that if the rate-limit is exceeded, no action is taken.
lower-priority		This optional parameter specifies that if the rate-limit is exceeded, packet priority is lowered.
lower-priority-except-control		This optional parameter specifies that if the rate-limit is exceeded, packet priority is lowered, except for control packets.
tos-rewrite	<num>	Specify this option if you want to rewrite the ToS byte when the rate limit is exceeded. The range for <num> is 0 to 255.

Parameter	Value	Meaning
tos-precedence-rewrite	<num>	This optional parameter specifies that if the rate-limit is exceeded, ToS precedence in the packet header is rewritten. The range for <num> is 0 to 7.
tos-rewrite-lower-priority	<num>	Specify this option to rewrite the ToS byte and lower the priority when the rate limit is exceeded. The range for <num> is 0 to 255.
tos-precedence-rewrite-lower-priority	<num>	This optional parameter specifies that if the rate-limit is exceeded, then ToS precedence in the packet header is rewritten and packet priority is lowered. The range for <num> is 0 to 7.
time-select	<num>	Use this parameter to specify a <i>time slice</i> for a given rate limit policy. The range for <num> is 0 to 10. The default value is chosen by the software based on the specified rate.

Restrictions

None.

Example

The following defines the port level rate limiting policy *department* for port et.2.1. The policy states that packets are dropped if a rate limit of 10 million bps is exceeded.

```
rs(config)# rate-limit department port-level input port et.2.1
rate 10000000 drop-packets
```

rate-limit port-level slot

Mode

Configure

Format

```
rate-limit <name> port-level slot <num> ignore-control-priority
```

Description

Use the **rate-limit port-level slot** command to configure slots to ignore control priority traffic. This means that there will be no rate limiting for control priority traffic. Note that this policy does not rate limit the traffic.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limiting policy.
slot	<num>	Specify the module or slot. The range for <num> is 1 to 32.
	all	Specify all to enable rate limiting on all modules or slots.
ignore-control-priority		This parameter specifies that if the rate-limit is exceeded, control priority packets will be ignored but not dropped.

Restrictions

None.

Example

The following defines the rate limiting policy *dontdrop*. This policy prevents control priority packets from being dropped if the rate limit of 10 million bps is exceeded.

```
rs(config)# rate-limit dontdrop port-level slot all ignore-control-priority
```

rate-limit port-level output

Mode
Configure

Format

rate-limit <name> port-level output port <port list> rate <num> drop-packets

Description

Use the **rate-limit port-level output** command to specify a policy for rate limiting on a per-port basis. This policy only affects outgoing traffic. The only exceed action available is **drop-packets**. This policy will only apply to a specific port and not an aggregation of flows.

Parameter	Value	Meaning
rate-limit	<name>	The name of the rate limit.
port	<port list>	Specify on which port to apply the rate-limiting policy.
	all-ports	Specify all-ports to enable rate limiting on all ports.
rate	<num>	The rate limit, in bps, for the flow. The range for <num> is 1000 to 1000000000.
drop-packets		This parameter specifies that if the rate-limit is exceeded, packets will be dropped.

Restrictions

None.

Example

The following defines a rate limit policy *department* for port et.2.1. The policy states that packets are dropped if a rate limit of 10 million bps is exceeded.

```
rs(config)# rate-limit department port-level output port et.2.1 rate 10000000 drop-packets
```

rate-limit show

Mode

Enable

Format

```
rate-limit show [all] | [policy-type flow-policies | flow-aggregate-policies |
aggregate-policies | portlevel-policies | all] | [policy-name <name>] | [interface <interface>] |
[port-level port <port list> | all-port] | [port-level policy-name <name>] | [rate-limiting-mode]
```

Description

The **rate-limit show** command displays information about rate limiting policies.

Parameter	Value	Meaning
show	all	Displays information on all rate limiting policies.
policy-type		The type of rate limiting policy.
	flow-policies	Displays all flow policies.
	flow-aggregate-policies	Displays all software-based flow-aggregate policies.
	aggregate-policies	Displays all aggregate policies.
	portlevel-policies	Displays all port level policies.
	all	Displays all rate limiting types.
policy-name	<name>	Displays rate limiting policies by name.
	all	Displays all rate limiting policies by name.
interface	<interface>	Displays rate limiting policies applied to interfaces.
	all	Displays all rate limiting policies applied to interfaces.
port-level port	<port list>	Displays rate limiting policies on a port.
	all-port	Displays rate limiting policies on all ports.
port-level policy-name	<name>	The name of the port-level rate limiting policy.
rate-limiting-mode		Displays the current rate limiting mode, either per-flow rate limiting or aggregate rate limiting.

Restrictions

None.

Example

To show all rate limit policies:

```
rs# rate-limit show all
```

Rate Limit Policy name : rlpol
Applied Interfaces : if0

ACL	Source IP/Mask	Dest. IP/Mask	SrcPort	DstPort	TOS	TOS-MASK	Prot
100	10.212.10.11/32	anywhere	any	any	any	None	IP
200	10.212.10.12/32	anywhere	any	any	any	None	IP
300	10.212.10.13/32	anywhere	any	any	any	None	IP
400	10.212.10.14/32	anywhere	any	any	any	None	IP
500	10.212.10.10/32	anywhere	any	any	any	None	IP

Seq	ACL	Rate Limit	Exceed Action	Credits	Time Interval
10	100	26000	Low Priority	218	8.59 sec
10	200	26000	Low Priority	218	8.59 sec
10	300	26000	Low Priority	218	8.59 sec
10	400	26000	Low Priority	218	8.59 sec
10	500	26000	Low Priority	218	8.59 sec

Table 56-1 Display Field Descriptions for the rate-limit show all Command

Field	Description
Rate Limit Policy Name	The name of the rate limit policy.
Applied Interfaces	The IP interface to which the rate limit is applied.
ACL	The name of the ACL that is associated with the rate limit.
Source IP/Mask	The source address and filtering mask specified by the ACL.
Dest. IP/Mask	The destination address and filtering mask specified by the ACL.
SrcPort	The number of the TCP or UDP source port.
DstPort	The number of the TCP or UDP destination port.
TOS	Type of Service.
TOS-MASK	The ToS mask.

Table 56-1 Display Field Descriptions for the rate-limit show all Command

Field	Description
Prot	The protocol for the ACL.
Seq	The sequence number for the policy.
ACL	The name of the ACL.
Rate Limit	The rate limit for the flow.
Exceed Action	The action to be taken if the rate limit is reached. Packets can be dropped or the priority set to low, medium, or high.
Credits	The number of credits allowed to pass in the <i>time interval</i> . This is a system-defined value. (The RS uses a hardware credit bucket algorithm for rate limiting).
Time Interval	The amount of time during which credits are allowed to pass. This is a system-defined value.

57 RDISC COMMANDS

The **rdisc** commands allow you to configure router advertisement on the RS.

57.1 COMMAND SUMMARY

The following table lists the **rdisc** commands. The sections following the table describe the command syntax.

rdisc add address <i><hostname-or-ipaddr></i>
rdisc add interface <i><name></i> all
rdisc set address <i><ipaddr></i> type multicast broadcast advertise enable disable preference <i><number></i> ineligible
rdisc set interface <i><name></i> all min-adv-interval <i><number></i> max-adv-interval <i><number></i> lifetime <i><number></i>
rdisc show
rdisc start
rdisc stop

rdisc add address

Mode

Configure

Format

rdisc add address *<hostname-or-ipaddr>*

Description

The **rdisc add address** command lets you define addresses to be included in router advertisements. If you configure this command, only the specified hostname(s) or IP address(es) are included in the router advertisements.

Parameter	Value	Meaning
address	<i><hostname-or-ipaddr></i>	Defines the hostname or IP address(es) to be included in the router advertisements.

Restrictions

None.

Example

To define an address to be included in router advertisements:

```
rs(config)# rdisc add address 10.10.5.254
```

rdisc add interface

Mode

Configure

Format

```
rdisc add interface <name>|all
```

Description

The **rdisc add interface** command lets you enable router advertisement on an interface. By default, all addresses on the interface are included in router advertisements sent by the RS. If you want to have only specific addresses included in router advertisements, use the **rdisc add address** command to specify those addresses.

Parameter	Value	Meaning
interface	<name>	The interface on which router advertisement is to be enabled.
	all	If all is specified, then router advertisement is enabled on all interfaces. By default, router advertisement is disabled on all interfaces.

Restrictions

None.

Example

To enable router advertisement on an interface:

```
rs(config)# rdisc add interface rs4
```

rdisc set address

Mode

Configure

Format

```
rdisc set address <ipaddr> type multicast|broadcast advertise enable|disable preference <number> |ineligible
```

Description

The **rdisc set address** command lets you specify the type of router advertisement in which the address is included and the preference of the address for use as a default route.

Parameter	Value	Meaning
address	<ipaddr>	Specifies the IP address.
type		Specifies the type of router advertisement in which the IP address is to be included.
	multicast	Specifies that the IP address should only be included in a multicast router advertisement. This is the default.
	broadcast	Specifies that the IP address should only be included in a broadcast router advertisement, even if IP multicast is available.
advertise		Specifies whether the IP address is included in the router advertisements.
	enable	Include the IP address in router advertisements. This is the default.
	disable	Do not include the IP address in router advertisements.
preference	<number>	Specifies the degree of preference of the IP address as a default route. The higher the value, the more preference. The default value is 0.
	ineligible	If the IP address is ineligible to be a default route, specify ineligible.

Restrictions

None

Examples

To specify that an address be included only in broadcast router advertisements and that the address is ineligible to be a default route:

```
rs#(config) rdisc set address 10.20.36.0 type broadcast preference ineligible
```

rdisc set interface

Mode

Configure

Format

```
rdisc set interface <name> [all min-adv-interval <number> max-adv-interval <number> lifetime <number>
```

Description

The **rdisc set interface** command lets you specify the intervals between the sending of router advertisements and the lifetime of addresses sent in a router advertisement.

Parameter	Value	Meaning
interface	<name>	Specifies the name of the interface.
	all	If all is specified, then the parameters set apply to all interfaces.
min-adv-interval	<number>	Specifies the minimum time, in seconds, allowed between the sending of unsolicited broadcast or multicast router advertisements. This value can be between 3-1800. The default is 0.75 times the max-adv-interval value.
max-adv-interval	<number>	Specifies the maximum time, in seconds, allowed between the sending of unsolicited broadcast or multicast router advertisements. This value can be between 4-1800. The default value is 600 seconds.
lifetime	<number>	Specifies the lifetime, in seconds, of addresses in a router advertisement. This value can be between 4-9000. The default is 3 times the max-adv-interval value.

Restrictions

None

Examples

To specify the maximum time between the sending of router advertisements on an interface:

```
rs#(config) rdisc set interface rs4 max-adv-interval 1200
```

Note that since the **min-adv-interval** and **lifetime** parameters were not specified, the default values for those parameters become 900 seconds and 3600 seconds, respectively.

rdisc show

Mode

Enable

Format

rdisc show all

Description

The **rdisc show** command shows the state of router discovery on the RS.

Parameter	Value	Meaning
show	all	Displays all router discovery information.

Restrictions

None.

Examples

To display router discovery information:

```
rs# rdisc show all

Task State: <Foreground NoResolv NoDetach> ❶

    Send buffer size 2048 at 812C68F8
    Recv buffer size 2048 at 812C60D0

Timers:

    RouterDiscoveryServer Priority 30

        RouterDiscoveryServer_RS2_RS3_IP <OneShot>
            last: 10:17:21 next: 10:25:05 ❷

Task RouterDiscoveryServer:
    Interfaces:
        Interface RS2_RS3_IP: ❸
            Group 224.0.0.1: ❹
                minadvint 7:30 maxadvint 10:00 lifetime 30:00 ❺

                Address 10.10.5.254: Preference: ❻

    Interface policy:
        Interface RS2_RS3_IP* MaxAdvInt 10:00 ❼
```

Legend:

1. Information about the RDISC task.
2. Shows when the last router advertisement was sent and when the next advertisement will be sent.
3. The interface on which router advertisement is enabled.
4. Multicast address.
5. Current values for the intervals between the sending of router advertisements and the lifetime of addresses sent in a router advertisement.
6. IP address that is included in router advertisement. The preference of this address as a default route is 0, the default value.
7. Shows configured values for the specified interface.

rdisc start

Mode

Configure

Format

rdisc start

Description

The **rdisc start** command lets you start router discovery on the RS. When router discovery is started, the RS multicasts or broadcasts periodic router advertisements on each configured interface. The router advertisements contain a list of addresses on a given interface and the preference of each address for use as the default route on the interface. By default, router discovery is disabled.

Restrictions

None

rdisc stop

Mode

Configure

Format

rdisc stop

Description

The **rdisc stop** command stops router discovery on the RS, thereby stopping router advertisements from being sent out.

Restrictions

None

58 REBOOT COMMAND

reboot

Mode

Enable

Format

reboot

Description

The reboot command reboots the RS.

Restrictions

None.

59 RIP COMMANDS

The Routing Information Protocol, Version 1 and Version 2 (RIPv1 and RIPv2), is the most commonly used interior gateway protocol. RIP selects the route with the lowest metric as the best route. The metric is a hop count representing the number of gateways through which data must pass in order to reach its destination. The longest path that RIP accepts is 15 hops. If the metric is greater than 15, a destination is considered unreachable and the RS discards the route. RIP assumes that the best route is the one that uses the fewest gateways, that is, the shortest path. RIPv1 is described in RFC 1058 and RIPv2 is described in RFC 1723.

59.1 COMMAND SUMMARY

The following table lists the **rip** commands. The sections following the table describe the command syntax.

<code>rip add interface <interfacename-or-IPaddr></code>
<code>rip add source-gateways <hostname-or-IPaddr></code>
<code>rip add trusted-gateways <hostname-or-IPaddr></code>
<code>rip set auto-summary disable enable</code>
<code>rip set broadcast-state always choose never</code>
<code>rip set check-zero disable enable</code>
<code>rip set check-zero-metric disable enable</code>
<code>rip set default-metric <num></code>
<code>rip set interface <interfacename-or-IPaddr> all [receive-rip enable disable] [send-rip enable disable] [metric-in <num>] [metric-out <num>] [version 1 version 2 [type broadcast multicast]] authentication-method [none (simple md5 key-chain <num-or-string>)][xmt-actual enable disable]</code>
<code>rip set max-routes <num></code>
<code>rip set multipath off</code>
<code>rip set poison-reverse disable enable</code>
<code>rip set preference <num></code>
<code>rip show <option-list></code>
<code>rip start</code>

rip stop
rip trace [packets request response local-options] [detail] [send receive]

rip add interface

Mode

Configure

Format

```
rip add interface <interfacename-or-IPaddr>|all
```

Description

By default, RIP is disabled on all RS interfaces. To enable RIP on an interface, you must use the `rip add interface` command.

Parameter	Value	Meaning
interface		Informs the RIP process about the specified interfaces.
	<interfacename-or-IPaddr>	You can specify a list of interface names or IP addresses.
	all	Use the all keyword to specify all interfaces.

Restrictions

None.

rip add source-gateways

Mode
Configure

Format

rip add source-gateways <hostname-or-IPaddr>

Description

The `rip add source-gateways` command lets you add routers that send RIP updates directly, rather than through broadcast or multicast.



Note Updates to source gateways are not affected by the RIP packet transmission state of the interface.

Parameter	Value	Meaning
source-gateways	<hostname-or-IPaddr>	The hostname or IP address of the source gateway.

Restrictions

None.

rip add trusted-gateways

Mode

Configure

Format

rip add trusted-gateways *<hostname-or-IPaddr>*

Description

The `rip add trusted-gateways` command lets you add trusted gateways, from which the RS will accept RIP updates. when you add trusted gateways, the RS does not accept RIP updates from sources other than those trusted gateways.

Parameter	Value	Meaning
trusted-gateways	<i><hostname-or-IPaddr></i>	The hostname or IP address of the source or trusted gateway.

Restrictions

None.

rip set auto-summary

Mode

Configure

Format

```
rip set auto-summary disable | enable
```

Description

The **rip set auto-summary** command specifies that routes to subnets should be automatically summarized by the classful network boundary and redistributed into RIP.

Parameter	Value	Meaning
auto-summary	disable	Disables automatic summarization and redistribution of RIP routes.
	enable	Enables automatic summarization and redistribution of RIP routes.

Restrictions

None.

rip set broadcast-state

Mode

Configure

Format

rip set broadcast-state always | choose | never

Description

The `rip set broadcast-state` command specifies whether the RS broadcasts RIP packets regardless of the number of interfaces present. This is useful when propagating static routes or routes learned from another protocol into RIP. In some cases, the use of broadcast when only one network interface is present can cause data packets to traverse a single network twice.

Parameter	Value	Meaning
broadcast-state		Specifies whether the RS broadcasts RIP packets regardless of the number of interfaces present.
	always	Always sends RIP broadcasts regardless of the number of interfaces present.
	choose	Sends RIP broadcasts only if more than one interface is configured on the RS. This is the default state.
	never	Never sends RIP broadcasts on attached interfaces.

Restrictions

None.

rip set check-zero

Mode

Configure

Format

```
rip set check-zero disable | enable
```

Description

The **rip set check-zero** command specifies whether RIP should make sure that reserved fields in incoming RIP V1 packets are zero. RIP will reject packets where the reserved fields are non-zero.

- If you use the **disable** keyword, RIP does not check the reserved field.
- If you use the **enable** keyword, RIP on the RS checks to ensure that the reserved fields in incoming RIP packets are zero. If the reserved field in a RIP packet is not zero, the RS discards the packet. This is the default state.

Parameter	Value	Meaning
check-zero	disable	Disables checking of the reserved field.
	enable	Enables checking of the reserved field.

Restrictions

None.

rip set check-zero-metric

Mode

Configure

Format

rip set check-zero-metric disable | enable

Description

The `rip set check-zero-metric` command specifies whether RIP should accept routes with a metric of zero. This may be necessary for interoperability with other RIP implementations that send routes with a metric of zero.

- If you use the `disable` keyword, RIP accepts routes that have a metric of zero and treats them as though they were received with a metric of 1.
- If you use the `enable` keyword, RIP rejects routes that have a metric of zero. This is the default state.

Parameter	Value	Meaning
check-zero-metric	disable	Disables acceptance of RIP routes that have a metric of zero.
	enable	Enables acceptance of RIP routes that have a metric of zero.

Restrictions

None.

rip set default-metric

Mode

Configure

Format

```
rip set default-metric <num>
```

Description

The `rip set default metric` command defines the metric used when advertising routes via RIP that were learned from other protocols. If not specified, the default value is 16 (unreachable). This choice of values requires you to explicitly specify a metric in order to export routes from other protocols into RIP. This metric may be overridden by a metric specified in the `export` command.



Note

The metric 16 is equivalent in RIP to “infinite” and makes a route unreachable. You must set the default metric to a value other than 16 in order to allow the RS to export routes from other protocols such as OSPF and BGP-4 into RIP.

Parameter	Value	Meaning
default-metric	<num>	Specifies the metric. Specify a number from 1 – 16. The default is 16.

Restrictions

None.

rip set interface

Mode

Configure

Format

```
rip set interface <interfacename-or-IPaddr> | all [advertise-classfull enable | disable ]
[receive-rip enable | disable] [send-rip enable | disable] [metric-in <num>]
[metric-out <num>][version 1|version 2 [type broadcast|multicast]]
[authentication-method none|(simple|md5 key-chain <num-or-string>)] [xmt-actual
enable|disable]
```

Description

The **rip set interface** command lets you set the following parameters for RIP interfaces:

- Whether the interface will accept RIP updates
- Whether the interface will send RIP updates
- The RIP version (RIP V1 or RIP V2)
- The packet type used for RIP V2 updates (broadcast or multicast)
- The metric added to incoming RIP updates
- The metric added to outgoing RIP updates
- The key-chain for RIP update authentication
- The authentication method used for RIP updates (none, simple, or MD5)

Parameter	Value	Meaning
interface	<interfacename-or-IPaddr>	The interface names or IP addresses of the interfaces for which you are setting RIP parameters.
	all	Specify the all keyword if you want to set RIP parameters for all IP interfaces on the RS.
advertise-classfull	enable	This command is used to announce a classfull network onto a subnetted RIPVersion 1 interface having the same classfull network.
	disable	
receive-rip		This option affects RIP updates sent from trusted gateways.
	enable	Specify enable if you want to receive RIP updates on the interface. The default is enable . If you specify enable and you have set up trusted gateways, the RS will accept updates only from those trusted gateways.

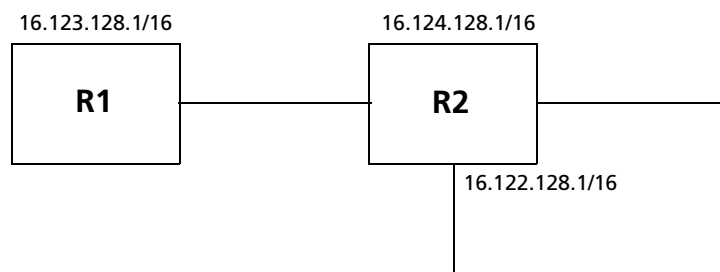
Parameter	Value	Meaning
	disable	If you specify disable , the RS will not receive any RIP updates, including those sent from trusted gateways.
send-rip		Specifies whether the interface(s) can send RIP updates. This option does not affect the sending of updates to source gateways.
	enable	Specify enable if you want to send RIP updates from this interface. The default is enable .
	disable	Specify disable if you <i>don't</i> want to send RIP updates from this interface.
metric-in	<num>	Specifies a metric that the interface adds to incoming RIP routes before adding them to the interface table. Specify a metric from 1 – 16. Use this option to make the RS prefer RIP routes learned from the specified interfaces less than RIP routes from other interfaces. The default is 1.
metric-out	<num>	Specifies a metric that the interface adds to outgoing RIP routes sent through the specified interfaces. The default is 0. Use this option to make other routers prefer other sources of RIP routes over this router.
version 1		Specifies that RIP version 1 is used on the interface(s).
version 2		Specifies that RIP version 2 is used on the interface(s).
type	broadcast	Causes RIP V2 packets that are RIP V1-compatible to be broadcast on this interface.
	multicast	Causes RIP V2 packets to be multicasted on this interface; this is the default.
authentication-method		The authentication method the interface uses to authenticate RIP updates.
	none	The interface does not use any authentication.
	simple	The interface uses a simple password in which an authentication key of up to 8 characters is included in the packet. If you choose this method, you must also specify a key-chain identifier using the key-chain option.
	md5	The interface uses MD5 authentication. This method uses the MD5 algorithm to create a crypto-checksum of a RIP packet and an authentication key of up to 16 characters. If you choose this method, you must also specify a key-chain identifier using the key-chain option.

Parameter	Value	Meaning
key-chain	<num-or-string>	The identifier of the key-chain containing the authentication keys. This parameter applies only if you specified simple or md5 for the authentication type.
xmt-actual		Enables or disables poison reverse/split horizon feature. Poison reverse/split horizon prevents loops.
	enable	Disables poison reverse/split horizon.
	disable	Enables poison reverse/split horizon.

Restrictions

None.

Example



In this example, router R1 has the following three interfaces:

1. It is connected to router R2 over interface 16.123.128.1/16. It is running RIP version 1 on this interface.
2. It has two other interfaces with the following addresses (16.124.128.1/16, 16.122.128.1/16).
3. Router R1 the entire class A network (16.0.0.0/8) behind it.

By default, router R1 would not announce a classful network (16.0.0.0/8) over a subnet (16.123.128.1/16). If that is something which is desired, then the below given command should be entered.

```
rip set interface 16.123.128.1 advertise-classfull enable | disable
```

Typically, a user would enable automatic summarization for RIP. This would create an implicit aggregate 16.0.0.0/8. If it is desired, that this classfull network is announced over a subnetted RIP Version 1 interface, then the above command should be entered.

rip set max-routes

Mode

Configure

Format

```
rip set max-routes <num>
```

Description

The **rip set max-routes** command defines the maximum number of RIP routes that can be maintained by the Routing Information Base (RIB).

Parameter	Value	Meaning
max-routes	<num>	Specifies the maximum number of routes. Specify a number from 1 – 4. The default is 4.

Restrictions

None.

rip set multipath

Mode

Configure

Format

```
rip set multipath off
```

Description

The **rip set multipath** command disables multipath route calculation for RIP routes. No multipath forwarding occurs when this command is used.

Parameter	Value	Meaning
multipath	off	Disables multipath route calculation.

Restrictions

None.

rip set poison-reverse

Mode
Configure

Format

rip set poison-reverse disable | enable

Description

The **rip set poison-reverse** command allows you to enable or disable poison reverse on all RS interfaces. The RS supports poison reverse as specified by RFC 1058.



Note Turning on poison reverse will approximately double the amount of RIP updates.

Parameter	Value	Meaning
disable		Disables poison reverse on the RS.
enable		Enables poison reverse on the RS.

Restrictions

None.

rip set preference

Mode

Configure

Format

rip set preference <num>

Description

The **rip set preference** command sets the preference for destinations learned through RIP. The preference you specify applies to all IP interfaces for which RIP is enabled on the RS. The default preference is 100. You can override this preference by specifying a different preference in an import policy.

Parameter	Value	Meaning
preference	<num>	Specifies the preference. Specify a number from 0 – 255. The default is 100. Lower numbers have higher preference.

Restrictions

None.

rip show

Mode

Enable

Format

rip show <option-list>

Description

The **rip show** command displays RIP information.

Parameter	Value	Meaning
show	<option-list>	Specifies the RIP dump information you want to display.
	all	Displays all RIP tables.
	globals	Displays RIP globals.
	timers	Displays RIP timers.
	interface	Displays RIP interfaces.
	active-gateways	Displays active gateways running RIP.
	interface-policies	Displays RIP interface policies.
	import-policies	Displays RIP import policies.
	export-policies	Displays RIP export policies.

Restrictions

None.

rip start

Mode

Configure

Purpose

Start RIP on the RS.



Note RIP is disabled by default.

Format

```
rip start
```

Description

The **rip start** command starts RIP on all IP interfaces on the RS for which RIP is enabled.

Restrictions

None.

rip stop

Mode

Configure

Purpose

Stop RIP on the RS.

Format

```
rip stop
```

Description

The **rip stop** command stops RIP on all IP interfaces on the RS for which RIP is enabled.

Restrictions

None.

rip trace

Mode

Configure

Purpose

Trace RIP packets.

Format

```
rip trace [packets|request|response|local-options] [detail | send|receive]
```

Description

The **rip trace** command traces the following sets of RIP packets:

- RIP request packets sent or received by the RS
- RIP response packets sent or received by the RS

Depending on the options you specify, you can trace all packets, request packets only, or receive packets only. In addition, you can select to trace the request packets, receive packets, or both that are sent by the RS, received by the RS, or all packets (both sent packets and received packets).

local-optionsSets trace options for this protocol only. Specify one or more of the following:

Parameter	Value	Meaning
packets		Traces all RIP packets, both request packets and response packets. This is the default.
request		Traces only request packets, such as REQUEST, POLL and POLLENTY packets.
response		Traces only response packets.
local-options		Sets trace options for this protocol only. These trace options are inherited from those set by the ip-router global set trace options command, or you can override them here.
	all	Turns on all tracing.
	general	Turns on normal and route tracing.
	state	Traces state machine transitions in the protocols.
	normal	Traces normal protocol occurrences. (Abnormal protocol occurrences are always traced.)
	policy	Traces application of protocol and user-specified policies to routes being imported and exported.
	task	Traces system processing associated with this protocol or peer.
	timer	Traces timer usage by this protocol or peer.

Parameter	Value	Meaning
	route	Traces routing table changes for routes installed by this protocol or peer.
detail		Shows detailed information about the traced packets.
send		Shows information about traced RIP packets received by the RS.
receive		Shows information about traced RIP packets sent by the RS.The default is to show both send and receive packets.

Restrictions

None.

60 RMON COMMANDS

The **rmon** commands let you display and set parameters for RMON statistics on a per-port basis. RMON information corresponds to RFCs 1757 and 2021.

60.1 COMMAND SUMMARY

The following table lists the **rmon** commands. The sections following the table describe the command syntax.

<code>rmon address-map index <index-number> port <port> [owner <string>] [status enable disable]</code>
<code>rmon al-matrix-top-n index <index-number> matrix-index <number> ratebase terminal-packets terminal-octets all-packets all-octets duration <number> size <number> [owner <string>] [status enable disable]</code>
<code>rmon alarm index <index-number> variable <string> [interval <seconds>] [falling-event-index <num>] [falling-threshold <num>] [owner <string>] [rising-event-index <num>] [rising-threshold <num>] [startup rising falling both] [status enable disable] [type absolute-value delta-value]</code>
<code>rmon apply cli-filters <filter id></code>
<code>rmon capture index <index-number> channel-index <number> [full-action lock wrap] [slice-size <number>] [download-slice-size <number>] [download-offset <number>] [max-octets <number>] [owner <string>] [status enable disable]</code>
<code>rmon channel index <index-number> port <port> [accept-type matched failed] [data-control on off] [turn-on-event-index <number>] [turn-off-event-index <number>] [event-index <number>] [channel-status ready always-ready] [description <string>] [owner <string>] [status enable disable]</code>
<code>rmon clear cli-filter</code>
<code>rmon enable</code>
<code>rmon etherstats index <index-number> port <port> [owner <string>] [status enable disable]</code>
<code>rmon event index <index-number> type none log trap both [community <string>] [description <string>] [owner <string>] [status enable disable]</code>

rmon filter index <index-number> channel-index <number> [data-offset <number>] [data <string>] [data-mask <string>] [data-not-mask <string>] [pkt-status <number>] [status-mask <number>] [status-not-mask <number>] [owner <string>] [status enable disable]
rmon history index <index-number> port <port> [interval <seconds>] [owner <string>] [samples <num>] [status enable disable]
rmon hl-host index <index-number> port <port> nl-max-entries <number> al-max-entries <number> [owner <string>] [status enable disable]
rmon hl-matrix index <index-number> port <port> nl-max-entries <number> al-max-entries <number> [owner <string>] [status enable disable]
rmon host index <index-number> port <port> [owner <string>] [status enable disable]
rmon host-top-n index <index-number> host-index <number> [base <statistics>] [duration <time>] [size <size>] [owner <string>] [status enable disable]
rmon matrix index <index-number> [port <port>] [owner <string>] [status enable disable]
rmon nl-matrix-top-n index <index-number> matrix-index <number> ratebase terminal-packets terminal-octets all-packets all-octets duration <number> size <number> [owner <string>] [status enable disable]
rmon protocol-distribution index <index-number> port <port> [owner <string>] [status enable disable]
rmon set lite standard professional default-tables yes no
rmon set cli-filter <filter-id> <parameter>
rmon set memory <number>
rmon set ports <port list> allports
rmon set protocol-directory <protocol> all-protocols [address-map on off na] [host on off na] [matrix on off na]
rmon show <rmon-parm>
rmon user-history-apply <groupname> to <user-history-index>
rmon user-history-control index <index-number> objects <number> samples <number> interval <number> [owner <string>] [status enable disable]
rmon user-history-objects <groupname> variable <oid> type absolute delta [status enable disable]

rmon address-map

Mode

Configure

Format

```
rmon address-map index <index-number> port <port> [owner <string>] [status enable|disable]
```

Description

The Address Map group maps MAC addresses to network address bindings that are discovered by the RS on a per-port basis. The **rmon address-map** command sets various parameters of the RMON 2 Address Map table.

If the default tables were turned on for the Professional group, an entry in the Address Map control table is created for each available port.

Use the **rmon show address-map** command to display the address map.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Address Map table.
port	<port>	Specifies the port from which to collect data.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables or disables this matrix.The default is enable.
	disable	Disables this matrix.

Restrictions

None.

Example

To create an entry in the Address Map table for port et.1.3:

```
rs(config)# rmon address-map index 20 port et.1.3
```

rmon al-matrix-top-n

Mode

Configure

Format

```
rmon al-matrix-top-n index <index-number> matrix-index <number> ratebase  
terminal-packets|terminal-octets|all-packets|all-octets duration <number> size <number>  
[owner <string>] [status enable|disable]
```

Description

The **rmon al-matrix-top-n** command gathers the top *n* Application Layer Matrix entries sorted by a specified statistic. To do this, you must first configure the Application Layer/Network Layer Matrix table using the **rmon hl-matrix** command.

Use the **rmon show al-matrix-top-n** command to display the top *n* Application Layer Matrix entries.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the application layer matrix table.
matrix-index	<number>	Specifies the index into the hl-matrix table. The default is 0.
ratebase		Specifies the sorting method.
	terminal-packets	Sort by terminal packets.
	terminal-octets	Sort by terminal octets.
	all-packets	Sort by all packets.
	all-octets	Sort by all octets.
duration	<number>	Specifies the duration, in seconds, between reports. If the duration is 0 (the default), this implies that no reports have been requested for this entry. The default is 0.
size	<number>	Specifies the maximum number of matrix entries to include in the report. The default is 150.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables or disables this matrix. The default is enable.
	disable	Disables this matrix.

Restrictions

None.

Example

To monitor the top n entries in the Application Layer Matrix, you should first configure the Application Layer/Network Layer Matrix table using the **rmon hl-matrix** command. Then, to gather the top 100 Application Layer Matrix entries sorted by all packets, use the following command:

```
rs(config)# rmon al-matrix-top-n index 25 matrix-index 50 ratebase  
all-packets duration 60 size 100
```

rmon alarm

Mode

Configure

Format

```
rmon alarm index <index-number> variable <string> [interval <seconds>] [falling-event-index <num>] [falling-threshold <num>] [owner <string>] [rising-event-index <num>] [rising-threshold <num>] [startup rising|falling|both] [status enable|disable] [type absolute-value|delta-value]
```

Description

The Alarm group takes periodic statistical samples and compares them with previously-configured thresholds. If a monitored variable crosses a threshold, an alarm is generated. The **rmon alarm** command sets various parameters of the RMON 1 Alarm control table.

Use the **rmon show alarm** command to display the alarm data.

Parameter	Value	Meaning
index	<index-number>	Is a number that uniquely identifies an entry in the alarm table. The value must be between 1 and 65535, inclusive.
variable	<string>	Specifies the object identifier of the variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER may be sampled.
interval	<seconds>	Specifies the sampling interval in seconds when statistical samples of variables are collected and compared to the rising and falling thresholds. The value must be between 1 and 2147483647, inclusive.
falling-event-index	<num>	Is the action to be taken as defined by the row with this index in the event table when a falling threshold is crossed. The value must be between 1 and 65535, inclusive.
falling-threshold	<num>	Specifies that the sample's value must be less than or equal to the threshold to trigger an alarm. When the sample's value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. The value must be between -2147483647 and 2147483647, inclusive.
owner	<string>	Specifies the owner of the alarm resource; for example, an IP address, machine name or person's name.
rising-event-index	<num>	Is the action to be taken as defined by the row with this index in the event table when a rising threshold is crossed. The value must be between 1 and 65535, inclusive.

Parameter	Value	Meaning
rising-threshold	<num>	Specifies that the sample's value must be greater than or equal to the threshold to trigger an alarm. When the sample's value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. The value must be between -2147483647 and 2147483647, inclusive.
startup	<keyword>	Specifies the condition for which the alarm is to be generated.
	rising	Causes an alarm to be generated if the sampled variable is greater than or equal to the rising threshold.
	falling	Causes an alarm to be generated if the sampled variable is less than or equal to the falling threshold.
	both	Causes an alarm to be generated if the sampled variable is greater than or equal to the rising threshold or less than or equal to the falling threshold.
status	enable	Enables this alarm.
	disable	Disables this alarm.
type	<keyword>	Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds.
	absolute-value	Monitor the absolute value over the sample interval of the variable against the threshold value.
	delta-value	Monitor the change in value over the sample interval of the variable against the threshold value.

Restrictions

None.

Examples

To cause an alarm event if the variable defined in alarm 10 crosses the rising threshold:

```
rs(config)# rmon alarm index 10 startup rising interval 30 variable
1.3.6.1.2.1.5.14.0 rising-threshold 40 rising-event-index 1
```

To monitor the absolute value of the variable against a threshold value:

```
rs(config)# rmon alarm index 10 type absolute-value startup rising
interval 30 variable 1.3.6.1.2.1.5.14.0 rising-threshold 40
rising-event-index 1
```

To specify Mike as the owner of alarm 10:

```
rs(config)# rmon alarm index 10 owner Mike type absolute-value startup  
rising interval 30 variable 1.3.6.1.2.1.5.14.0 rising-threshold 40  
rising-event-index 1
```

To specify a 5-second interval on alarm 10:

```
rs(config)# rmon alarm index 10 interval 5 type absolute-value startup  
rising interval 30 variable 1.3.6.1.2.1.5.14.0 rising-threshold 40  
rising-event-index 1
```

To specify the rising threshold at 10 on alarm 10:

```
rs(config)# rmon alarm index 10 rising-threshold 10 type delta-value  
startup rising interval 30 variable 1.3.6.1.2.1.5.14.0  
rising-event-index 1
```

rmon apply cli-filters

Mode

Enable

Format

```
rmon apply cli-filters <filter id>
```

Description

The **rmon apply cli-filters** command applies a specific CLI RMON filter to the current Telnet or Console session. This enables different users to select the different CLI filters which you should define using the **rmon set cli-filter** command.

Use the **rmon show cli-filters** command to see the RMON CLI filters that have been defined on the RS. Use the **rmon clear cli-filter** command to clear the applied filter.

Parameter	Value	Meaning
cli-filters	<filter id>	Is a number between 1 and 65535 that identifies the filter ID to apply.

Restrictions

None.

Example

To apply filter ID 2:

```
rs> rmon apply cli-filters 2
```

To see a list of CLI RMON filters:

```
rs> rmon show cli-filters
RMON CLI Filters
Id  Filter
--  -----
 1  (inpkts >= 0)
 2  (inpkts >= 0 and outoctets >= 0)
 3  srcmac 222222222222 and (outoctets >= 0)
You have selected a filter: (inpkts >= 0)
```

rmon capture

Mode

Configure

Format

```
rmon capture index <index-number> channel-index <number> [full-action lock|wrap]
[slice-size <number>] [download-slice-size <number>] [download-offset <number>]
[max-octets <number>] [owner <string>] [status enable|disable]
```

Description

The Packet Capture group allows packets to be captured after they have flowed through a channel. The **rmon capture** command sets various parameters of the RMON 1 Packet Capture table.

Use the **rmon show packet-capture** command to display the Packet Capture table.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Packet Capture table.
channel-index	<number>	Is a number between 1 and 65535 that identifies the channel that is the source of packets. The default is 0.
full-action		Specifies the action of the buffer when it reaches the full status,
	lock	Stop capturing packets when the buffer reaches the full status.
	wrap	Wrap around when the buffer reaches the full status.
slice-size	<number>	Is a number between 0 and 2147483647 that is the maximum number of octets that will be saved in this capture buffer. The default is 100.
download-slice-size	<number>	Is a number between 0 and 2147483647 that is the maximum number of octets that will be returned in an SNMP retrieval. The default is 100.
download-offset	<number>	Is a number between 0 and 2147483647 that is the offset of the first octet of each packet that will be returned in an SNMP retrieval. The default is 0.
max-octets	<number>	Is a number between 0 and 2147483647 that is maximum number of octets to be saved. The default is 1.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables or disables this channel. The default is enable.
	disable	Disables this channel.

Restrictions

None.

Example

To create an entry in the Packet Capture table:

```
rs(config)# rmon capture index 20 channel-index 1 full-action wrap
```

rmon channel

Mode

Configure

Format

```
rmon channel index <index-number> port <port> [accept-type matched|failed] [data-control on|off] [turn-on-event-index <number>] [turn-off-event-index <number>] [event-index <number>] [channel-status ready|always-ready] [description <string>] [owner <string>] [status enable|disable]
```

Description

The Filter Channel group must be configured in order to configure the Filter group. The **rmon channel** command sets various parameters of the RMON 1 Filter Channel table. After a channel row has been created, a filter must be defined with the **rmon filter** command.

Use the **rmon show channels** command to display all the channels configured on the RS.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Filter Channel table.
port	<port>	Identifies the port from which data is collected.
accept-type		Specifies the action of the filters associated with this channel.
	matched	Packets will be accepted if they are accepted by both the packet data and packet status matches of an associated filter.
	failed	Packets will be accepted only if they fail either the packet data match or the packet status match of each of the associated filters.
data-control		Specifies the flow control of the data
	on	Implies data, status, and events flow through this channel.
	off	Implies data, status, and events will not flow through this channel.
turn-on-event-index	<number>	Is a number between 0 and 65535 that identifies the event configured to turn the associated data control from off to on.
turn-off-event-index	<number>	Is a number between 0 and 65535 that identifies the event configured to turn the associated data control from on to off.
event-index	<number>	Is a number between 0 and 65535 that identifies the event configured to be generated when the associated data control is on and a packet is matched.
channel-status		Specifies the status.

Parameter	Value	Meaning
	ready	A single event is generated.
	always-ready	Allows events to be generated at will.
description	<string>	Describes this channel in a maximum of 127 bytes.
owner	<string>	Specifies the owner of packet capture; for example, an IP address, machine name or person's name.
status	enable	Enables this channel. The default is enable.
	disable	Disables this channel.

Restrictions

None.

Example

To create an entry in the Filter Channel table:

```
rs(config)# rmon channel index 25 port et.1.3 accept-type matched data-control on  
turn-on-event-index 30 turn-off-event-index 55 event-index 60 channel-status ready
```

rmon clear cli-filter

Mode

Enable

Format

```
rmon clear cli-filter
```

Description

The **rmon clear cli-filter** command clears the CLI RMON filter that was applied with the **rmon apply cli-filters** command.

Restrictions

None.

rmon enable

Mode

Configure

Format

```
rmon enable
```

Description

When the RS is booted, RMON is off by default. The **rmon enable** command turns RMON on. At least one of the Lite, Standard, or Professional RMON groups must be configured first before you can turn on RMON. Use the **rmon set** command to configure the Lite, Standard, or Professional RMON groups.

To disable RMON, the **rmon enable** command must be negated. This frees up all resources associated with RMON, including any memory allocated to RMON.

Restrictions

If the SNMP agent is disabled, RMON cannot be enabled. If RMON is enabled and the SNMP agent is disabled, then RMON will be turned off.

rmon etherstats

Mode

Configure

Format

```
rmon etherstats index <index-number> port <port> [owner <string>] [status enable|disable]
```

Description

The Etherstats group contains statistics for RS ports. The **rmon etherstats** command sets various parameters of the RMON 1 Etherstats control table. If default tables were turned on for the Lite group, a entry is created in the Etherstats control table for each available port.

Use the **rmon show etherstats** command to display the Etherstats data.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Etherstats control table.
port	<port>	Specifies the physical port from which to collect data.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables or disables this Etherstat. The default is enable.
	disable	Disables this Etherstat.

Restrictions

None.

Example

To create an entry in the Etherstats control table:

```
rs(config)# rmon etherstats index 10 port et.1.3
```

rmon event

Mode

Configure

Format

```
rmon event index <index-number> type none|log|trap|both [community <string>] [description <string>] [owner <string>] [status enable|disable]
```

Description

The Event group controls the generation and notification of events. The **rmon event** command sets various parameters of the RMON 1 Event control table.

Use the **rmon show event** command to display the event data.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies an entry in the Event table.
type		Specifies what action to be taken when the event occurs.
	none	Causes no notification to be sent for the event.
	log	Causes an entry for the event to be made in the log table for each event.
	trap	Causes an SNMP trap to be sent to one or more management stations for the event.
	both	Causes both an entry to be made in the log table and an SNMP trap to be sent to one or more management stations.
community	<string>	Specifies the SNMP community string to be sent with the trap. If an SNMP trap is to be sent, it will go to the SNMP community specified in this string.
description	<string>	Specifies a comment describing this event.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this event. The default is enable.
	disable	Disables this event.

Restrictions

None.

Examples

To set the event community string to public:

```
rs(config)# rmon event index 10 community public
```

To add the description “num-pkts” to event 10:

```
rs(config)# rmon event index 10 description num-pkts
```

To specify Ed as the owner of event 10:

```
rs(config)# rmon event index 10 owner Ed
```

To send an SNMP trap when event 10 is triggered:

```
rs(config)# rmon event index 10 type trap
```

rmon filter

Mode

Configure

Format

```
rmon filter index <index-number> channel-index <number> [data-offset <number>] [data
<string>] [data-mask <string>] [data-not-mask <string>] [pkt-status <number>] [status-mask
<number>] [status-not-mask <number>] [owner <string>] [status enable|disable]
```

Description

The Filter group allows packets to be matched on certain criteria. The **rmon filter** command sets various parameters of the RMON 1 Filter table. To configure the Filter group, the Filter Channel group must first be configured with the **rmon channel** command.

Use the **rmon show filters** command to display the filters defined on the RS.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Filter table.
channel-index	<number>	Is a number between 1 and 65535 that identifies the channel of which this filter is a part.
data-offset	<number>	Is a number between 0 and 2147483647 that is the offset from the beginning of each packet where a match of packet data will be attempted.
data	<string>	Is a string of up to 512 characters that is the data that is to be matched with the input packet.
data-mask	<string>	Is a string of up to 512 characters that is the mask that is applied to the match process.
data-not-mask	<string>	Is a string of up to 512 characters that is the inversion mask that is applied to the match process.
pkt-status	<number>	Is a number between 0 and 2147483647 that is the status that is to be matched with the input packet.
status-mask	<number>	Is a number between 0 and 2147483647 that is the mask that is applied to the status match process.
status-not-mask	<number>	Is a number between 0 and 2147483647 that is the inversion mask that is applied to the status match process.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this channel. The default is enable.
	disable	Disables this channel.

Restrictions

None.

Example

To create an entry in the Filter table:

```
rs(config)# rmon filter index 25 channel-index 35 data kgreen
```

rmon history

Mode

Configure

Format

```
rmon history index <index-number> port <port> [interval <seconds>] [owner <string>] [samples <num>] [status enable|disable]
```

Description

The RMON History group periodically records samples of variables and stores them for later retrieval. You use the `rmon history` command to specify the RS port to collect data from, the number of samples, the sampling interval, and the owner. If default tables were turned on for the Lite group, an entry is created in the History control table for each available port.

Use the `rmon show history` command to display the history data.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies an entry in the History table.
port	<port>	Specifies the port from which to collect data.
interval	<seconds>	Specifies the sampling interval in seconds. This value must be between 1 and 3600, inclusive. The default value is 1800.
owner	<string>	Specifies the owner of the history resource; for example, an IP address, machine name or person's name.
samples	<num>	Specifies the number of samples to be collected before wrapping counters. This value must be between 1 and 65535, inclusive. The default value is 50.
status	enable	Enables this history control row.
	disable	Disables this history control row.

Restrictions

None.

Example

To specify that port et.3.1 collect 60 samples at an interval of 30 seconds:

```
rs(config)# rmon history index 10 port et.3.1 samples 60 interval 30
```

rmon hl-host

Mode

Configure

Format

```
rmon hl-host index <index-number> port <port> nl-max-entries <number> <number> [owner <string>] [status enable|disable]
```

Description

The **rmon hl-host** command sets various parameters of the RMON 2 Application Layer and Network Layer Host groups. The Application Layer Host group monitors traffic from the network layer up to the application layer for any protocol communication defined in the protocol directory. The Network Layer Host group monitors traffic at the network layer for any protocol defined in the protocol directory.

Configuration of the Application Layer/Network Layer Host table involves configuring only one control row in the Application Layer Host control table. This table, when configured, captures both application layer and network layer host data. If the default tables were turned on for the Professional group, an entry is created in the Application Layer Host control table for each available port.

Use the **rmon show al-host** command to display the Application Layer Host table. Use the **rmon show nl-host** command to display the Network Layer Host table.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the application layer host control table.
port	<port>	Specifies the port from which to collect data.
nl-max-entries	<number>	Specifies the maximum number of network layer entries. The default is 1.
al-max-entries	<string>	Specifies the maximum number of application layer entries. The default is 1.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables or disables this matrix. The default is enable.
	disable	Disables this matrix.

Restrictions

None.

Example

To create an entry in the Application Layer Host control table:

```
rs(config)# rmon hl-host index 20 port et.1.3
```

rmon hl-matrix

Mode

Configure

Format

```
rmon hl-matrix index <index-number> port <port> nl-max-entries <number> al-max-entries  
<number> [owner <string>] [status enable|disable]
```

Description

The **rmon hl-matrix** command sets various parameters of the RMON 2 Application Layer Matrix and Network Layer Matrix groups. The Application Layer Matrix group monitors traffic from the network layer up to the application layer for any protocol communication defined in the protocol directory. The Network Layer Matrix group monitors traffic at the network layer for any protocol defined in the protocol directory.

Configuration of the Application Layer/Network Layer Matrix table involves configuring only one control row in the Application Layer Matrix control table. When configured, this table captures both application layer and network layer matrix data. If the default tables were turned on for the Professional group, an entry is created in the Application Layer Matrix control table for each available port.

Use the **rmon show al-matrix** command to display the Application Layer Matrix table. Use the **rmon show nl-matrix** command to display the Network Layer Matrix table.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the application layer matrix control table.
port	<port>	Specifies the port from which to collect data.
nl-max-entries	<number>	Specifies the maximum number of network layer entries. The default is 1.
al-max-entries	<number>	Specifies the maximum number of application layer entries. The default is 1.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this matrix. The default is enable.
	disable	Disables this matrix.

Restrictions

None.

Example

To create an entry in the Application Layer Matrix control table:

```
rs(config)# rmon hl-matrix index 20 port et.1.3
```

rmon host

Mode

Configure

Format

```
rmon host index <index-number> port <port> [owner <string>] [status enable|disable]
```

Description

The RMON 1 Host group captures L2 information from hosts coming in on a particular port. The **rmon host** command sets various parameters of the Host group. If default tables were turned on for the standard group, an entry is created in the Host control table for each available port.

Use the **rmon show hosts** command to display the host data and logs.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Host table.
port	<port>	Specifies the physical port from which to collect data.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this host. The default is enable.
	disable	Disables this host.

Restrictions

None.

Example

To create an entry in the Host control table:

```
rs(config)# rmon hosts index 20 port et.1.3
```

rmon host-top-n

Mode

Configure

Format

```
rmon host-top-n index <index-number> host-index <number> [base <statistics>] [duration <time>] [size <size>] [owner <string>] [status enable|disable]
```

Description

The HostTopN group displays the top n number of hosts, sorted by a specified statistic. The **rmon host-top-n** command sets various parameters of the RMON 1 HostTopN control table. The HostTopN group depends upon the Host group and the host-index specified in the HostTopN control table must correspond to a pre-defined host index in the Host control table.

Use the **rmon show host-top-n** command to display the control table row.

Note that Host Top N report runs once. To run the reports again via the CLI, the control row must be disabled and then enabled. If the report has already been run, the Time Remaining field is set to zero. Otherwise, the Time Remaining field will be decremented until the report is run.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Host Top N table.
host-index	<number>	Is a number between 1 and 65535 that is the index into the host table identified by hostIndex.
base	<statistics>	Specifies the type of statistic from which to collect data.
	in-packets	Gather top statistics according to In-Packets.
	out-packets	Gather top statistics according to Out-Packets.
	in-octets	Gather top statistics according to In-Octets.
	out-octets	Gather top statistics according to Out-Octets.
	out-errors	Gather top statistics according to Out-Errors.
	out-broadcastPkts	Gather top statistics according to Out-BroadcastPkts.
	out-multicastPkts	Gather top statistics according to Out-MulticastPkts.
duration	<time>	Is a number between 1 and 2147483647 that is the duration, in seconds, between reports. The default is 0.
size	<size>	Is a number between 1 and 2147483647 that is the maximum number of hosts to include in the table. The default is 10.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.

Parameter	Value	Meaning
status	enable	Enables this hostTopN. .
	disable	Disables this hostTopN.

Restrictions

None.

Example

To create an entry in the HostTopN control table:

```
rs(config)# rmon host-top-n index 25 host-index 55 base in-packets  
duration 60 size 24
```

rmon matrix

Mode

Configure

Format

```
rmon matrix index <index-number> [port <port>] [owner <string>] [status enable|disable]
```

Description

The Matrix group captures L2 traffic on a particular port between two hosts (a source MAC and destination MAC address). The **rmon matrix** command sets various parameters of the RMON 1 Matrix control table. If default tables were turned on for the Standard group, an entry is created in the Matrix control table for each available port.



Note By default, ports on the RS operate in address-bridging mode. The port must be enabled in *flow-bridging* mode in order for layer 2 matrix information to be captured.

Use the **rmon show matrix** command to display the matrix group and logs.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Matrix table.
port	<port>	Specifies the port from which to collect data.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this matrix. The default is enable.
	disable	Disables this matrix.

Restrictions

None.

Example

To create an entry in the Matrix control table:

```
rs(config)# rmon matrix index 25 port et.1.3
```

rmon nl-matrix-top-n

Mode

Configure

Format

```
rmon nl-matrix-top-n index <index-number> matrix-index <number> ratebase  
terminal-packets|terminal-octets|all-packets|all-octets duration <number> size <number>  
[owner <string>] [status enable|disable]
```

Description

The **rmon nl-matrix-top-n** command gathers the top n Network Layer Matrix entries. Before you do this, you should first configure the Application Layer/Network Layer Matrix table using the **rmon hl-matrix** command.

Use the **rmon show nl-matrix-top-n** command to display the top n Network Layer Matrix entries.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the network layer matrix table.
matrix-index	<number>	Specifies the index into the hl-matrix table. The default is 0.
ratebase		Specifies the sorting method.
	terminal-packets	Sort by terminal packets.
	terminal-octets	Sort by terminal octets.
	all-packets	Sort by all packets.
	all-octets	Sort by all octets.
duration	<number>	Specifies the duration, in seconds, between reports. The default is 0.
size	<number>	Specifies the maximum number of matrix entries to include in the report. The default is 150.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this matrix. The default is enable.
	disable	Disables this matrix.

Restrictions

None.

Example

To gather the top n Network Layer Matrix entries:

```
rs(config)# rmon nl-matrix-top-n index 2 matrix-index 25 ratebase  
all-packets duration 60 size 100
```

rmon protocol-distribution

Mode

Configure

Format

```
rmon protocol-distribution index <index-number> port <port> [owner <string>] [status enable|disable]
```

Description

The Protocol Distribution group displays the packets and octets on a protocol and port basis. The **rmon protocol-distribution** command sets various parameters of the RMON 2 Protocol Distribution control table. If default tables were turned on for the Professional group, an entry is created in the Protocol Distribution control table for each available port.

Use the **rmon show protocol-distribution** command to display the protocol distribution.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Protocol Distribution table.
port	<port>	Specifies the port from which to collect data.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this matrix. The default is enable.
	disable	Disables this matrix. The default is enable.

Restrictions

None.

Example

To create an entry in the Protocol Distribution control table:

```
rs(config)# rmon protocol-distribution index 25 port et.1.3
```

rmon set

Mode

Configure

Format

```
rmon set lite|standard|professional default-tables yes|no
```

Description

You can enable various levels of support (Lite, Standard, or Professional) for RMON groups on a specified set of ports.

Lite adds support for the following RMON 1 groups:

- Ethernet statistics (Etherstats)
- History
- Alarm
- Event

Standard adds support for the following RMON 1 groups:

- Host
- HostTopN
- Matrix
- Filter
- Packet Capture

Professional adds support for the following RMON 2 groups:

- Protocol Directory
- Protocol Distribution
- Address Map
- Network Layer Host
- Network Layer Matrix
- Application Layer Host
- Application Layer Matrix
- User History
- Probe Configuration

A group can consist of a control table and a data table. A control table specifies the statistics to be collected. Each row in the control table specifies the entities for which data is collected, for example, physical ports. The data tables contain the statistics that are collected based on the control table information.

Parameter	Value	Meaning
set	lite	Specifies the Lite RMON group.
	standard	Specifies the Standard RMON group.
	professional	Specifies the Professional RMON group.
default-tables		Creates control tables for the following Lite, Standard, or Professional RMON groups: Lite groups:Etherstats History Standard groups:Host Matrix Professional groups:Protocol Distribution Address Map Application Layer/Network Layer Host Application Layer/Network Layer Matrix
	yes	A row in each control table is created for each port on the RS, with the default owner “monitor”.
	no	Removes all control table rows with the owner “monitor”. If you wish to save a particular control table row, you must change the owner to a value other than “monitor”.

Restrictions

None.

Example

To configure the RMON Lite groups and create default control tables:

```
rs(config)# rmon set lite default-tables yes
```

rmon set cli-filter

Mode

Configure

Format

```
rmon set cli-filter <filter-id> <parameter>
```

Description

You can define filters that CLI users can apply to certain RMON groups. The filters you define are visible to all users that have a Telnet or Console session on the RS. Each user has the choice of whether or not to apply a particular filter using the **rmon apply cli-filters** command.

RMON CLI filters only affect the output of the following RMON groups:

- Host
- Matrix
- Network Layer Host
- Application Layer Host
- Network Layer Matrix
- Application Layer Matrix
- Protocol Distribution

The **rmon show cli-filters** command displays the RMON CLI filters that have been defined on the RS.

Parameter	Value	Meaning
cli-filter	<filter-id>	Is a number between 1 and 65535 that uniquely identifies a CLI filter.
src-mac	<MAC-addr>	Sets the filter on a source MAC Address.
dst-mac	<MAC-addr>	Sets the filter on a destination MAC Address.
inpkts		Sets the filter on In Packets.
inoctets		Sets the filter on In Octets.
outpkts		Sets the filter on out packets.
outoctets		Sets the filter on out Octets.
multicast		Sets the filter on multicast packets.
broadcast		Sets the filter on broadcast packets.
errors		Sets the filter on errors.

The following operands can also be used:

andAND

orOr

=Equal to

<Less than

<=Less than or equal to

>Greater than

>=Greater than or equal to

!=Not equal to

(Left bracket

)Right Bracket



Note The **src-mac** and **dst-mac** can be specified once and the other parameters can be specified multiple times.

Restrictions

None.

Example

To configure an RMON CLI filter on a source MAC address of 123456:123456 and on input packets greater than 1000 and error packets greater than 10 or out packets less than 10000, use the following command:

```
rs(config)# rmon set cli-filter 3 src-mac 123456:123456 and ((inpkts > 1000 and errors > 10) or (outpkts < 10000))
```

rmon set memory

Mode

Enable

Format

```
rmon set memory <number>
```

Description

RMON allocates memory depending on the number of ports enabled for RMON, the groups that have been configured (Lite, Standard, or Professional) and whether or not default tables have been turned on or off. You can dynamically allocate additional memory to RMON, if needed.

Later, if this additional memory is no longer required, you can reduce the allocation; this change will not take effect until RMON is restarted. This is because memory cannot be freed while RMON is still using it.

Use the **rmon show status** command to display the amount of memory currently allocated to RMON.

Parameter	Value	Meaning
memory	<number>	Specifies the total amount of memory, in Mbytes, to be allocated to RMON. The value can be between 2 and 96.



Note The number specified is the total number of Mbytes of memory to be allocated; it is not an increment of memory.

Restrictions

The maximum amount of memory that you can allocate to RMON depends upon the RS model, as shown in the table below.

Table 60-1 Maximum memory allocations for RMON

RS platform	Maximum memory
RS 32000	96 MB
RS 8600	48 MB
RS 8000	24 MB
RS 3000, RS 2100, RS 2000, RS 1000	12 MB

Example

To show the amount of memory allocated to RMON:

```
rs# rmon show status
```

To increase the amount of memory allocated to RMON:

```
rs# rmon set memory 32
```


rmon set ports

Mode

Configure

Format

```
rmon set ports <port list>|allports
```

Description

Since RMON uses many system resources, RMON can be enabled on a set of ports. Ports can be dynamically added and removed from the port list. For example, if default tables are turned on for the Lite group and port et.2.1 is then added to the port list, an entry for port et.2.1 is automatically created in the Etherstats and History control tables.

Parameter	Value	Meaning
ports	<port list>	Specifies the port(s) on which RMON is enabled.
	allports	Specify allports to enable RMON for all ports on the RS.

Restrictions

None.

Example

To enable RMON on all ports on the RS:

```
rs(config)# rmon set ports allports
```

rmon set protocol-directory

Mode

Configure

Format

```
rmon set protocol-directory <protocol> |all-protocols [address-map on|off|na] [host on|off|na] [matrix on|off|na]
```

Description

The **rmon set protocol-directory** command defines the protocols that are managed with RMON on the RS.

Parameter	Value	Meaning
protocol-directory	<protocol>	Specifies the protocol encapsulations that are managed with the Protocol Directory group on the RS. (See Appendix A, "RMON 2 Protocol Directory." for a list of protocols supported on the RS.)
	all-protocols	Specify all-protocols to manage all protocols that are supported on the RS.
address-map	on	Configures support for the Address Map group for the specified protocol(s).
	off	
	na	
host	on	Configures support for the Host group for the specified protocol(s).
	off	
	na	
matrix	on	Configures support for the Matrix group for the specified protocol(s).
	off	
	na	

Restrictions

The Protocol Directory group is part of the RMON Professional group. To use the **rmon set protocol-directory** command you must enable the RMON Professional group with the **rmon set professional** command.

Example

To configure a protocol encapsulation for the Protocol Directory group:

```
rs(config)# rmon set protocol-directory all-protocols address-map on  
host on matrix on
```

rmon show address-map

Mode

Enable

Format

```
rmon show address-map-logs <port-list>|all-ports
```

Description

The **rmon show address-map-logs** command displays entries in the RMON 2 Address Map table. Entries in this table are created automatically when default tables are turned on for the Professional group. You can show address bindings for specific ports or for all ports.

Parameter	Value	Meaning
address-map-logs	<port-list>	The port(s) for which you want to display MAC-network address information.
	all-ports	Use the keyword all-ports to show information for all ports.

Restrictions

This command is only available if you have configured the Professional group and Address Map control table entries exist for the specified port.

Example

To display the address map log table for all ports:

```
rs# rmon show address-map-logs all-ports
RMON II Address Map Control Table
```

① Port	② macAdd	③ nlAdd	④ Protocol
----	-----	-----	-----
et.5.1	00001D:CBA3FD	192.100.81.1	ether2.ip-v4
et.5.1	00001D:CBA3FD	192.100.81.1	*ether2.ip-v4
et.5.1	00001D:CBA3FD	10.60.89.88	ether2.ip-v4
et.5.1	00001D:CBA3FD	10.60.89.88	*ether2.ip-v4
et.5.5	00001D:CBA3FD	192.100.81.3	ether2.ip-v4
et.5.5	00001D:CBA3FD	192.100.81.3	*ether2.ip-v4
et.5.5	080020:835CAA	10.60.89.88	ether2.ip-v4
et.5.5	080020:835CAA	10.60.89.88	*ether2.ip-v4
et.5.1	0080C8:C172A6	192.100.81.3	ether2.ip-v4
et.5.1	0080C8:C172A6	192.100.81.3	*ether2.ip-v4

Legend:

1. The port on which the MAC address-network address binding was discovered.
2. The MAC address for the binding.
3. The network layer address for the binding.
4. The protocol, as specified in the RMON Protocol Directory for the RS.

rmon show al-host

Mode

Enable

Format

```
rmon show al-host <port-list>|all-ports [summary]
```

Description

The **rmon show al-host** command shows entries in the RMON 2 Application Layer Host table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when the Application Layer Host table is displayed. This command shows control rows and their corresponding logs only if there are logs. A control row with no data will not appear in the report.

The Application Layer host group is configured with the **rmon hl-host** command.

Parameter	Value	Meaning
al-host	<port-list>	The port(s) for which you want to display application layer traffic information.
	all-ports	Use the keyword all-ports to show traffic information for all the ports.
summary		Use the keyword summary to display control row summary information only.

Restrictions

This command is only available if you have configured the Professional group and control table entries exist for the specified port.

Example

To show Application Layer Host tables on all ports:

```
rs# rmon show al-host all-ports
RMON II Application Layer Host Table

Index: 500, Port: et.5.1, Inserts: 9, Deletes: 0, Owner:  monitor1
```

2	3	4	5	6	7
Address	InPkts	InOctets	OutPkts	OutOctets	Protocol
-----	-----	-----	-----	-----	-----
10.60.89.88	1080	879418	2	164	*ether2.ip-v4
10.60.89.88	1080	879418	2	164	
*ether2.ip-v4.tcp					
10.60.89.88	1080	879418	2	164	
*ether2.ip-v4.tcp.telnet					
192.100.81.1	1	100	1	100	*ether2.ip-v4
192.100.81.1	1	100	1	100	
*ether2.ip-v4.icmp					
192.100.81.3	3	264	1081	879518	*ether2.ip-v4
192.100.81.3	1	100	1	100	
*ether2.ip-v4.icmp					
192.100.81.3	2	164	1080	879418	
*ether2.ip-v4.tcp					
192.100.81.3	2	164	1080	879418	
*ether2.ip-v4.tcp.telnet					

```
Index: 504, Port: et.5.5, Inserts: 6, Deletes: 0, Owner:  monitor
```

Address	InPkts	InOctets	OutPkts	OutOctets	Protocol
-----	-----	-----	-----	-----	-----
10.60.89.88	3	246	1141	92563	*ether2.ip-v4
10.60.89.88	3	246	1141	92563	
*ether2.ip-v4.tcp					
10.60.89.88	3	246	1141	92563	
*ether2.ip-v4.tcp.telnet					
192.100.81.3	1141	92563	3	246	*ether2.ip-v4
192.100.81.3	1141	92563	3	246	
*ether2.ip-v4.tcp					
192.100.81.3	1141	92563	3	246	
*ether2.ip-v4.tcp.telnet					

Legend:

1. The control table entry for this port:

Index: uniquely identifies the entry in the control table.

Port: port name.

Inserts: number of Application Layer Host table entries for this port.

Deletes: number of Application Layer Host table entries deleted for this port.

Owner: default owner "monitor."

2. Network address discovered on the port.
3. Number of packets transmitted without errors to the network address for the protocol.
4. Number of octets transmitted without errors to the network address for the protocol.
5. Number of packets transmitted without errors from the network address for the protocol.

6. Number of octets transmitted without errors from the network address for the protocol.
7. The protocol, as specified in the RMON Protocol Directory for the RS. Note that this shows the destination socket, as well as application/protocol information.

rmon show al-matrix

Mode

Enable

Format

```
rmon show al-matrix <port-list>|all-ports [order-by srcdst|dstsrc] [summary]
```

Description

The **rmon show al-matrix** command shows entries in the RMON 2 Application Layer Matrix table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when this table is displayed. The control rows and their corresponding logs are displayed only if there are logs. A control row with no data will not appear in the report.

Parameter	Value	Meaning
al-matrix	<port-list>	The port(s) for which you want to display application layer traffic information.
	all-ports	Use the keyword all-ports to show traffic information for all the ports.
order-by	srcdst	Orders the logs by source address , then destination address (default).
	dstsrc	Orders the logs by destination address, then source address.
summary		Displays control row summary information only.

Restrictions

This command is only available if you have configured the Professional group and control table entries exist for the specified port.

Example

To show the Application Layer Matrix table for all ports:.

```
rs# rmon show al-matrix all-ports
RMON II Application Layer Host Table

Index: 500, Port: et.5.1, Inserts: 10, Deletes: 0, Owner:  monitor1

2
SrcAddr      3
DstAddr      4
Packets      5
Octets       6
Protocol

-----
10.60.89.88   192.100.81.3      2      164   *ether2.ip-v4
10.60.89.88   192.100.81.3      2      164   *ether2.ip-v4.tcp
10.60.89.88   192.100.81.3      2      164   *ether2.ip-v4.tcp.telnet
192.100.81.1  192.100.81.3      1      100   *ether2.ip-v4
192.100.81.1  192.100.81.3      1      100   *ether2.ip-v4.icmp
192.100.81.3  10.60.89.88      1181   972211 *ether2.ip-v4
192.100.81.3  10.60.89.88      1181   972211 *ether2.ip-v4.tcp
192.100.81.3  10.60.89.88      1181   972211 *ether2.ip-v4.tcp.telnet
192.100.81.3  192.100.81.1      1      100   *ether2.ip-v4
192.100.81.3  192.100.81.1      1      100   *ether2.ip-v4.icmp

Index: 504, Port: et.5.5, Inserts: 6, Deletes: 0, Owner: monitor
SrcAddr      DstAddr      Packets      Octets      Protocol
-----
10.60.89.88   192.100.81.3   1242   100744   *ether2.ip-v4
10.60.89.88   192.100.81.3   1242   100744   *ether2.ip-v4.tcp
10.60.89.88   192.100.81.3   1242   100744   *ether2.ip-v4.tcp.telnet
192.100.81.3  10.60.89.88     3      246   *ether2.ip-v4
192.100.81.3  10.60.89.88     3      246   *ether2.ip-v4.tcp
192.100.81.3  10.60.89.88     3      246   *ether2.ip-v4.tcp.telnet
```

Legend:

1. The control table entry for this port:

Index: uniquely identifies the entry in the control table.

Port: port name.

Inserts: number of application layer host table entries for this port.

Deletes: number of application layer host table entries deleted for this port.

Owner: default owner "monitor."

2. Source address.
3. Destination address.
4. Number of link layer packets transmitted from the source to the destination without errors for the protocol.
5. Number of octets transmitted from the source to the destination without errors for the protocol.
6. The protocol, as specified in the RMON Protocol Directory for the RS.

rmon show al-matrix-top-n

Mode

Enable

Format

```
rmon show al-matrix-top-n
```

Description

The **rmon show al-matrix-top-n** command shows entries in the RMON 2 Application Layer Matrix Top N table.

Restrictions

This command is only available if you have enabled the Professional RMON group and entries exist in the Application Layer Matrix Top N table.

Example

Consider the following command to gather the top n Application Layer Matrix entries:

```
rs(config)# rmon al-matrix-top-n index 1 matrix-index 500 ratebase
all-packets duration 20 size 5
```

To show the top n entries in the Application Layer Matrix table, as specified by the previous command:

```
rs# rmon show al-matrix-top-n
RMON II Al Matrix Table
```

1	2	3	4	5	6	7	8	9
Index	M-Index	RateBase	TimeRem	Duration	Size	StartTime	Reports	Owner
1	500	All-Packets	14	20	5	00D 00H 50M 25S	1	Usama

10	11	12	13	14	15	16
SrcAddr	DstAddr	PktRate	R-PktRate	OctetRate	R-OctetRate	Protocol
-----	-----	-----	-----	-----	-----	-----
192.100.81.3	10.60.89.88	21	0	19836	0	
*ether2.ip-v4.tcp.telnet						
192.100.81.3	10.60.89.88	21	0	19836	0	
*ether2.ip-v4.tcp						
192.100.81.3	10.60.89.88	21	0	19836	0	
*ether2.ip-v4						
192.100.81.1	192.100.81.3	0	0	0	0	*ether2.ip-v4
192.100.81.3	192.100.81.1	0	0	0	0	*ether2.ip-v4

Legend:

1. Index number that identifies this entry in the Application Layer Matrix Top N control table.
2. The Application Layer Matrix table for which the top N report is shown.

3. The parameter on which the entries are sorted.
4. Number of seconds left in the report currently being collected.
5. Number of seconds that this report has collected during the last sampling interval.
6. Maximum number of matrix entries in this report.
7. The time when this report was last started.
8. The number of reports generated by this entry.
9. The entity that configured this entry.
10. Network address of the source host.
11. Network address of the destination host.
12. Number of packets from the source to the destination during the sampling interval.
13. Number of packets from the destination to the source during the sampling interval.
14. Number of octets from the source to the destination during the sampling interval.
15. Number of octets from the destination to the source during the sampling interval.
16. The protocol, as defined in the RMON Protocol Directory group on the RS.

rmon show alarm

Mode

Enable

Format

```
rmon show alarm
```

Description

The **rmon show alarm** command displays the RMON Alarm table.

Restrictions

This command is only available if you have configured the Lite group.

Example

To show configured RMON alarms:

```
rs# rmon show alarm
```

rmon show channels

Mode

Enable

Format

```
rmon show channels
```

Description

The **rmon show channels** command displays the contents of the Filter Channel table.

Restrictions

This command is only available if you have configured the Standard group.

Example

To show the contents of the Filter Channel table:

```
rs# rmon show channels
RMON 1 Channel Table
      No channels defined
```

rmon show cli-filters

Mode

User and
Enable

Format

```
rmon show cli-filters
```

Description

The **rmon show cli-filters** command displays the RMON CLI filters that have been defined for use on the RS. Use the **rmon apply cli-filters** command to apply a filter to your current Telnet or Console session.

Restrictions

None.

Example

To show RMON CLI filters that are defined on the RS:

```
rs> rmon show cli-filters
RMON CLI Filters

  ❶    ❷
Id    Filter
--    -
  1    (inpkts >= 0)
  2    (inpkts >= 0 and outoctets >= 0)
  3    srcmac 222222222222 and (outoctets >= 0)
You have selected a filter: (inpkts >= 0) ❸
```

Legend:

1. The filter ID. You use this value to apply a filter with the **rmon apply cli-filters** command.
2. The filter parameters that were specified with the **rmon set cli-filter** command.
3. This shows the parameters of the filter that is currently applied to your Telnet or Console session.

rmon show etherstats

Mode
Enable

Format

rmon show etherstats <port-list>|all-ports

Description

The **rmon show etherstats** command displays entries in the Ethernet table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Lite group.

Parameter	Value	Meaning
etherstats	<port-list>	The port(s) for which you want Ethernet statistics displayed.
	all-ports	Use the keyword all-ports to show Ethernet statistics on all ports.

Restrictions

This command is only available if you have configured the Lite group.

Example

To display Ethernet statistics on a specified port:

```
rs# rmon show etherstats et.5.1
RMON I Ethernet Statistics Table
Index: 502, Port: et.5.1, Owner: monitor 1
-----
RMON EtherStats          Total
-----
Octets                    2          83616016
Unicast Frames            3          86185
Broadcast Frames          4           0
Multicast Frames          5           0
Collisions                6           0
64 Byte Frames            7          292
65-127 Byte Frames       16625
128-255 Byte Frames       6145
256-511 Byte Frames       4520
512-1023 Byte Frames      7992
1024-1518 Byte Frames    50611
```

Legend:

- 1. The EtherStats control table entry for this port:

Index: uniquely identifies this entry.

Port: port et.5.1.

Owner: default owner “monitor.”

2. Number of octets of data received on the network.
3. Number of good frames received that were directed to a Unicast address.
4. Number of good frames received that were directed to a broadcast address.
5. Number of good frames received that were directed to a multicast address.
6. Number of collisions on this Ethernet segment.
7. Number of good and bad frames received, for various frame size ranges.

rmon show events

Mode
Enable

Format

rmon show events

Description

The **rmon show events** command displays configured events and the logs, if any, of triggered events.

Restrictions

This command is only available if you have configured the Lite group.

Example

To show RMON events and logs:

```
rs# rmon show events
RMON I Event table

  1      2      3              4              5
Index Type Community      Description      Owner
   1 log   public      Log Only      Usama
No event logs found
Index Type Community      Description      Owner
   2 both private  Log & Trap      Usama
No event logs found
```

Legend:

- 1. Index number that identifies this entry in the Event table.
- 2. Type of event: log, trap, or both log and trap.
- 3. Community string used for this event.
- 4. User-defined description of this event.
- 5. Owner of this event entry.

rmon show filters

Mode

Enable

Format

```
rmon show filters
```

Description

The **rmon show filters** command show the contents of the Filter table.

Restrictions

This command is only available if you have configured the Standard group.

Example

To show the contents of the Filter table:

```
rs# rmon show filters
RMON 1 Filter Table
    No filters defined
```

rmon show history

Mode
Enable

Format

rmon show history <port-list>|all-ports

Description

The **rmon show history** command displays statistical samples that are stored in the RMON History group. Entries in this table are created automatically when default tables are turned on for the Lite group.

Parameter	Value	Meaning
history	<port-list>	The port(s) for which the history is to be displayed.
	all-ports	Use the keyword all-ports to show history information on all the ports.

Restrictions

This command is only available if you have configured the Lite group.

Example

To display history information for a specific port:

rs# rmon show history et.5.1

RMON I History Table

1	2	3	4	5								
Index	Port	Interval(secs)	Buckets	Owner								
502	et.5.1	300	50/50	monitor								
6	7	8	9	10	11	12	13					
Index	SysUpTime	Octets	Packets	Bcst	Mcst	Colls	%Util	Other				
213	00D 17H 45M 47S	318114	336	0	0	0	0	0				
214	00D 17H 50M 47S	323928	341	0	0	0	0	0				
215	00D 17H 55M 48S	323586	335	0	0	0	0	0				
216	00D 18H 00M 49S	317186	320	0	0	0	0	0				
217	00D 18H 05M 49S	323470	333	0	0	0	0	0				
			.									
			.									
			.									
258	00D 21H 31M 03S	322264	312	0	0	0	0	0				
259	00D 21H 36M 03S	327944	315	0	0	0	0	0				
260	00D 21H 41M 04S	333138	309	0	0	0	0	0				
261	00D 21H 46M 06S	327782	312	0	0	0	0	0				
262	00D 21H 51M 07S	332268	294	0	0	0	0	0				

Legend:

- 1.** Index number that identifies the entry for this port in the History control table.
- 2.** Port name.
- 3.** Interval (in seconds) for data samples for each data bucket.
- 4.** The actual number of buckets/the requested number of buckets.
- 5.** Owner of this entry “monitor” (default).
- 6.** Index number for this data bucket.
- 7.** Time at which the sample was measured.
- 8.** Total number of octets received on the network.
- 9.** Number of packets received during the sampling period.
- 10.** Number of good packets received during the sampling interval that were directed to a broadcast address.
- 11.** Number of good packets received during the sampling interval that were directed to a multicast.
- 12.** The number of collisions on this Ethernet segment during the sampling interval (best estimate).
- 13.** The percentage of the network being utilized (best estimate).

rmon show host-top-n

Mode
Enable

Format

rmon show host-top-n

Description

The **rmon show host-top-n** command displays a report of the top hosts for a specified statistic. Note that the Host Top N report runs once. To run the reports again via the CLI, the control row must be disabled and then enabled. If the report has already been run, the Time Remaining field is set to zero. Otherwise, the Time Remaining field will be decremented until the report is run.

Restrictions

This command is only available if you have configured the Standard group and Host Top N control table entries exist.

Example

Consider the following command to gather the top n Host entries:

```
rs(config)# rmon host-top-n index 1 host-index 500 base out-octets duration 20
size 5
```

To display the Host Top N report, as specified by the previous command:

```
rs# rmon show host-top-n
RMON I HostTopN Table

  1      2      3      4      5      6      7
  8
Index HostIndex RateBase      TimeRem Duration Buckets StartTime
Owner
1      500      Out-Octets    0          20      5/5      00D 00H 39M 29S
Usama

  9
Address      10
Rate
-----
0080C8:C172A6 19911
00001D:CBA3FD 0
```

Legend:

- 1. Index number that identifies this entry in the HostTop N control table.
- 2. Index number that identifies the Host control table entry.

3. The parameter used to order the list of top “n” entries.
4. Number of seconds left in the report currently being collected.
5. Number of seconds that this report has collected during the last (or current) sampling interval.
6. Maximum number of hosts requested for the Top N table/maximum number of hosts in the Top N table.
7. The time of the sampling.
8. The owner of this entry.
9. The host address.
10. The value of the statistic for the host address.

rmon show hosts

Mode

Enable

Format

```
rmon show hosts <port-list>|all-ports [summary]
```

Description

The **rmon show hosts** command displays entries in the Hosts table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Standard group.

If CLI filters have been applied, they will take effect when the Host table is displayed. This command will display control rows and their corresponding logs only if there are logs. A control row that has no data is not displayed.

Parameter	Value	Meaning
hosts	<port-list>	The port(s) for which host information is to be shown.
	all-ports	Use the keyword all-ports to show host information on all the ports.
summary		Use the keyword summary to show a summary of all control table rows with the number of logs in each row.

Restrictions

This command is only available if you have configured the Standard group and control table entries exist for the specified port.

Example

To show host information for a specific port:

```
rs# rmon show hosts et.5.1
RMON I Host Table
Index: 502, Port: et.5.1, Owner: monitor ①
```

②	③	④	⑤	⑥	⑦	
⑧						
Address	InPkts	InOctets	OutPkts	OutOctets	Bcst	Mcst
-----	-----	-----	-----	-----	-----	-----
00001D:CBA3FD	88917	88436760	62132	5 095029	0	0
0080C8:C172A6	62132	5095029	88920	88437062	0	0

Legend:

1. Host control table information for this port:

Index: number that identifies the entry for this port in the table.

Port: port name.

Owner: the default owner "monitor."

1. MAC address of the discovered host.
2. Number of good packets transmitted to this address.
3. Number of good octets transmitted to this address.
4. Number of good packets transmitted from this address.
5. Number of good octets transmitted from this address.
6. Number of good packets transmitted by this address that were directed to a broadcast address.
7. Number of good packets transmitted by this address that were directed to a multicast address.

To show a summary of host information:

```
rs# rmon show all-ports summary
RMON I Host Table Summary
```

1	2	3	4	5	6
Index	Data Rows	Port	Status	Mode	Owner
500	1	et.5.1	Up	Address	monitor
501	1	et.5.2	Up	Address	monitor
502	0	et.5.3	Down	Flow	monitor
503	17	et.5.4	Up	Flow	monitor
504	0	et.5.5	Down	Flow	monitor
505	0	et.5.6	Down	Flow	monitor
506	0	et.5.7	Down	Flow	monitor
507	0	et.5.8	Down	Flow	monitor

Legend:

1. Index number that identifies this entry in the Host control table.
2. Number of data rows associated with this index number.
3. Port.
4. Current state of the port.
5. Source of the data for this entry.
6. Owner of this entry.

rmon show matrix

Mode
Enable

Format

```
rmon show matrix <port-list> [all-ports [summary] [order-by srcdst|dstsrc]
```

Description

The **rmon show matrix** command displays entries in the Matrix table. Entries in this table are automatically created when default tables are turned on for the Standard group.

If CLI filters have been applied, they will take effect when the Matrix table is displayed. This command will display control rows and their corresponding logs only if there are logs. A control row that has no data is not displayed.

Parameter	Value	Meaning
matrix	<port-list>	The port(s) for which you want to display information.
	all-ports	Use the keyword all-ports to show matrix information on all the ports.
summary		Use the keyword summary to display the control rows only.
order-by		Use the keyword order-by to display entries by source/destination or by destination/source.
	srcdst	Use the keyword srcdst to display the entries by source/destination.
	dstsrc	Use the keyword dstsrc to display entries by destination/source.

Restrictions

This command is only available if you have configured the Standard group.

Example

To show statistics for source-destination address pairs:

```
rs# rmon show matrix all-ports
RMON I Matrix Table

Port: et.5.1, Index: 500, Owner: monitor ❶
```

❷ SrcAddr -----	❸ DstAddr -----	❹ Packets -----	❺ Octets -----
00001D:CBA3FD	0080C8:C172A6	3	264
0080C8:C172A6	00001D:CBA3FD	4	346

```
Port: et.5.5, Index: 504, Owner: monitor
SrcAddr          DstAddr          Packets          Octets
-----          -
```

SrcAddr -----	DstAddr -----	Packets -----	Octets -----
00001D:CBA3FD	080020:835CAA	3	246
080020:835CAA	00001D:CBA3FD	2	164

Legend:

1. The Matrix control table entry for this port:
 Port: the name of the port.
 Index: the index number for this port in the Matrix table.
 Owner: default "monitor."
2. Source MAC address.
3. Destination MAC address.
4. Number of packets transmitted from the source to the destination address, including bad packets.
5. Number of octets transmitted from the source to the destination address.

To show control row summary statistics:

```
rs# rmon show matrix all-ports summary
RMON I Matrix Table Summary
  Index  Data Rows  Port    Status  Mode    Owner
-----
500      0        et.1.1  Up      Address monitor
501      0        et.1.2  Down    Address monitor
502      0        et.1.3  Down    Address monitor
503      0        et.1.4  Up      Address monitor
504      0        et.1.5  Down    Address monitor
505      0        et.1.6  Down    Address monitor
506      0        et.1.7  Down    Address monitor
507      0        et.1.8  Up      Address monitor
508      0        gi.4.1  Up      Address monitor
509      0        gi.4.2  Up      Address monitor
510      0        et.7.1  Up      Address monitor
511      0        et.7.2  Down    Address monitor
512      0        et.7.3  Down    Address monitor
513      0        et.7.4  Down    Address monitor
514      0        et.7.5  Down    Address monitor
515      0        et.7.6  Down    Address monitor
516      0        et.7.7  Down    Address monitor
517      0        et.7.8  Down    Address monitor
25       0        et.1.3  Down    Address
```

rmon show nl-host

Mode

Enable

Format

```
rmon show nl-host <port-list>|all-ports [summary]
```

Description

The **rmon show nl-host** command shows entries in the RMON 2 Network Layer Host table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when the Network Layer host table is displayed. This command shows control rows and their corresponding logs only if there are logs. A control row with no data will not appear in the report.

Parameter	Value	Meaning
nl-host	<port-list>	The port(s) for which you want to display traffic information.
	all-ports	Use the keyword all-ports to show information on all the ports.
	summary	Use the keyword summary to display control row summary information only.

Restrictions

This command is only available if you have configured the Professional RMON group and control table entries exist for the specified port.

Example

To display the network layer host table for all ports:

```
rs# rmon show nl-host all-ports
```

RMON II Network Layer Host Table					
Index: 500, Port: et.5.1, Inserts: 3, Deletes: 0, Owner: monitor ¹					
² Address	³ InPkts	⁴ InOctets	⁵ OutPkts	⁶ OutOctets	⁷ Protocol
-----	-----	-----	-----	-----	-----
10.60.89.88	1159	952300	2	164	*ether2.ip-v4
192.100.81.1	1	100	1	100	*ether2.ip-v4
192.100.81.3	3	264	1160	952400	*ether2.ip-v4
Index: 504, Port: et.5.5, Inserts: 2, Deletes: 0, Owner: monitor					
Address	InPkts	InOctets	OutPkts	OutOctets	Protocol
-----	-----	-----	-----	-----	-----
10.60.89.88	3	246	1220	98962	*ether2.ip-v4
192.100.81.3	1220	98962	3	246	*ether2.ip-v4

Legend:

1. The control table entry for this port:

Index: index number that identifies this entry in the hl host control table.

Port: name of port.

Inserts: number of inserts in the network layer host table for this entry.

Deletes: number of deletions in the network layer host table for this entry.

Owner: the entity that configured this entry.

2. The network address.
3. Number of packets received by this network address.
4. Number of octets received by this network address.
5. Number of packets sent by this network address.
6. Number of octets sent by this network address.
7. The protocol, as defined in the RMON Protocol Directory for the RS. Note that this shows the network layer protocol encapsulations only. If you want to see application/protocol information, such as the destination socket, use the **rmon show al-host** command.

rmon show nl-matrix

Mode

Enable

Format

```
rmon show nl-matrix <port-list> [all-ports [order-by srcdst|dstsrc] [summary]
```

Description

The **rmon show nl-matrix** command shows entries in the Network Layer Matrix table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when this table is displayed. The control rows and their corresponding logs are displayed only if there are logs. A control row with no data will not appear in the report.

Parameter	Value	Meaning
nl-matrix	<port-list>	The port(s) for which you want to display network layer traffic information.
	all-ports	Use the keyword all-ports to show information for all ports.
order-by	srcdst	Orders the logs by source address, then destination address (default).
	dstsrc	Orders the logs by destination address, then source address.
summary		Use the keyword summary to display control row summary information only.

Restrictions

This command is only available if you have configured the Professional group and control table entries exist for the specified port.

Example

To show the Network Layer Matrix table for all ports:

```
rs# rmon show nl-matrix all-ports
RMON II Network Layer Matrix Table

Index: 500, Port: et.5.1, Inserts: 4, Deletes: 0, Owner:  monitor1
```

² SrcAddr	³ DstAddr	⁴ Packets	⁵ Octets	⁶ Protocol
-----	-----	-----	-----	-----
10.60.89.88	192.100.81.3	2	164	*ether2.ip-v4
192.100.81.1	192.100.81.3	1	100	*ether2.ip-v4
192.100.81.3	10.60.89.88	1241	1025436	*ether2.ip-v4
192.100.81.3	192.100.81.1	1	100	*ether2.ip-v4

```
Index: 504, Port: et.5.5, Inserts: 2, Deletes: 0, Owner:  monitor
SrcAddr      DstAddr      Packets      Octets      Protocol
-----
10.60.89.88   192.100.81.3   1302        105604      *ether2.ip-v4
192.100.81.3  10.60.89.88    3           246         *ether2.ip-v4
```

Legend:

1. The control table entry for this port:

Index: index number that identifies this entry in the control table.

Port: name of port.

Inserts: number of inserts in the Network Layer Matrix table for this entry.

Deletes: number of deletions in the Network Layer Matrix table for this entry.

Owner: the entity that configured this entry.

2. Source network address.
3. Destination network address.
4. Number of packets transmitted without error from the source to the destination.
5. Number of octets transmitted without error from the source to the destination.
6. The protocol, as specified in the RMON Protocol Directory for the RS.

rmon show nl-matrix-top-n

Mode
Enable

Format

rmon show nl-matrix-top-n

Description

The rmon show nl-matrix-top-n command shows entries in the RMON 2 Network Layer Matrix Top N table.

Restrictions

This command is only available if you have configured the Professional group and entries exist in the Network Layer Matrix Top N table.

Example

Consider the following command to gather the top n Network Layer Matrix entries:

```
rs(config)# rmon nl-matrix-top-n index 1 matrix-index 500 ratebase
all-octets duration 20 size 5
```

To show the top n entries in the Network Layer Matrix table, as specified by the previous command:

rs# rmon show nl-matrix-top-n
RMON II Nl Matrix Table

1	2	3	4	5	6	7	8	9
Index	M-Index	RateBase	TimeRem	Duration	Size	StartTime		Reports
1	500	Octets	20	20	5	00D 00H 51M 37S		1
								Usama
10		11	12	13	14	15	16	
SrcAddr		DstAddr	PktRate	R-PktRate	OctetRate	R-OctetRate		
Protocol								
-----		-----	-----	-----	-----	-----		

192.100.81.3		10.60.89.88		23	0	19986		0
*ether2.ip-v4								
192.100.81.1		192.100.81.3		0	0	0		0
*ether2.ip-v4								
192.100.81.3		192.100.81.1		0	0	0		0
*ether2.ip-v4								
10.60.89.88		192.100.81.3		0	23	0		19986
*ether2.ip-v4								

Legend:

- 1. Index number that identifies this entry in the network layer MatrixTop N control table.
- 2. The Network Layer Matrix table for which the top N report is shown.

3. The parameter on which the entries are sorted.
4. Number of seconds left in the report currently being collected.
5. Number of seconds that this report has collected during the last sampling interval.
6. Maximum number of matrix entries in this report.
7. The time when this report was last started.
8. The number of reports generated by this entry.
9. The entity that configured this entry.
10. Network address of the source host.
11. Network address of the destination host.
12. Number of packets from the source to the destination during the sampling interval.
13. Number of packets from the destination to the source during the sampling interval.
14. Number of octets from the source to the destination during the sampling interval.
15. Number of octets from the destination to the source during the sampling interval.
16. The protocol, as defined in the RMON Protocol Directory for the RS.

rmon show packet-capture

Mode

Enable

Format

```
rmon show packet-capture
```

Description

The **rmon show packet-capture** command shows the buffer table for captured packets. Before you use this command, first configure the Filter Channel group using the **rmon channel index** command. Then use the **rmon capture** command to configure the Packet Capture group which allows packets to be captured after they have flowed through a channel.

Restrictions

This command is only available if you have enabled the Standard RMON groups.

rmon show probe-config

Mode

Enable

Format

probe-config [basic] [net-config] [trap-dest]

Description

The **rmon show probe-config** command shows entries in the RMON 2 Probe Configuration table.

Parameter	Value	Meaning
basic		Shows basic probe configuration information.
net-config		Shows network configuration table.
trap-dest		Shows trap destination table.

Restrictions

This command is only available if you have configured the Professional group.

rmon show protocol-directory

Mode

Enable

Format

```
rmon show protocol-directory <protocol>|all-protocols
```

Description

The **rmon show protocol-directory** command displays the protocol encapsulations that are defined in the RMON 2 Protocol Directory group for the RS.

Parameter	Value	Meaning
protocol-directory	<protocol>	The specific protocol encapsulation that is managed with the RMON 2 Protocol Directory group. (See Appendix A, "RMON 2 Protocol Directory." for protocol encapsulations that are supported on the RS.)
	all-protocols	Use the keyword all-protocols to display all protocol encapsulations that are managed with the Protocol Directory group.

Restrictions

This command is only available if you have configured the Professional group.

Example

Following is an example of the **rmon show protocol-directory all protocols** command. Note that the example shows a partial listing only.:

```
rs# rmon show protocol-directory all-protocols
RMON II Protocol Directory Table
```

```
Last Change: 00D 00H 00M 00S
```

Index	AddrMap	Host	Matrix	Status	Protocol

1	Off	Off	Off	Active	ether2
2	NA	Off	Off	Active	idp
3	NA	Off	Off	Active	ip-v4
4	NA	Off	Off	Active	chaosnet
5	NA	Off	Off	Active	arp
6	NA	Off	Off	Active	rarp
7	NA	Off	Off	Active	vip
8	NA	Off	Off	Active	vloop
9	NA	Off	Off	Active	vloop2
10	NA	Off	Off	Active	vecho
11	NA	Off	Off	Active	vecho2
12	NA	Off	Off	Active	ipx
13	NA	Off	Off	Active	netbios-3com
14	NA	Off	Off	Active	atalk
15	NA	Off	Off	Active	aarp

...

rmon show protocol-distribution

Mode

Enable

Format

rmon show protocol-distribution <port-list>|all-ports

Description

The **rmon show protocol-distribution** command displays the RMON 2 Protocol Distribution table. This table contains a list of protocols, defined in the RMON 2 Protocol Directory, that are discovered by the RS. Entries in this table are created automatically when default tables are turned on for the Professional group. If you delete an entry in the Protocol Directory, then entries in this table associated with the deleted protocol are also deleted.

If CLI filters have been applied, they will take effect when the Protocol Distribution table is displayed.

Parameter	Value	Meaning
protocol-distribution	<port-list>	The port(s) for which you want to show protocol distribution.
	all-ports	Use the keyword all-ports to show protocol distribution information on all the ports.

Restrictions

This command is only available if you have configured the Professional group.

Example

To show the RMON 2 Protocol Distribution table:

:

```
rs(config)# rmon show protocol-distribution all-ports
RMON II Protocol Distribution Table

Index: 508, Port: gi.4.1, Owner: monitor
Pkts Octets Protocol
----
3312 304550 ether2
3312 304550 ip-v4
2459 234564 icmp
 853  69986 tcp
 853  69986 telnet
```

rmon show status

Mode
Enable

Format

rmon show status

Description

The **rmon show status** command shows whether RMON is enabled, the RMON groups that are configured, the ports on which RMON is enabled, and the memory allocated and used by RMON.

Example

To show RMON status:

```
rs# rmon show status
RMON Status
-----
* RMON is ENABL1
* RMON initialization successful.

+-----+
| RMON  Group  Status          |
+-----+-----+-----+
| Group | Status | Default |
+-----+-----+-----+
| Lite  |      On |      Yes |
+-----+-----+-----+
| Std   |      On |      Yes |
+-----+-----+-----+
| Pro   |      On |      Yes |
+-----+-----+-----+

RMON is enabled on: et.5.1, et.5.2, et.5.3, et.5.4, et.5.5, et.5.6,
et.5.7, et.5.83

RMON Memory Utilization 4
-----
Total Bytes Available: 48530436

Total Bytes Allocated to RMON: 4000000
Total Bytes Used: 2637872
Total Bytes Free: 1362128
```

Legend:

- 1. When the RS is booted, RMON is off by default. RMON is enabled with the **rmon enable** command.

2. Shows which RMON group (Lite, Standard, or Professional) is configured and whether default control tables are turned on.
3. Shows the ports on which RMON is enabled.
4. Shows RMON memory utilization. You can adjust the amount of memory allocated to RMON with the **rmon set memory** command.

rmon show user-history

Mode

Enable

Format

```
rmon <string> show user-history [all-indexes]
```

Description

The **rmon show user-history** command shows the User History table.

Parameter	Value	Meaning
rmon	<string>	Specifies a particular rmon.
all-indexes		This optional parameter displays all indexes.

Restrictions

This command is only available if you have configured the Professional group.

rmon user-history-apply

Mode

Configure

Format

```
rmon user-history-apply <groupname> to <user-history-index>
```

Description

The **rmon user-history-apply** command applies all objects in the group created with the **rmon user-history-objects** command to the row in the User History control table. If the number of objects specified in the control row is greater than those in the group, the remaining OIDs are set to 0.0. If the number of objects specified in the control row is less than those in the group, the remaining are discarded.

Parameter	Value	Meaning
user-history-apply	<groupname>	Is the name of a group of objects that has been created with the rmon-user-history-objects command.
to	<user-history-index>	Specifies the row in the User History control table.

Restrictions

None.

rmon user-history-control

Mode

Configure

Format

```
rmon user-history-control index <index-number> objects <number> samples <number> interval  
<number> [owner <string>] [status enable|disable]
```

Description

The **rmon user-history-control** command monitors the group of objects that are defined with the **rmon user-history-objects** command. This command creates an entry in the User History control table.

Use the **rmon show user-history** command to display the User History table.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the user history control table.
objects	<number>	Specifies the number of MIB objects to be collected.
samples	<number>	Specifies the number of discrete time intervals over which data is to be saved.
interval	<number>	Specifies the interval, in seconds, between samples.
owner	<string>	Specifies the owner of the event; for example, an IP address, machine name or person's name.
status	enable	Enables this matrix. The default is enable.
	disable	Disables this matrix. The default is enable.

Restrictions

None.

rmon user-history-objects

Mode

Configure

Format

```
rmon user-history-objects <groupname> variable <oid> type absolute-value|delta-value  
[status enable|disable]
```

Description

The **rmon user-history-objects** command defines the group of objects that can be monitored with the **rmon user-history-control** command. This command creates a group with a single OID as a member of the group. To add several objects to the group, you need to issue multiple **user-history-objects** commands. Each object appears as a separate row in the User History control table.

Parameter	Value	Meaning
user-history-objects	<groupname>	Is the name of the group of objects.
variable	<oid>	Specifies the object identifier to be monitored.
type		Specifies the method of sampling for the selected variable.
	absolute	Monitor the absolute value of this variable against a threshold value.
	delta	Monitor the change in value over the interval of this variable against a threshold value.
status	enable	Enables this matrix. The default is enable.
	disable	Disables this matrix.

Restrictions

None.

61 ROUTE-MAP COMMANDS

The **route-map** commands allow you to create a route-map that defines the conditions for importing routes from a BGP peer, exporting routes to a BGP peer, redistributing routes from any routing protocol into BGP, or redistributing routes from BGP into any other routing protocol.

61.1 COMMAND SUMMARY

The following table lists the **route-map** commands. The sections following the table describe the command syntax.

<code>route-map <number-or-string> permit <sequence-number> <match-criteria> <action></code> <code>route-map <number-or-string> deny <sequence-number> <match-criteria></code>
<code>route-map <number-or-string> set dampenflap [state enable disable]</code> <code> [suppress-above <num>] [reuse-below <num>] [max-flap</code> <code><num>] [unreach-decay <num>] [reach-decay <num>] [keep-history <num>]</code>
<code>route-map show [identifier <number-or-string>] all</code>

route-map permit/deny

Mode

Configure

Format

```
route-map <number-or-string> permit <sequence-number> <match-criteria> <action>
route-map <number-or-string> deny <sequence-number> <match-criteria>
```

Description

The **route-map permit** command permits the routes that are matched by the route-map definition to be imported, exported, or redistributed. The **route-map deny** command prevents the routes that are matched by the route-map definition from being imported, exported, or redistributed.

Parameter	Value	Meaning
route-map	<number-or-string>	Specifies the identifier of a route-map. The routes which are not matched by all the route-maps will not be imported/exported. Hence there should be a route-map to allow the desired routes.
permit		Permits the routes matched by this route-map to be imported/exported and sets the values as specified by actions.
deny		Prevents the routes matched by this route-map to be imported/exported.
	<sequence-number>	Number that indicates the position a new route map is to have in the list of route maps already configured with the same identifier. Route-maps with the same identifier are executed in the order of increasing sequence numbers.
	<match-criteria>	can be the following:
match-route-map	<number-or-string>	Matches the route specified by a previously-defined route map.
match-prefix		Matches the prefix of a route as per the route filter or by the specified network.

Parameter	Value	Meaning
filter	<filter-id>	Specifies the route filter. This route filter should have already been created using the ip-router policy create filter command.
network	<ipAddr/mask>	Specifies networks that are to be filtered. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be filtered are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the exact, refines, or between parameters, the mask of the destination is also considered.
	all	Matches any network. This is equivalent to specifying network 0.0.0.0/0.0.0.0.
	default	Matches the default address with a mask of all zeroes. This is equivalent to specifying network 0.0.0.0/0.0.0.0 with the exact parameter.
exact		Specifies that the mask of the routes to be filtered must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.
refines		Specifies that the mask of the routes to be filtered must be more specific (i.e. longer) than the supplied mask. This is used to match subnets.

Parameter	Value	Meaning
between	<low-high>	Specifies that the mask of the destination must be as or more specific (i.e., as long as longer) than the lower limit (the first number parameter) and no more specific (i.e. as long as or shorter) than the upper limit (the second parameter).
match-route-type	<protocol>	Matches the source protocol of the route. Used for redistribution and not for importing routes. This option is typically used when the route-map-in or route-map-out option is used in the bgp set peer-group or bgp set peer-host command.
	direct	Specifies that the redistributed routes are direct routes
	static	Specifies that the redistributed routes are static routes
	aggregate	Specifies that the redistributed routes are aggregate routes
	rip	Specifies that the redistributed routes are RIP routes
	ospf	Specifies that the redistributed routes are OSPF routes
	ospf-ase	Specifies that the redistributed routes are OSPF ASE routes
	isis-level-1	Specifies that the redistributed routes are IS-IS level 1 routes
	isis-level-2	Specifies that the redistributed routes are IS-IS level 2 routes
	bgp	Specifies that the redistributed routes are BGP routes
	any	Specifies that routes from all sources are redistributed
match-next-hop-list	<route-filter identifier>	Matches the next hop for a route as per the route-filter. This route filter should have already been created using the ip-router policy create filter command.

Parameter	Value	Meaning
match-local-preference	<number>	Matches the value of the local preference attribute of BGP.
match-metric	<number>	Matches the value of the Multi Exit Discriminator (MED) attribute of BGP.
match-origin	any	Matches the origin as per the origin attribute of BGP.
	igp	
	egp	
	incomplete	
match-aspath-regular-expression	<identifier>	Specifies the identifier of the AS path regular expression list that must be satisfied for the route to be exported. The AS path regular expression list and its identifier must have previously been created with the ip-router policy create aspath-regular-expression command.
	<expression>	Specifies a regular expression. Enclose the expression in quotes.
match-community-list	<community-list-identifier>	Matches the communities present in the route as per the community list specified by <community-list-identifier>. This option will succeed if the communities are <i>part</i> of communities present in the route. The community list should have been already created using the ip-router policy create community-list command or be a well-known community represented by one of the keywords shown below:
	no-export	Matches the community as per the well-known community NO_EXPORT (65535:65281).
	no-advertise	Matches the community as per the well-known community NO_ADVERTISE (65535:65282).

Parameter	Value	Meaning
	no-export-subconfed	Matches the community as per the well-known community NO_EXPORT_SUBCONFED (65535:65283).
match-community-list-exact	<community-list-identifier>	Matches the communities present in the route as per the community list specified by <community-list-identifier>. This option will succeed only if the communities are <i>exactly</i> the same as that of the route. The community-list should have been already created using the ip-router policy create community-list command or be a well-known community represented by one of the keywords shown below
	no-export	Matches the community as per the well-known community NO_EXPORT (65535:65281).
	no-advertise	Matches the community as per the well-known community NO_ADVERTISE (65535:65282).
	no-export-subconfed	Matches the community as per the well-known community NO_EXPORT_SUBCONFED (65535:65283).
<action>		This is used only with the route-map permit command.
set-next-hop	<ip-address>	Sets the next hop for the route.
	self	The keyword self sets the next hop for the route to the local router's address.
set-local-preference	<number>	Sets the local preference for a route.

Parameter	Value	Meaning
set-metric	<metric>	Sets the Multi Exit Discriminator (MED) for a route. This number must be enclosed in <i>quotes</i> . Specify a number, in quotes, between 0 and 65535 to set the metric to that value. If the number is preceded by a plus sign (+), the number is <i>added</i> to the metric for the route. If the number is preceded by a minus sign (-), the number is <i>subtracted</i> from the metric for the route.
set-origin		Sets the origin for a route.
	igp	
	egp	
	incomplete	
set-as-path-prepend	<AS numbers>	Prepends the AS numbers to the existing AS path for a route. By varying the length of the AS-PATH, a BGP speaker can influence the best path selection by a peer further away. Improper selection of this parameter could cause routing loops. AS numbers should be a quoted string with AS numbers in decimal form.
set-community-list		Sets the community for the route.
	<community-list-identifier>	This can be a list of communities within quotes, like "a:b c:d" where a and c are the AS portion of a community split and b and d are the community identifier portion of a community split. Or, you can specify a community list identifier that you previously created with the ip-router policy create community-list command.
	<keyword>	You can specify the following keywords.
	no-export	Sets the community to the well-known community NO_EXPORT (65535:65281)

Parameter	Value	Meaning
	no-advertise	Sets the community to the well-known community NO_ADVERTISE (65535:65282)
	no-export-subconfed	Sets the community to the well-known community NO_EXPORT_SUBCONFED (65535:65283)
	none	Removes the community attribute from a route.
additive		Adds the communities specified with the set-community-list parameter to the existing community list for a route.
delete-community-list		Deletes the specified communities from the route.
	<community-string>	This can be a list of communities within quotes, like "a:b:c:d" where a and c are the AS portion of a community split and b and d are the community identifier portion of a community split. Or, you can specify a community list identifier that you previously created with the ip-router policy create community-list command.
	<keyword>	You can specify the following keywords
	no-export	Deletes the well-known community NO_EXPORT (65535:65281)
	no-advertise	Deletes the well-known community NO_ADVERTISE (65535:65282)
	no-export-subconfed	Deletes the well-known community NO_EXPORT_SUBCONFED (65535:65283)
	all	Deletes all communities

Parameter	Value	Meaning
set-preference	<number>	Specifies the preference with which the imported routes that match the specified route-map should be installed.
set-traffic-index	<index>	Specifies the traffic bucket number. When BGP accounting is enabled, the number of packets/bytes for each traffic bucket is collected.

Restrictions

None.

route-map set dampenflap

Mode

Configure

Format

```
route-map <number-or-string> set dampenflap [state enable|disable][suppress-above  
<num>][reuse-below <num>][max-flap <num>][unreach-decay <num>][reach-decay  
<num>][keep-history <num>]
```

Description

The **route-map set dampenflap** command configures the state of Weighted Route Dampening.

Parameter	Value	Meaning
state		Causes the Route Instability History to be maintained (enable option) or not (disable option).
	enable	Causes the Route Instability History to be maintained.
	disable	Causes the Route Instability History to not be maintained.
suppress-above	<num>	Is the value of the instability metric at which route suppression will take place. A route will not be installed in the FIB or announced even if it is reachable during the period that it is suppressed. The default is 3.0.
reuse-below	<num>	Is the value of the instability metric at which a suppressed route will become unsuppressed, if it is reachable but currently suppressed. The value must be less than that for the suppress-above option. The default is 2.0.
max-flap	<num>	Is the upper limit of the instability metric. This value must be greater than the larger of 1 and that for suppress-above. The default is 16.0.
unreach-decay	<num>	Specifies the time in seconds for the instability metric value to reach one-half of its current value when the route is <i>unreachable</i> . This half-life value determines the rate at which the metric value is decayed. The default is 900.

Parameter	Value	Meaning
reach-decay	<num>	Specifies the time in seconds for the instability metric value to reach one half of its current value when the route is <i>reachable</i> . This half-life value determines the rate at which the metric value is decayed. A smaller half-life value will make a suppressed route reusable sooner than a larger value. The default is 300.
keep-history	<num>	Specifies the period in seconds over which the route flapping history is to maintained for a given route. The size of the configuration arrays is directly affected by this value. The default is 1800.

Restrictions

None

route-map show

Mode
Enable

Format

route-map show [identifier <number-or-string>] | all

Description

The **route-map show identifier** command displays either all the route-maps configured for a specified route-map identifier or all configured route-maps. Route-maps are shown in order of increasing sequence numbers. For route-maps created with the **route-map permit** command, the configured <match-criteria> and <action> clauses are shown. For route-maps created with the **route-map deny** command, the configured <match-criteria> is shown.

Parameter	Value	Meaning
identifier	<number-or-string>	Specifies the identifier of a route-map.
	all	This keyword specifies all configured route-maps.

Example

To display the route-map with the identifier ‘8’:

```
rs# route-map show identifier 8

route-map 8, permit, sequence 1
  Match clauses
    prefix 1.0.0.0/24 Exact
    route-type OSPF
    local preference 50
    metric(MED) 60
    origin EGP
    community list 1:2 3:4 5:6 7:8
  Set clauses
    nexthop 1.1.1.1
    local preference 100
    metric(MED) 110
    origin IGP
    set community COMMUNITY_NO_EXPORT_SUB

route-map 8, permit, sequence 2
  Match clauses
  Set clauses
```

In the example shown above, routes that match sequence 1 will have parameters set to the values specified in the set clauses. Routes that do not match sequence 1 will still be imported or exported, as specified with sequence 2.

62 RSVP COMMANDS

The **rsvp** commands allow you to configure Resource Reservation Protocol (RSVP) features on the RS, as well as display various RSVP parameters.

62.1 COMMAND SUMMARY

The following table lists the **rsvp** commands. The sections following the table describe each command in greater detail.

<code>rsvp add interface <name> <ip-address> all</code>
<code>rsvp set global path-refresh-interval <number> path-multiplier <number> resv-refresh-interval <number> resv-multiplier <number> hello-interval <number> hello-multiplier <number> bundle-interval <number> blockade-aging-interval <number> msgid-list-interval <number> msgack-interval <number></code>
<code>rsvp set interface <name> <ip-address> all hello-enable aggregate-enable msgid-extensions-enable auth-method md5 none auth-key <string></code>
<code>rsvp set trace-level <level></code>
<code>rsvp set trace-options <option></code>
<code>rsvp show all</code>
<code>rsvp show global</code>
<code>rsvp show interface <name> <ip-address> all [brief] [verbose] [statistics]</code>
<code>rsvp show neighbors <name> <ip-address> all</code>
<code>rsvp show psb <name> <ip-address> all</code>
<code>rsvp show rsb <name> <ip-address> all</code>
<code>rsvp show session <name> <ip-address> all</code>
<code>rsvp show tcbs <name> <ip-address> all</code>
<code>rsvp start</code>

rsvp add interface

Mode

Configure

Format

```
rsvp add interface <name> | <ip-address> | all
```

Description

The **rsvp add interface** command allows you to enable RSVP on an interface.

Parameter	Value	Meaning
interface	<name> <ip-address>	Specifies an interface. RSVP is enabled on this interface. Specify an interface name or an IP address.
	all	Specify all to enable RSVP on all interfaces.

Restrictions

None

Example

The following command enables RSVP on the interface 'group1':

```
rs(config)# rsvp add interface group1
```

rsvp set global

Mode

Configure

Format

```
rsvp set global path-refresh-interval <number> path-multiplier <number>
resv-refresh-interval <number> resv-multiplier <number> hello-interval <number>
hello-multiplier <number> bundle-interval <number> blockade-aging-interval <number>
msgid-list-interval <number> msgack-interval <number>
```

Description

The **rsvp set global** command allows you to set various global parameters that will be applied to all RSVP interfaces.

Parameter	Value	Meaning
path-refresh-interval	<number>	Sets the path refresh interval for all RSVP interfaces, in seconds. This refresh interval determines how often an RSVP interface will send out path messages to the downstream neighbor, preventing path states from timing out. Specify a decimal number between 1 and 65535. The default value is 30 seconds.
path-multiplier	<number>	Sets the path multiplier variable. The path multiplier variable is used to compute how long to keep a path state as a valid state. Specify a decimal number between 1 and 255. The default value is 3. For hops with a high loss rate, you may want to set this number higher.
resv-refresh-interval	<number>	Sets the reservation request interval for all RSVP interfaces, in seconds. This refresh interval determines how often an RSVP interface will send out reservation requests to the upstream neighbor, preventing a reservation state from timing out. Specify a decimal number between 1 and 65535. The default value is 30 seconds.
resv-multiplier	<number>	Sets the reservation multiplier variable. The reservation multiplier variable is used to compute how long to keep a reservation state as a valid state. Specify a number between 1 and 255. The default value is 3. For hops with a high loss rate, you may want to set this number higher.
hello-interval	<number>	Sets the hello packet interval, in seconds, when sending of RSVP hello packets is enabled with the hello-enable parameter of the rsvp set interface command. The hello interval determines how often an RSVP interface will send out a hello packet to its neighbor in order to detect RSVP state loss on a neighbor node. Specify a decimal number between 1 and 65535. The default value is 3 seconds.

Parameter	Value	Meaning
hello-multiplier	<number>	Sets the hello multiplier variable, when sending of RSVP hello packets is enabled with the hello-enable parameter of the rsvp set interface command. If hello-interval * hello-multiplier seconds pass without a hello packet from a neighbor, the neighbor and all sessions with that neighbor are considered to be down. Specify a number between 1 and 255. The default value is 3.
bundle-interval	<number>	Sets the bundle interval, in seconds, when RSVP message aggregation is enabled with the aggregate-enable parameter of the rsvp set interface command. A bundle interval determines how long to aggregate traffic headed to a specific destination. Specify a number between 1 and 65535. The default value is 5 seconds.
blockade-aging-interval	<number>	Sets the blockade aging interval, in seconds. Blockades allow smaller reservation requests to be forwarded and established when a reservation for a larger request fails (also referred to as the “killer reservation” problem). This parameter determines how long to keep a blockade alive. Specify a number between 1 and 65535. The default value is 60 seconds.
msgid-list-interval	<number>	Sets the message ID list interval, in seconds. Specify a number between 1 and 65535. The default value is 3 seconds.
msgack-interval	<number>	Sets the message acknowledgement interval, in seconds. Specify a number between 1 and 65535. The default value is 1 second.

Restrictions

None

Example

The following command sets the RSVP hello interval to 10 seconds, the path refresh to 15 seconds, and reservation refresh to 15 seconds:

```
rs(config)# rsvp set global path-refresh-interval 15 resv-refresh-interval 15  
hello-interval 10
```

rsvp set interface

Mode

Configure

Format

rsvp set interface <name> | <ip-address> | all hello-enable aggregate-enable
msgid-extensions-enable auth-method md5|none auth-key <string>

Description

The **rsvp set interface** command allows you to configure various parameters on an RSVP interface.

Parameter	Value	Meaning
interface	<name ip-address>	Specifies the RSVP interface. Specify an interface name or IP address.
	all	Specify all to configure all RSVP interfaces.
hello-enable		Enables hello packets on this RSVP interface.
aggregate-enable		Enables RSVP message aggregation on this interface. Messages to the same destination are bundled according to the bundle interval global parameter.
msgid-extensions-enable		Enables RSVP message ID extensions for this interface.
auth-method		Selects the RSVP authentication scheme for this interface. RSVP authentication prevents unauthorized neighbors from setting up reservations on an interface.
	md5	Enables MD5 authentication.
	none	Disables authentication. This is the default.
auth-key	<string>	Specifies the authentication key for the authentication method. Specify a character string up to 16 characters.

Restrictions

None

Example

The following command configures hello packets and selects MD5 authentication on the interface 'sector1':

```
rs(config)# rsvp set interface sector1 hello-enable auth-method md5
```

rsvp set trace-level

Mode

Enable/
Configure

Format

```
rsvp set trace-level <level>
```

Description

The **rsvp set trace-level** command allows you to set the RSVP tracing level.

Parameter	Value	Meaning
trace-level	<level>	Specifies the RSVP tracing level. Specify 0 to disable tracing. Otherwise, specify a value between 1-4, where 4 provides the most detailed level of tracing.

Restrictions

None

Example

The following command sets the tracing level to 4:

```
rs# rsvp set trace-level 4
```


rsvp set trace-options

Mode

Enable/
Configure

Format

rsvp set trace-options <option>

Description

The **rsvp set trace-options** command allows you to enable the type of tracing that is performed.

Parameter	Value	Meaning
trace-options	<option>	Specifies the type of tracing to be performed. Specify one or more of the following:
	path	Enables path tracing.
	resv	Enables resv tracing.
	traffic-control	Enables traffic control tracing.
	session	Enables session tracing.
	packets	Enables packet tracing.
	timer	Enables timer tracing.
	error	Enables error tracing.
	none	No tracing is displayed.
	all	All tracing is displayed.

Restrictions

None

Example

The following command enables path tracing:

```

rs# rsvp set trace-options path

```

rsvp show all

Mode

Enable

Format

rsvp show all

Description

The **rsvp show all** command allows you to display various RSVP information and statistics.

Restrictions

None.

Example

The following is an example of the **rsvp show all** command:

```
RS# rsvp show all
RSVP Global Configuration:
-----
  RSVP Instance: <rsvp_1>
  -----
  path refresh interval: 1 sec. path multiplier: 255
  resv refresh interval: 255 sec. resv multiplier: 255
  hello interval: 3 sec. hello multiplier: 1
  bundle interval: 65535 sec.
  msgid-list interval: 1 sec.
  msgack interval: 65535 sec.
  blockade aging interval: 65535 sec.

  trace flags: 00 trace level: 0

Path State Blocks:
-----
RSVP_PSB <rsvp_1>: (psb = 0x82abbfd8)
  session-attr: name: LSP1 flags: 0x2 setup-pri: 7 holding-pri: 0
  session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202
  send-templ: sender: 2.2.2.2 lsp-id: 5
  prev-hop: 0.0.0.0 lih: 0
  in-if: <Local-API> out-if: <to_rs5>
  explicit-route: 15.15.15.2=>16.16.16.1
  sender-tspec: qos: CL cdr: 0 pbs: 0 pdr: 2139095040 mpu: 20 mtu: 1436
  block-tspec:
  psb refresh timer: time-to-expire: 0.190000 sec.
  psb cleanup timer: time-to-expire: 254.720000 sec.
  ref-count: 1
  LSP-handle: 0x82b9a730
  Session: 0x82b9aaa0

RSVP_PSB <rsvp_1>: (psb = 0x82abaf28)
  session-attr: name: LSP4 flags: 0x0 setup-pri: 7 holding-pri: 0
  session: end-point: 4.4.4.4 tunnel-id: 10 ext-tunnel-id: 0x2020202
  send-templ: sender: 2.2.2.2 lsp-id: 4
  prev-hop: 0.0.0.0 lih: 0
  in-if: <Local-API> out-if: <to_rs5>
  explicit-route: 15.15.15.2=>16.16.16.1
  sender-tspec: qos: CL cdr: 0 pbs: 0 pdr: 2139095040 mpu: 20 mtu: 1436
  block-tspec:
  psb refresh timer: time-to-expire: 0.200000 sec.
```

```

RS# rsvp show all
RSVP Global Configuration:
    psb cleanup timer:  time-to-expire: 254.730000 sec.
    ref-count: 1
    LSP-handle: 0x82ab9be0
    Session: 0x82ab9a90

Resv State Blocks:
-----

RSVP_RSB <rsvp_1>: (rsb = 0x82b9ab80)
    session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202
    style: FF
    in-if: <to_rs5>
    rsb refresh timer:  time-to-expire: 0.000000 sec.
    filter-spec: sender: 2.2.2.2 lsp-id: 5
    remote-labels: [20]
    local-labels: []
    filt-spec cleanup timer:  time-to-expire: 336.270000 sec.
    Session: 0x82b9aaa0

RSVP_RSB <rsvp_1>: (rsb = 0x82b98948)
    session: end-point: 4.4.4.4 tunnel-id: 10 ext-tunnel-id: 0x2020202
    style: FF
    in-if: <to_rs5>
    rsb refresh timer:  time-to-expire: 0.000000 sec.
    filter-spec: sender: 2.2.2.2 lsp-id: 4
    remote-labels: [19]
    local-labels: []
    filt-spec cleanup timer:  time-to-expire: 327.670000 sec.
    Session: 0x82ab9a90

Traffic-control State Blocks:
-----

RSVP_TCSB <rsvp_1>: (tcsb = 0x82b9c670)
    session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202
    filter-spec: sender: 2.2.2.2 lsp-id: 5
    Session: 0x82b9aaa0

RSVP_TCSB <rsvp_1>: (tcsb = 0x82ab4078)
    session: end-point: 4.4.4.4 tunnel-id: 10 ext-tunnel-id: 0x2020202
    filter-spec: sender: 2.2.2.2 lsp-id: 4
    Session: 0x82ab9a90

Sessions:
-----

RSVP_SM <rsvp_1>: (session = 0x82b9aaa0)
    session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202
    next-hop: 15.15.15.2 <to_rs5>
    sender: 2.2.2.2
    Neighbor: 0x82b99580

RSVP_SM <rsvp_1>: (session = 0x82ab9a90)
    session: end-point: 4.4.4.4 tunnel-id: 10 ext-tunnel-id: 0x2020202
    next-hop: 15.15.15.2 <to_rs5>
    sender: 2.2.2.2
    Neighbor: 0x82b99580

Neighbors:
-----

RSVP_SM <rsvp_1>: (neighbor = 0x82b99580), next-hop: 15.15.15.2 <to_rs5>
    No. of session: 2

```

Table 62-1 Display field descriptions for the rsvp show all command

Field	Description
RSVP Global Configuration	Displays parameter values that are applied to all RSVP interfaces. See the rsvp show global command for specific information.
Path State Blocks	Displays RSVP path state block information. See the rsvp show psb command for specific information.
Resv State Blocks	Displays RSVP reservation state block information. See the rsvp show rsb command for specific information.
Traffic-control State Blocks	Displays RSVP traffic control state block information. See the rsvp show tcsb command for specific information.
Sessions	Displays RSVP session information. See the rsvp show session command for specific information.
Neighbors	Displays information about RSVP neighbors. See the rsvp show neighbors command for specific information.

rsvp show global

Mode
Enable

Format

rsvp show global

Description

The **rsvp show global** command allows you to display the values of parameters that are applied to all RSVP interfaces. Default parameter values can be changed using the **rsvp set global** command.

Restrictions

None.

Example

The following is an example of the **rsvp show global** command:

```
RS# rsvp show global
RSVP Global Configuration:
-----
    RSVP Instance: <rsvp_1>
    -----
    path refresh interval: 1 sec.  path multiplier:      255
    resv refresh interval: 255 sec.  resv multiplier:    255
    hello interval:       3 sec.  hello multiplier:     1
    bundle interval:      65535 sec.
    msgid-list interval:  1 sec.
    msgack interval:      65535 sec.
    blockade aging interval:65535 sec.

    trace flags:          00      trace level:         0
```

Table 62-2 Display field descriptions for the rsvp show global command

Field	Description
RSVP Instance	Internal identifier for RSVP.
path refresh interval	Path refresh interval (in seconds).
path multiplier	Path multiplier variable.
resv refresh interval	Reservation request interval (in seconds).

Table 62-2 Display field descriptions for the rsvp show global command

Field	Description
resv multiplier	Reservation multiplier variable.
hello interval	Hello packet interval (in seconds).
hello multiplier	Hello multiplier variable.
bundle interval	Bundle interval (in seconds) for aggregating traffic.
msgid-list interval	Message ID list interval (in seconds).
msgack interval	Message acknowledgement interval (in seconds).
blockade aging interval	Blockade aging interval (in seconds).
trace flags	Trace options set with the rsvp set trace-options command.
trace level	Trace level set with the rsvp set trace-level command.

rsvp show interface

Mode

Enable

Format

```
rsvp show interface <name> [< ip-address>] all [brief] [verbose] [statistics]
```

Description

The **rsvp show interface** command allows you to display RSVP interface information.

Parameter	Value	Meaning
interface	<name ip-address>	Displays RSVP interface information. Specify an interface name or an IP address.
	all	Specify all to display information on all RSVP interfaces.
brief		Displays a summary of the information. This is the default.
verbose		Displays detailed information.
statistics		Displays statistics information.

Restrictions

None.

Example

The following is an example of the **rsvp show interface** command:

rs# rsvp show interface all			
Interface	Type	Attributes	Path-MTU

RS7-RS1	Enet/POS	<>	1436
RS7-RS3	Enet/POS	<AUTH_EN HELLO REF-RED MSG-ID>	1482
RS7-RS4	Enet/POS	<HELLO>	1482

Table 62-3 Display field descriptions for the rsvp show interface command

Field	Description
Interface	Interface name.
Type	Encapsulation type.
Attributes	Attributes configured with the rsvp set interface command.
Path-MTU	MTU configured with the mpls set interface command.

The following is an example of the **rsvp show interface** command with the **verbose** option:

```
rs# rsvp show interface all verbose
RSVP Interface Configuration:
-----
RS7-RS1
  type: Enet/POS
  attributes: <>
  path-mtu: 1436
  path-vector-limit: 8
  hop-count-limit: 8
  rapid-retransmit-interval: 1000 sec.
  rapid-retransmit-delta: 2 sec.
  rapid-retry-limit: 3
  current-msg-id: 0x0
  epoch: 0xa3
  seq-no: 0x0:0x356a7321
RS7-RS3
  type: Enet/POS
  attributes: <AUTH_EN HELLO REF-RED MSG-ID>
  path-mtu: 1482
  auth-key: olive
  path-vector-limit: 8
  hop-count-limit: 8
  rapid-retransmit-interval: 1000 sec.
  rapid-retransmit-delta: 2 sec.
  rapid-retry-limit: 3
  current-msg-id: 0x3
  epoch: 0xa3
  seq-no: 0x0:0x356c1362
```

Table 62-4 Display field descriptions for the rsvp show interface command with verbose option

Field	Description
type	Interface type.
attributes	Attributes set with the rsvp set interface command.
path-mtu	MTU for the path.
path-vector-limit	Vector limit for the path.
hop-count-limit	Hop limit.

Table 62-4 Display field descriptions for the rsvp show interface command with verbose option

Field	Description
rapid-retransmit-interval	Message ID extensions refresh timers set with rsvp set global command.
rapid-retransmit-delta	Message ID extensions refresh timers set with rsvp set global command.
rapid-retry-limit	Message ID extensions refresh timers set with rsvp set global command.
current-msg-id	Message ID.

The following is an example of the **rsvp show interface** command with the **statistics** option:

```

rs# rsvp show interface RS7-RS1 statistics
RSVP Interface Configuration:
-----
RS7-RS1
  type:          Enet/POS
  attributes:    <>
  path-mtu:      1436

  Send Statistics
  -----
  path:          0          resv:          2337
  path-err:      0          resv-err:       0
  path-tear:     0          resv-tear:      0
  resv-conf:     0
  hello:         0          bundle:         0
  s-refresh:     0          msg-acks:       0

  Recv Statistics
  -----
  path:          2416       resv:          0
  path-err:      0          resv-err:       0
  path-tear:     3          resv-tear:      0
  resv-conf:     0
  hello:         0          bundle:         0
  s-refresh:     0          msg-acks:       0
  bad packets:   0

```

Table 62-5 Display field descriptions for the rsvp show interface command with statistics option

Field	Description
RSVP Interface Configuration	Configuration for the indicated interface.
Send Statistics	Statistics on RSVP messages sent.
Recv Statistics	Statistics on RSVP messages received.

rsvp show neighbors

Mode
Enable

Format

rsvp show neighbors <name> | <ip-address> | all

Description

The **rsvp show neighbors** command allows you to display information about RSVP neighbors.

Parameter	Value	Meaning
neighbors	<name ip-address>	Displays information about RSVP neighbors. Specify an interface name or an IP address.
	all	Specify all to display information on all interfaces.

Restrictions

None.

Example

The following is an example of the **rsvp show neighbors** command:

```
RS# rsvp show neighbors all
Neighbors:
-----

RSVP_SM <rsvp_1>: (neighbor = 0x82fef1e0), next-hop: 201.135.89.130 <RS3-RS5>
      No. of session: 2

RSVP_SM <rsvp_1>: (neighbor = 0x82ff55a8), next-hop: 200.135.89.73 <RS3-RS7>
      No. of session: 0
```

Table 62-6 Display field descriptions for the rsvp show neighbors command

Field	Description
Neighbors	Internal identifier for RSVP neighbor.

Table 62-6 Display field descriptions for the rsvp show neighbors command

Field	Description
next-hop	IP address of next hop.
No. of session	Number of RSVP sessions with neighbor.

rsvp show psb

Mode

Enable

Format

rsvp show psb <name> | <ip-address> | all

Description

The **rsvp show psb** command allows you to display RSVP path state block objects and sub-objects, as specified by RFC 2210.

Parameter	Value	Meaning
psb	<name ip-address>	Displays path state block information. Specify an interface name or an IP address.
	all	Specify all to display information on all interfaces.

Restrictions

None.

Example

The following is an example of the **rsvp show psb** command:

```
RS7# rsvp show psb all

Path State Blocks:
-----

RSVP_PSB <rsvp_1>: (psb = 0x81f88e50)
  session-attr: name: dl1_r7-r3-r5-r2 flags: 0x2 setup-pri: 7 holding-pri: 0
  session: end-point: 2.2.2.2 tunnel-id: 16387 ext-tunnel-id: 0x7070707
  send-templ: sender: 7.7.7.7 tunnel-id: 12
  prev-hop: 0.0.0.0 lih: 0
  in-if: <Local-API> out-if: <RS7-RS3>
  explicit-route: 200.135.89.76=>201.135.89.130=>201.135.89.197
  sender-tspec: qos: CL cdr: 0 pbs: 0 pdr: 2139095040 mpu: 20 mtu: 1436
  block-tspec:
  psb refresh timer:   time-to-expire: 11.200000 sec.
  psb cleanup timer:  time-to-expire: 71.200000 sec.
  ref-count: 1
  LSP-handle: 0x82a4ca88
  Session: 0x82a5c508
```

rsvp show rsb

Mode

Enable

Format

```
rsvp show rsb <name> |< ip-address> | all
```

Description

The **rsvp show rsb** command allows you to display RSVP reservation state block objects and sub-objects, as specified by RFC 2210.

Parameter	Value	Meaning
rsb	<name ip-address>	Displays reservation state block information. Specify an interface name or an IP address.
	all	Specify all to display information on all interfaces.

Restrictions

None.

Example

The following is an example of the **rsvp show rsb** command:

```
RS5# rsvp show rsb all

Resv State Blocks:
-----

RSVP_RSB <rsvp_1>: (rsb = 0x82b9ab80)
  session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202
  style: FF
  in-if: <to_rs5>
  rsb refresh timer:  time-to-expire: 0.000000 sec.
  filter-spec: sender: 2.2.2.2 lsp-id: 5
  remote-labels: [20]
  local-labels: []
  filt-spec cleanup timer:  time-to-expire: 539.820000 sec.
  Session: 0x82b9aaa0
```

rsvp show session

Mode
Enable

Format

rsvp show session <name> |< ip-address> | all

Description

The **rsvp show session** command allows you to display RSVP session information.

Parameter	Value	Meaning
session	<name ip-address>	Displays RSVP session information. Specify an interface name or an IP address.
	all	Specify all to display information on all interfaces.

Restrictions

None.

Example

The following is an example of the **rsvp show session** command:

```
RS7# rsvp show session all

RSVP_SM <rsvp_1>: (session = 0x82b9aaa0)
  session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202
  next-hop: 15.15.15.2 <to_rs5>
  sender: 2.2.2.2
  Neighbor: 0x82b99580

RSVP_SM <rsvp_1>: (session = 0x82ab9a90)
  session: end-point: 4.4.4.4 tunnel-id: 10 ext-tunnel-id: 0x2020202
  next-hop: 15.15.15.2 <to_rs5>
  sender: 2.2.2.2
  Neighbor: 0x82b99580
```

Table 62-7 Display field descriptions for the rsvp show session command

Field	Description
end-point	Session destination.
next-hop	Next hop for the session.
sender	Session source.
Neighbor	Session neighbor.

rsvp show tcsb

Mode

Enable

Format

rsvp show tcsb <name> | <ip-address> | all

Description

The **rsvp show tcsb** command allows you to display RSVP traffic control state block objects and sub-objects, as specified by RFC 2210.

Parameter	Value	Meaning
tcsb	<name ip-address>	Displays traffic-control state block information. Specify an interface name or an IP address.
	all	Specify all to display information on all interfaces.

Restrictions

None.

Example

The following is an example of the **rsvp show tcsb** command:

<pre>RS5# rsvp show tcsb all Traffic-control State Blocks: ----- RSVP_TCSB <rsvp_1>: (tcsb = 0x82b9c670) session: end-point: 4.4.4.4 tunnel-id: 7 ext-tunnel-id: 0x2020202 filter-spec: sender: 2.2.2.2 lsp-id: 5 Session: 0x82b9aaa0 RSVP_TCSB <rsvp_1>: (tcsb = 0x82ab4078) session: end-point: 4.4.4.4 tunnel-id: 10 ext-tunnel-id: 0x2020202 filter-spec: sender: 2.2.2.2 lsp-id: 4 Session: 0x82ab9a90</pre>

rsvp start

Mode

Configure

Format

rsvp start

Description

The **rsvp start** command allows you to start RSVP on the RS. You must first enable RSVP on the appropriate interfaces with the **rsvp add interface** command.

Parameter	Value	Meaning
start		Enables RSVP functionality.

Restrictions

None

Example

The following commands enable RSVP on the interface 'group1' and start RSVP on the RS:

```
rs(config)# rsvp add interface group1
rs(config)# rsvp start
```


63 SAVE COMMAND

save

Mode

Configure

Format

save active|startup



Note

If you are in Enable mode, you still can save the active configuration changes to the Startup configuration file by entering the **copy active to startup** command.

Description

The **save** command saves the configuration changes you have entered during the current CLI session.

Parameter	Value	Meaning
active		If you use the active keyword, uncommitted changes in the scratchpad are activated. The RS accumulates configuration commands in the scratchpad until you activate them or clear them (or reboot). When you activate the changes, the RS runs the commands.
startup		If you use the startup keyword, the configuration of the running system is saved in the Startup configuration file and re-instated by the server the next time you reboot.

Restrictions

None.

save

save command

64 SERVICE COMMANDS

The **service** commands allow administrators to create rate-limiting services. With this facility, multiple users can use one service. Multiple services do not have to be created.

64.1 COMMAND SUMMARY

The following table lists the **service** commands. The sections following the table describe the command syntax.

<code>service <name> apply rate-limit acl <aclname> {interface <interface-name> all} port <port-number></code>
<code>service <name> apply rate-limit mf-classifier {interface <interface-name> all} port <port-number> [source-addr-mask <srcadd>] [destination-addr-mask <dstadd>] [source-port <num-or-numrange> <port>] [destination-port <num-or-numrange> <port>] [tos <num>] [tos-mask <tosmask>] [any]</code>
<code>service <name> create rate-limit aggregate rate <rate> [no-action drop-packets lower-priority lower-priority-except-control tos-precedence-rewrite <num> tos-precedence-rewrite-lower-priority <num> tos-rewrite <num> tos-rewrite-lower-priority <num>] [time-select <num>]</code>
<code>service <name> create rate-limit burst-safe car-rate <rate> burst-rate <rate> [car-no-action car-drop-packets car-lower-priority car-lower-priority-except-control car-tos-precedence-rewrite <num> car-tos-precedence-rewrite-lower-priority <num> car-tos-rewrite <num> car-tos-rewrite-lower-priority <num>] [burst-no-action burst-drop-packets burst-lower-priority burst-lower-priority-except-control burst-tos-precedence-rewrite <num> burst-tos-precedence-rewrite-lower-priority <num> burst-tos-rewrite <num> burst-tos-rewrite-lower-priority <num>] [time-select <num>]</code>
<code>service <name> create rate-limit flow-aggregate rate <rate> [exceed-action <action>] [min-bandwidth <minbw>] [distribute-among <number-of-flows>] [time-select <num>]</code>
<code>service <name> create rate-limit per-flow rate <rate> [exceed-action <action>] [time-select <num>]</code>
<code>service show rate-limit aggregate <name> all [detailed show-applied]</code>
<code>service show rate-limit all [detailed show-applied]</code>

service show rate-limit burst-safe < <i>string</i> > all [detailed show-applied]
service show rate-limit flow-aggregate < <i>name</i> > all [detailed show-applied]
service show rate-limit per-flow < <i>name</i> > all [detailed show-applied]

service apply rate-limit acl

Mode

Configure

Format

```
service <name> apply rate-limit acl <aclname> {interface <interface-name> | all} | port  
<port-number>
```

Description

The **service apply rate limit** command applies a previously-defined rate limit service to an interface or to a port. It also specifies the traffic profile, via the ACL, to which the rate limit service applies.

Parameter	Value	Meaning
service	<name>	Identifies the rate limit service to be applied.
acl	<acl-name>	Name of the ACL that defines the traffic to which the rate limit service will be applied.
interface	<interface-name>	Specify to which interface the service will be applied.
	all	Applies the service to all interfaces.
port	<port-number>	Specify to which port the service will be applied. You can apply a service only to ports in L4 bridging mode.

Restrictions

None.

Example

Apply a service to an interface *sqainterface1* and specify the ACL to use for rate limiting.

```
rs(config)# service priorityaggregate1 apply rate-limit acl testacl1 interface  
interface1
```

service apply rate-limit mf-classifier

Mode

Configure

Format

```
service <name> apply rate-limit mf-classifier {interface <interface-name> | all} | port
<port-number> [source-addr-mask <srcadd>] [destination-addr-mask <dstadd>] [source-port
<num-or-numrange> | <port>] [destination-port <num-or-numrange> | <port>] [tos <num>] [tos-mask
<tosmask>] [any]
```

Description

The **service apply rate-limit mf-classifier** (Multi Field Classifier) command applies a rate limit service to an interface or to a port. Instead of using an ACL to define a traffic profile, you can use the various parameters in this command to define the traffic profile for the rate limit service.

Parameter	Value	Meaning
service	<name>	Identifies the rate limit service to be applied.
interface	<intfname>	Specify to which interface the service will be applied. .
	all	Applies the service to all interfaces.
port	<port>	Specify to which port the service will be applied. You can apply a service only to ports in L4 bridging mode.
source-addr-mask	<srcadd>	The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format ("255.255.0.0") or the CIDR format ("/16")
destination-addr-mask	<dstadd>	The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.
source-port		You can specify a port number or a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024). You can also enter a keyword that identifies the port. The ports of some popular services have been defined as keywords. .
	dns	DNS port (53)
	finger	Finger port (79)

Parameter	Value	Meaning
	ftp-cmd	FTP command port (21)
	ftp-data	FTP data port (20)
	http	HTTP (WWW) port (80)
	https	HTTP-Secure (WWW) port (443)
	imap3	IMAP3 port (220)
	imap4	IMAP4 port (143)
	lpr	lpr port (515)
	nfs	NFS port (2049)
	nntp	NNTP port (119)
	ntp	NTP port (123)
	pop3	POP3 port (110)
	portmapper	Portmapper port (111)
	rexec	R-Exec port (512)
	rlogin	R-Login port (513)
	rshell	R-Shell port (514)
	snmp	SNMP port (161)
	smtp	SMTP port (25)
	telnet	Telnet port (23)
	tftp	TFTP port (69)
	x11	X11 port (6000)
destination-port		Specify the destination port of the rate-limited traffic. The requirements, restrictions and possible values for this parameter are the same as those of the source-port parameter.
tos	<num>	Specify the IP ToS (Type of Service) value. You can specify a ToS value from 0 – 255.
tos-mask	<tosmask>	Mask value used for the ToS byte. You can specify a mask value from 1– 255. Default is 30 .
	any	Specify any for any ToS value.

Restrictions

None.

Example

The following example applies the service *priorityaggregate1* to an interface.

```
rs(config)# service priorityaggregate1 apply rate-limit mf-classifier  
interface sqainterface1 source-addr-mask 10.10.10.80 source-port 80 tos 2
```

service create rate-limit aggregate

Mode

Configure

Format

```
service <name> create rate-limit aggregate rate <rate> [no-action | drop-packets |
lower-priority | lower-priority-except-control | tos-precedence-rewrite <num> |
tos-precedence-rewrite-lower-priority <num> | tos-rewrite <num> |
tos-rewrite-lower-priority <num>] [time-select <num>]
```

Description

The **service create rate-limit aggregate** command specifies the rate limiting service for an aggregation of flows. This service affects the entire aggregation and not just individual flows

Parameter	Value	Meaning
service	<name>	Identifies the rate limit service.
rate	<rate>	The rate limit, in bits per second (bps), for the aggregation of flows. Enter a value between 3000 to 1000000000, inclusive.
no-action		Specifies that no action will be taken when the rate limit is exceeded.
drop-packets		Specifies that packets will be dropped when the rate limit is exceeded.
lower-priority		Specifies that the packet's priority will be lowered when the rate limit is exceeded.
lower-priority-except-control		Specifies that the packet's priority will be lowered, except control packets, when the rate limit is exceeded.
tos-precedence-rewrite	<num>	Specifies that if the rate limit is exceeded, the ToS precedence in the packet will be rewritten. The range of <num> is 0 to 7.
tos-precedence-rewrite-lower-priority	<num>	Specifies that if the rate limit is exceeded, the ToS precedence in the packet is rewritten and the packet priority is lowered. The range of <num> is 0 to 7.
tos-rewrite	<num>	Specifies that if the rate limit is exceeded, the ToS byte is rewritten. The range of <num> is 0 to 255.
tos-rewrite-lower-priority	<num>	Specifies that if the rate limit is exceeded, the ToS byte is rewritten and the packet's priority is lowered. The range of <num> is 0 to 255.
time-select	<num>	Use this parameter to specify a time <i>slice</i> for a given rate limit service. The range for <num> is 0 to 10. The default value is chosen by the software based on the specified rate.

Restrictions

None.

Examples

The following command creates the service *priorityaggregate1* with a rate limit of 500 million bps. If this rate limit is exceeded, the router drops packets.

```
rs(config)# service priorityaggregate1 create rate-limit aggregate rate  
500000000 drop-packets
```

service create rate-limit burst-safe

Mode

Configure

Format

```
service <name> create rate-limit burst-safe car-rate <rate> burst-rate <rate> [car-no-action |
car-drop-packets | car-lower-priority | car-lower-priority-except-control |
car-tos-precedence-rewrite <num> | car-tos-precedence-rewrite-lower-priority <num> |
car-tos-rewrite <num> | car-tos-rewrite-lower-priority <num> ] [burst-no-action |
burst-drop-packets | burst-lower-priority | burst-lower-priority-except-control |
burst-tos-precedence-rewrite <num> | burst-tos-precedence-rewrite-lower-priority <num> |
burst-tos-rewrite <num> | burst-tos-rewrite-lower-priority <num>] [time-select <num>]
```

Description

The **service create rate-limit burst-safe** command creates a rate limit service based on the committed access rate (CAR) and burst rate.

Parameter	Value	Meaning
service	<name>	Identifies the rate limit service.
car-rate	<rate>	The CAR, in bits per second (bps). Specify a number between 3000 to 1000000000, inclusive.
car-no-action		Specifies that if the CAR is exceeded, no action is taken.
car-drop-packets		Specifies that if the CAR is exceeded, packets are dropped.
car-lower-priority		Specifies that if the CAR is exceeded, the packet priority is lowered.
car-lower-priority-except-control		Specifies that if the CAR is exceeded, the packet's priority is lowered if it is not a control packet.
car-tos-precedence-rewrite	<num>	Specifies that if the CAR is exceeded, the ToS precedence is rewritten to the specified value. Enter a number between 0 and 7, inclusive, for the ToS precedence.
car-tos-precedence-rewrite-lower-priority	<num>	Specifies that if the CAR is exceeded, the ToS precedence is rewritten to the specified value and the packet priority is lowered. Enter a number between 0 and 7, inclusive, for the ToS precedence.
car-tos-rewrite	<num>	Specifies that if the CAR is exceeded, the ToS byte is rewritten to the value specified. Specify a value between 0 and 255, inclusive, for the ToS byte.

Parameter	Value	Meaning
car-tos-rewrite-lower-priority	<num>	Specifies that if the CAR is exceeded, the ToS byte is rewritten to the value specified and the packet priority is lowered. Specify a value between 0 and 255, inclusive, for the ToS byte.
burst-rate	<rate>	The burst rate, in bits per second (bps), for the flow. Specify a value between 3000 and 1000000000, inclusive.
burst-no-action		Specifies that if the burst rate is exceeded, no action will be taken.
burst-drop-packets		Specifies that if the burst rate is exceeded, the packets are dropped.
burst-lower-priority		Specifies that if the burst rate is exceeded, the packet's priority is lowered.
burst-lower-priority-except-control		Specifies that if the burst rate is exceeded, the packet's priority is lowered if it is not a control packet.
burst-tos-precedence-rewrite	<num>	Specifies that if the burst rate is exceeded, the ToS precedence is rewritten to the value specified. Specify a value between 0 and 7, inclusive, for the ToS precedence.
burst-tos-precedence-rewrite-lower-priority	<num>	Specifies that if the burst rate is exceeded, the ToS precedence is rewritten to the value specified and the packet priority is lowered. Specify a value between 0 and 7, inclusive, for the ToS precedence.
burst-tos-rewrite	<num>	Specifies that if the burst rate is exceeded, the ToS byte is rewritten to the value specified. Specify a value between 0 and 255, inclusive, for the ToS byte.
burst-tos-rewrite-lower-priority	<num>	Specifies that if the burst rate is exceeded, the ToS byte is rewritten to the value specified and the packet priority is lowered. Specify a value between 0 and 255, inclusive, for the ToS byte.
time-select	<num>	Use this parameter to specify a time <i>slice</i> for a given rate limit service. The range for <num> is 0 to 10. The default value is chosen by the software based on the specified rate.

Restrictions

None.

Example

The following command creates the service *carlimit1* with a CAR of 300 million bps. If this CAR is exceeded, packets will be dropped.

```
rs(config)# service carlimit1 create rate-limit burst-safe car-rate 300000000
car-drop-packets
```

service create rate-limit flow-aggregate

Mode

Configure

Format

```
service <name> create rate-limit flow-aggregate rate <rate> [exceed-action <action>]  
[min-bandwidth <minbw>] [distribute-among <number-of-flows>] | time-select <num>]
```

Description

The **service create rate-limit flow-aggregate** command creates a software-based aggregate rate limit service.

Parameter	Value	Meaning
service	<name>	Identifies the rate limit service.
rate	<rate>	The rate limit, in bits per second (bps), for the flow. Enter a value between 3000 to 1000000000, inclusive.
exceed-action	<action>	The action taken if the rate limit is exceeded.
	drop-packets	Drop the incoming packets.
	set-priority-low	Set the packet priority to low.
	set-priority-medium	Set the packet priority to medium.
	set-priority-high	Set the packet priority to high.
min-bandwidth	<minbw>	The minimum bandwidth for each flow. Specify a value between 3000 and 1000000000, inclusive.
distribute-among		The number of flows among which freed bandwidth is distributed. Enter a distribution value of 1 to 10, inclusive. The default is 1.
time-select	<num>	Use this parameter to specify a time <i>slice</i> for a given rate limit service. The range for <num> is 0 to 10. The default value is chosen by the software based on the specified rate.

Restrictions

None.

Example

The following command creates the service *priorityflowaggregate* with a rate limit of 400 million bps. Packets are dropped if the rate limit exceeds 400 million. The minimum bandwidth is 400 million which is distributed across 10 flows.

```
rs(config)# service priorityflowaggregate create rate-limit flow-aggregate  
rate 400000000 exceed-action drop-packets min-bandwidth 400000000  
distribute-among 10
```


service create rate-limit per-flow

Mode

Configure

Format

```
service <name> create rate-limit per-flow rate <rate> [exceed-action <action>] [time-select <num>]
```

Description

The **service create rate-limit per-flow** command creates a rate limit service that limits an individual flow to the specified rate.

Parameter	Value	Meaning
rate	<rate>	The rate limit, in bits per second (bps), for the flow. Specify a number between 3000 and 1000000000, inclusive.
exceed-action	<action>	The action taken if the rate limit is exceeded.
	drop-packets	Drop the packets.
	set-priority-low	Set the packet priority to low.
	set-priority-medium	Set the packet priority to medium.
	set-priority-high	Set the packet priority to high.
time-select	<num>	Use this parameter to specify a time <i>slice</i> for a given rate limit service. The range for <num> is 0 to 10. The default value is chosen by the software based on the specified rate.

Restrictions

None.

Example

The following command creates the service *priorityperflow* with a rate limit of 900 million bps. The packets priority is set to low if the rate limit is exceeded.

```
rs(config)# service priorityperflow create rate-limit rate 900000000  
set-priority-low
```

service show rate-limit aggregate

Mode
Enable

Format

service show rate-limit aggregate <name> | all [detailed | show-applied]

Description

The **service show rate-limit aggregate** command displays the specified aggregate rate limit service(s).

Parameter	Value	Meaning
aggregate	<name>	Name of the aggregate rate limit service.
	all	Specify all to display all aggregate rate limit services.
detailed		Specifies a detailed display.
show-applied		Displays where the service was applied.

Restrictions

None.

Example

Following is an example of the **service show rate-limit aggregate** command.

```
rs# service show rate-limit aggregate testservice2
-----
Service Name: testservice2           Service Type : Aggregate Rate Limit
Rate       : 600000000 bps          Exceed Action: Drop Packets
Timeselect : 9                      Credits   : 83
-----
```

Table 64-1 Display field descriptions for the service show rate-limit aggregate command

FIELD	DESCRIPTION
Service Name	Name of the service displayed.
Rate	Displays the rate limiting rate.
Service Type	Displays the type of service.
Exceed Action	Displays the action to be taken.

service show rate-limit all

Mode

Enable

Format

service show rate-limit all [detailed | show-applied]

Description

The service show rate-limit all command displays all rate limit services.

Parameter	Value	Meaning
detailed		Specifies a detailed display.
show-applied		Displays where the service was applied.

Restrictions

None.

Example

Following is an example of the **service show rate-limit all** command.

```

rs# service show rate-limit all show-applied
-----
Service Name : stoptraffic1      Service Type : Flow Aggregate Rate Limit
Rate         : 5000000 bps      Exceed Action : Drop Packets

Service stoptraffic1 is applied on interface site1 with following
traffic classification
Source IP/Mask   Dest. IP/Mask   SrcPort   DstPort   TOS TOS-MASK   Prot
-----
1.2.3.4/24      anywhere      80        any       any None      IP
-----
Service Name : stoptraffic2      Service Type: Aggregate Rate Limit
Rate         : 6000000 bps      Exceed Action : Lower Priority

Service stoptraffic2 is not applied anywhere
-----
Service Name : stoptraffic3      Service Type: Aggregate Rate Limit
Rate         : 4000000 bps      Exceed Action : Drop Packets

Service stoptraffic3 is not applied anywhere
-----

```

Table 64-2 Display field descriptions for the service show rate limit all command

FIELD	DESCRIPTION
Service Name	Name of the service shown.
Rate	Displays the rate limiting rate.
Service Type	Displays the type of service.
Exceed Action	Displays the action to be taken.
Source IP/Mask	The source IP address and mask.
Dest. IP/Mask	The destination IP address and mask.
SrcPort	The source port.
DstPort	The destination port.
TOS	Type of service.
TOS-MASK	ToS mask.
Prot	The protocol used.

service show rate-limit burst-safe

Mode

Enable

Format

```
service show rate-limit burst-safe <name> | all [detailed | show-applied]
```

Description

The **service show rate-limit burst-safe** command displays the specified burst-safe rate limit services.

Parameter	Value	Meaning
burst-safe	<name>	Name of the burst-safe rate limit service.
	all	Specify all to display all burst-safe rate limit services.
detailed		Specifies a detailed display.
show-applied		Displays where the service was applied.

Restrictions

None.

Example

The following is an example of the output as a result of the applied command.

```
rs# service show rate-limit burst-safe testservice5
-----
Service Name   : testservice2           Service Type   : Burst-safe Rate Limit
Rate          : 800000000 bps          Exceed Action  : Drop Packets
-----
```

Table 64-3 Display field descriptions for the service show rate-limit burst-safe command

FIELD	DESCRIPTION
Service Name	Name of the service displayed.
Rate	Displays the rate limiting rate.
Service Type	Displays the type of service.
Exceed Action	Displays the action to be taken.

service show rate-limit flow-aggregate

Mode
Enable

Format

service show rate-limit flow-aggregate <name> | all [detailed | show-applied]

Description

The **service show rate-limit flow-aggregate** command displays the specified flow-aggregate rate limit service(s).

Parameter	Value	Meaning
flow-aggregate	<name>	Name of the flow-aggregate rate limit service.
	all	Specify all to display all flow-aggregate rate limit services.
detailed		Specifies a detailed display.
show-applied		Displays where the service was applied.

Restrictions

None.

Example

Following is an example of the **service show rate-limit flow-aggregate** command.

```
rs# service show rate-limit flow-aggregate testservice3
-----
Service Name: testservice3           Service Type : Flow Aggregate Rate Limit
Rate      : 500000000 bps           Exceed Action: Priority Medium
-----
```

Table 64-4 Display field descriptions for the service show rate-limit flow-aggregate command

FIELD	DESCRIPTION
Service Name	Name of the service displayed.
Rate	Displays the rate limiting rate.
Service Type	Displays the type of service.
Exceed Action	Displays the action to be taken.

service show rate-limit per-flow

Mode

Enable

Format

```
service show rate-limit per-flow <name> | all [detailed | show-applied]
```

Description

The **service show rate-limit per-flow** command displays the specified per-flow rate limit service(s).

Parameter	Value	Meaning
per-flow	<name>	Name of the per-flow rate limit service.
	all	Specify all to display all per-flow rate limit services.
detailed		Specifies a detailed display.
show-applied		Displays where the service was applied.

Restrictions

None.

Example

Following is an example of the **service show rate-limit per-flow** command.

```
rs# service show rate-limit per-flow testservice4
-----
Service Name: testservice4           Service Type : Per Flow Rate Limit
Rate       : 700000000 bps          Exceed Action: Priority High
-----
```

Table 64-5 Display field descriptions for the service show rate-limit per-flow command

FIELD	DESCRIPTION
Service Name	Name of the service displayed.
Rate	Displays the rate limiting rate.
Service Type	Displays the type of service.
Exceed Action	Displays the action to be taken.

65 SFS COMMANDS

The sfs commands set and display the following parameters:

- Cabletron Discovery Protocol (CDP) parameters

65.1 COMMAND SUMMARY

The following table lists the port commands. The sections following the table describe the command syntax.

<code>sfs enable cdp-hello <port-list> all-ports</code>
<code>sfs set cdp-hello transmit-frequency</code>
<code>sfs show cdp-hello port-status <port-list> all-ports</code>
<code>sfs show cdp-hello transmit-frequency</code>

sfs enable cdp-hello

Mode

Configure

Format

```
sfs enable cdp-hello <port-list>|all-ports
```

Description

The **sfs enable cdp-hello** command enables the sending of CDP (Cabletron Discovery Protocol) Hello packets. These are special packets sent out periodically by the router to announce itself to other Riverstone devices or applications. CDP Hello packets can be enabled to be sent out to all available ports or selected ports only.

Parameter	Value	Meaning
cdp-hello	<port-list>	Specifies the ports you want to enable CDP Hello packets.
	all-ports	Enables CDP Hello packets for all the RS ports.

Restrictions

None.

Examples

To enable the sending of CDP Hello packets on port 3 of slot 1:

```
rs(config)# sfs enable cdp-hello et.1.3
```

To send CDP Hello packets on all ports:

```
rs(config)# sfs enable cdp-hello all-ports
```

sfs set cdp-hello transmit-frequency

Mode

Configure

Format

```
sfs set cdp-hello transmit-frequency <secs>
```

Description

The `sfs set cdp-hello transmit-frequency` command specifies how often CDP Hello packets should be sent. The interval is specified in seconds. The default transmit frequency is one packet every 5 seconds.

Parameter	Value	Meaning
transmit-frequency	<secs>	Specifies the interval in seconds between the transmission of CDP Hello packets. Acceptable value is 1-300. Default is 5 seconds.

Restrictions

None.

Examples

To set the transmit frequency to 10 seconds:

```
rs(config)# sfs set cdp-hello transmit-frequency 10
```

sfs show cdp-hello port-status

Mode

Enable

Format

sfs show cdp-hello port-status <port-list>|all-ports

Description

The **sfs show cdp-hello port-status** command displays CDP Hello information of RS ports.

Parameter	Value	Meaning
port-status	<port-list>	Specifies the ports for which you want to display information.
	all-ports	Displays the selected information for all the RS ports.

Restrictions

None.

Examples

To display CDP Hello status on all RS ports:

```
rs# sfs show cdp-hello port-status all-ports
```

sfs show cdp-hello transmit-frequency

Mode

Enable

Format

sfs show cdp-hello transmit-frequency

Description

The **sfs show cdp-hello transmit-frequency** command display the transmit frequency of CDP Hello packets on the RS.

Restrictions

None.

Examples

To display the transmit frequency of CDP Hello packets:

```
rs# sfs show cdp-hello transmit-frequency
```


66 SHOW COMMAND

show

Mode

Configure

Format

show active| scratchpad| startup

Description

The **show** command displays the configuration of your running system as well as any non-committed changes in the scratchpad. Each CLI command is preceded with a number. This number can be used with the **negate** command to negate one or more commands. If you see the character **E** (for Error) immediately following the command number, it means the command did not execute successfully due to an earlier error condition. To get rid of the command in error, you can either negate it or fix the original error condition.

There are three modes for the **show** command: **active**, **scratchpad**, and **startup**. Specifying **active** shows the configuration that is currently active on the router. Specifying **scratchpad** shows the configuration currently in the scratchpad that has yet to be applied as active. Specifying **startup** shows the configuration that will be applied at the next bootup. You must specify one of these three modes as a parameter for the show command.

When viewing the active configuration file, the CLI displays the configuration file command lines with the following possible annotations:

- Commands without errors are displayed without any annotation.
- Commands with errors are annotated with an “E”.
- If a particular command has been applied such that it can be expanded on additional interfaces/modules, then it is annotated with a “P”. For example, if you enable STP on all ports in the current system, but the RS contains only one module, then that particular command will be extended to all modules when they have been added to the RS.

A command like **stp enable et.*.*** would be displayed as follows:

```
P: stp enable et.*.*
```

indicating that it is only partially applied. If you add more modules to the RS at a later date and then update the configuration file to encompass all of the available modules in the RS, the “P:” portion of the above command line would disappear from the configuration file.

If a potentially partial command, which was originally configured to encompass all of the available modules on the RS, becomes only partially activated (after a hotswap or some such chassis reconfiguration), then the status of that command line will automatically change to “P:”, indicating a partial completion status.



Note Commands with no annotation or annotated with a “P:” are not in error.

Parameter	Value	Meaning
active		Specify this parameter to show the configuration currently active on the router.
scratchpad		Specify this parameter to show the configuration currently in the scratchpad that has yet to be applied as active.
startup		Specify this parameter to show the configuration that will be applied at the next bootup.

Restrictions

None.

Examples

The following command shows the active configuration:

```
rs(config)# show active
Running system configuration:
!
! Last modified from Console on 2000-02-09 13:00:46
!
1E: atm create vcl port at.9.1.1.200
!
2E: interface create ip pos11 address-netmask 20.11.11.20/24
peer-address 20.11
.11.21 type point-to-point port so.13.1
3E: interface create ip atm1 address-netmask 12.1.1.1/24 port
at.9.1.1.200
4 : interface add ip en0 address-netmask 134.141.179.147/27
!
5 : ip add route 134.141.173.0/24 gateway 134.141.179.129
6 : ip add route 134.141.176.0/24 gateway 134.141.179.129
7 : ip add route 134.141.172.0/24 gateway 134.141.179.129
!
8 : system set idle-timeout telnet 0
9 : system set idle-timeout serial 0
```


The following command shows the configuration currently in the scratchpad:

```
rs(config)# show scratchpad

***** Non-committed changes in Scratchpad *****
1*: atm define service service1 srv-cat cbr pcr 100000
!
2*: vlan create vlan1 ip id 5
!
3*: ip add route default host gateway 100.0.0.1
```

The following command shows the saved startup configuration that will be loaded at the next bootup:

```
rs(config)# show startup
!
! Startup configuration for the next system reboot
!
! Last modified from Console on 1999-12-28 16:51:19
!
version 3.1
atm create vcl port at.9.1.1.200
interface create ip pos11 address-netmask 20.11.11.20/24 peer-address
20.11.11.2
1 type point-to-point port so.13.1
interface create ip atm1 address-netmask 12.1.1.1/24 port at.9.1.1.200
interface add ip en0 address-netmask 134.141.179.147/27
ip add route 134.141.173.0/24 gateway 134.141.179.129
ip add route 134.141.176.0/24 gateway 134.141.179.129
ip add route 134.141.172.0/24 gateway 134.141.179.129
system set idle-timeout telnet 0
system set idle-timeout serial 0
pos set so.13.1 working protecting so.13.2
```

show

show Command

67 SLOGIN COMMAND

slogin

Mode

Enable

Format

```
slogin [<user>@]<host> [port <number>]
```

Description

The **slogin** command allows you to open a Secure Shell (SSH) session to the specified host.

Parameter	Value	Meaning
slogin	[<user>@]<host>	The host name or IP address of the remote computer that you want to access. The user name (enable or login) can optionally be specified.
port	<number>	The port through which the SSH session will be opened. Specify a port number between 1-65535. The default port number is 22.

Restrictions

None.

Examples

To open an SSH session to 'rs1':

```
rs# slogin enable@rs1
```


68 SMARTTRUNK COMMANDS

The `smarttrunk` commands let you display and set parameters for SmartTRUNK ports. SmartTRUNK ports are groups of ports that have been logically combined to increase throughput and provide link redundancy.

68.1 COMMAND SUMMARY

The following table lists the `smarttrunk` commands. The sections following the table describe the command syntax.

<code>smarttrunk add ports <port list> to <smarttrunk></code>
<code>smarttrunk clear load-distribution <smarttrunk></code>
<code>smarttrunk create <smarttrunk> protocol <protocol></code>
<code>smarttrunk set load-policy round-robin link-utilization single-load-policy on <smarttrunk list> all-smarttrunks</code>
<code>smarttrunk set load-redistribution-params <smarttrunk list> all-smarttrunks enable [<parameters>]</code>
<code>smarttrunk show connections <smarttrunk list> all-smarttrunks</code>
<code>smarttrunk show distribution <smarttrunk list> all-smarttrunks</code>
<code>smarttrunk show load-redistribution-params <smarttrunk list> all-smarttrunks</code>
<code>smarttrunk show protocol-state <smarttrunk list> all-smarttrunks</code>
<code>smarttrunk show trunks <smarttrunk list> all-smarttrunks</code>

smarttrunk add ports

Mode

Configure

Format

```
smarttrunk add ports <port list> to <smarttrunk>
```

Description

The smarttrunk **add ports** command allows you to add the ports specified in <port list> to a SmartTRUNK. The SmartTRUNK must already have been created with the smarttrunk **create** command. The ports in the SmartTRUNK must be set to full duplex.

Parameter	Value	Meaning
ports	<port list>	One or more ports to be added to an existing SmartTRUNK. All the ports in the SmartTRUNK must be connected to the same destination.
	<smarttrunk>	The name of an existing SmartTRUNK.

Restrictions

Ports added to a SmartTRUNK must:

- Be set to full duplex
- Be in the default VLAN
- Have the same properties (L2 aging, STP state, and so on)

Example

To add ports **et.1.1**, **et.1.2**, and **et.1.3** to SmartTRUNK **st.1**:

```
rs(config)# smarttrunk add ports et.1.(1-3) to st.1
```

smartrunk clear load-distribution

Mode

Enable

Format

```
smartrunk clear load-distribution <smartrunk list> | all-smartrunks
```

Description

The smartrunk **clear load-distribution** command is used in conjunction with the smartrunk **show distribution** command, which gathers statistics for the transmitted bytes per second flowing through the SmartTRUNK and each port in it. The smartrunk **clear load-distribution** command lets you reset load distribution statistics to zero.

Parameter	Value	Meaning
load-distribution	<smartrunk list>	The name of one or more existing SmartTRUNKs.
	all-smartrunks	Causes load distribution information to be cleared for all SmartTRUNKs.

Restrictions

None.

Example

To clear load distribution information from SmartTRUNK **st.1**:

```
rs# smartrunk clear load-distribution st.1
```

smartrunk create

Mode

Configure

Format

```
smartrunk create <smartrunk> protocol no-protocol|huntgroup|lacp [no-llap-ack]
```

Description

The smartrunk **create** command is used to create a SmartTRUNK. Once a SmartTRUNK is created, add physical ports to it with the smartrunk **add ports** command.

SmartTRUNKs on the RS are compatible with the DEC Hunt Groups control protocol. If you are connecting the SmartTRUNK to another RS, Riverstone switch, or Digital GIGAswitch/Router, you can specify that the SmartTRUNK uses the Hunt Group control protocol. SmartTRUNKs and the Hunt Groups control protocol are comprised of two protocols:

- Logical Link Aging Protocol (LLAP) – Assists in learning and aging
- Physical Link Affinity Protocol (PLAP) – Monitors and maintains the trunking states

SmartTRUNKs also support the use of 803.ad standard Link Aggregation Control Protocol (LACP), which aggregates links into Link Aggregation Groups (LAGs) and assigns them to an Aggregator (SmartTRUNK).



Note See [Chapter 35, "lacp Commands"](#) for commands used to configure LACP parameters.

If you are connecting a SmartTRUNK to a device that does not support either Hunt Groups or LACP, no control protocol is used. In this case, specify the **no-protocol** keyword in the smartrunk **create** command.

Parameter	Value	Meaning
create	<smartrunk>	The name of the SmartTRUNK to create. The name of the SmartTRUNK must be in the form st.x ; for example, st.1 .
protocol		Specifies the control protocol to be used.
	no-protocol	Specifies that no control protocol be used. Use this keyword if the SmartTRUNK is connected to a device that does not support the DEC Hunt Group control protocol or LACP.
	huntgroup	Specifies that the DEC Hunt Group control protocol be used. Use this keyword if you are connecting the SmartTRUNK to another RS, Riverstone switch, or Digital GIGAswitch/Router.

Parameter	Value	Meaning
	lacp	Specifies that the Link Aggregation Control Protocol (LACP) be used. Use this keyword if you are creating a SmartTRUNK for an Aggregator.
no-llap-ack		Specifies that no LLAP acknowledgement packets are to be sent. This option should only be used when the huntgroup protocol is used. By default, the RS sends out extra LLAP acknowledgement packets; this operation is for backward compatibility with some Cabletron products. If you specify this option, no extra LLAP packets are sent.

Restrictions

None.

Example

The following command creates a SmartTRUNK named **st.1**, using the DEC Hunt Group control protocol.

```
rs(config)# smarttrunk create st.1 protocol huntgroup
```

smartrunk set load-policy

Mode

Configure

Format

```
smartrunk set load-policy round-robin|link-utilization on <smartrunk  
list>|all-smartrunks
```

Description

The smartrunk **set load-policy** command lets you specify how a SmartTRUNK assigns flows among its ports. There are two options: round-robin (the default) and link-utilization.

Round-robin means that flows are assigned to ports on a sequential basis. The first flow goes to the first port in the SmartTRUNK, the second flow to the second port, and so on. Link-utilization means that a flow is assigned to the least-used port in the SmartTRUNK.

Parameter	Value	Meaning
load-policy	round-robin	Specifies that new flows are distributed sequentially across all ports.
	link-utilization	Specifies that new flows are set up on the least-used port in the SmartTRUNK (the default).
	single-load-policy	This option insures proper load balancing when using the round-robin load distribution policy between two or more SmartTRUNKs where two or more end-stations are connecting to the same MAC address. If this is not the case, do not use this option.
on	<smartrunk list>	The name of one or more SmartTRUNKs. Use commas to separate SmartTRUNK names.
	all-smartrunks	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None.

Example

To specify that SmartTRUNK **st.1** distribute flows based on current link utilization among its component ports:

```
rs(config)# smartrunk set load-policy on st.1 link-utilization
```

smartrunk set load-redistribution-params

Mode

Configure

Format

```
smartrunk set load-redistribution-params <smartrunk list> | all-smartrunks
redistribution [<parameters>]
```

Description

The smartrunk **set load-redistribution-params** command lets you specify various load policy parameters for SmartTRUNK Load Redistribution (SLR). Specify the **redistribution** parameter to enable load redistribution; other parameters are optional.

Parameter	Value	Meaning
load-redistribution-params	<smartrunk list>	The name of one or more SmartTRUNKs. Use commas to separate SmartTRUNK names.
	all-smartrunks	Specifies that the command be applied to all SmartTRUNKs.
dont-ignore-lwm-events		Don't ignore lwm events. By default, SLR ignores Low Water-mark events. However, by enabling lwm events, SLR can detect links that are under utilized, and redistribute flows to balance traffic across the SmartTRUNK. Low Water-mark events should be used only on SmartTRUNKs that consist of links of equal bandwidth.
enable		Enables dynamic load redistribution (SLR) of flows across ports.
stats-interval	<seconds>	Specifies the number of seconds that elapse before port statistics are gathered. Specify a number equal to or greater than 1. The default is 1 second.
redistribute-interval	<number>	Specifies the number of stats-interval periods that elapse before load redistribution is considered. Specify a number equal to or greater than 5. The default is 5 stats-interval periods.
stats-discard	<number>	Specifies the maximum number of stats-interval periods allowed with invalid statistics for the redistribute-interval . If this maximum is reached, all the statistics of a given port are discarded for the redistribute-interval . Specify a number equal to or greater than 3. The default is 3.

Parameter	Value	Meaning
hwm	<i><percentage></i>	Specifies the high water mark in percentage of capacity for SmartTRUNK ports. This threshold applies to all ports in the specified SmartTRUNK. Specify a number between 61-100. The default is 80 per cent.
mwm	<i><percentage></i>	Specifies the medium water mark in percentage of capacity for SmartTRUNK ports. This threshold applies to all ports in the specified SmartTRUNK. Specify a number between 40-60. The default is 50 per cent.
lwm	<i><percentage></i>	Specifies the low water mark in percentage of capacity for SmartTRUNK ports. This threshold applies to all ports in the specified SmartTRUNK. Specify a number between 0-39. The default is 20 per cent.
max-flow-search-attempts	<i><number of flows></i>	The maximum number of sequential flows searched for the purposes of redistribution during each Redistribution Interval; must be a value equal to or greater than 10, the default is 100 flows. This sets a limit on the amount of system resources used by SLR.
no-L2-redistribution		Specifies that L2 flows are not considered for redistribution. By default, this is disabled.
redistribute-ip		Specifies that IP L3 flows are considered for redistribution; the default is L3 flows are not considered for redistribution.
verbose		Displays load distribution messages to the Console and SYSLOG if a flow is remapped or deleted; the default is non-verbose.

Restrictions

None.

Example

To enable SLR on SmartTRUNK **st.2**:

```
rs(config)# smarttrunk set load-redistribution-params st.2 enable
```

smarttrunk show connections

Mode

Enable

Format

smarttrunk show connections <smarttrunk list> |all-smarttrunks

Description

The smarttrunk **show connections** command shows information about the SmartTRUNK connection, including the MAC address of the remote switch, and the module number and port number of each remote port. Connection information is reported only if the Hunt Group protocol is enabled for the SmartTRUNK.

Parameter	Value	Meaning
connections	<smarttrunk list>	The name of one or more SmartTRUNKs.
	all-smarttrunks	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None.

Examples

To show connection information for all SmartTRUNKs:

rs# smarttrunk show connections all-smarttrunks							
SmartTRUNK	Local Port	Remote Switch	Remote Module	Remote Port	State	Actor Key	Partner Key
st.1	et.2.1	Riverstone A9:6E:57	3	1	Up		
st.1	et.2.2	Riverstone A9:6E:57	3	2	Up		
st.1	et.2.3	Riverstone A9:6E:57	3	3	Up		
st.1	gi.3.1	Riverstone A9:6E:57	4	5	Up		
st.2	et.2.4	--	--	--	Up		
st.2	et.2.5	--	--	--	Up		
st.2	et.2.6	--	--	--	Up		



Note

In the example above, SmartTRUNK **st.2** does not use a control protocol. As a result, remote switch information cannot be communicated to this RS, and the fields are left blank.

Table 68-1 Display Field Description

FIELD	DESCRIPTION
SmartTRUNK	Name of SmartTRUNKs for which connection information is displayed.
Local Port	The ports belonging to the corresponding SmartTRUNK.
Remote Switch	An Identifier consisting of the first three bytes of the MAC address translated to its industry unique correspondence and the last three bytes of the MAC address in hexadecimal.
Remote Module	Slot number of the line card in the system at the other end of the link.
Remote Port	Corresponding line card port number in the system at the other end of the link.
State	Current link group status. Possible states are up or down . Will show down only if all links for that SmartTRUNK are down
*Actor Key	Displays the LACP Actor Aggregator's administrative key.
*Partner Key	Displays the LACP Partner system's administrative key.

*These fields appear only if one or more of the SmartTRUNKs is using LACP.

smartrunk show distribution

Mode

Enable

Format

```
smartrunk show distribution <smartrunk list>|all-smartrunks
```

Description

The smartrunk **show distribution** command provides statistics on how traffic is distributed across the ports in a SmartTRUNK.

Parameter	Value	Meaning
distribution	<smartrunk list>	The name of one or more SmartTRUNKs.
	all-smartrunks	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None.

Example

To show how traffic is distributed across the ports on SmartTRUNK **st.1**:

```
rs# smartrunk show distribution st.1
```

SmartTRUNK	Member	% Link Utilization	Link Status	Grp Status
st.1	et.1.1	38.27	Forwarding	Up
st.1	et.1.2	45.93	Forwarding	Up
st.1	et.1.3	34.05	Forwarding	Up
st.1	et.1.4	19.54	Forwarding	Up

Table 68-2 Display Field Description

FIELD	DESCRIPTION
SmartTRUNK	Name of SmartTRUNKs for which connection information is displayed.
Member	The ports belonging to the corresponding SmartTRUNK.

Table 68-2 Display Field Description (Continued)

FIELD	DESCRIPTION
Link Utilization	The percent bandwidth utilized on this SmartTRUNK link. Applies only to data transmission (not reception) on the link.
Link Status	The current status of the link. Possible values are forwarding and inactive . The inactive state occurs if a link is either manually or operationally disabled.
Grp Status	The current Link Group Status of a SmartTRUNK. Possible values are up or down . Displays down only if all links in the SmartTRUNK are down.

smartrunk show load-redistribution-params

Mode

Enable

Format

```
smartrunk show load-redistribution-params <smartrunk list> [all-smartrunks  
[configuration] [statistics] [summary]
```

Description

The smartrunk **show load-redistribution-params** command provides information on SmartTRUNK Load Redistribution configurations and statistics related to the ports.

Parameter	Value	Meaning
load-redistribution-params	<smartrunk list>	The name of one or more SmartTRUNKs.
	all-smartrunks	Specifies that the command be applied to all SmartTRUNKs.
configuration		Displays the SLR configuration of a SmartTRUNK.
statistics		Displays SLR related statistics for all ports belonging to a SmartTRUNK.
summary		Displays a count of the number of redistributed flows that have occurred since the SmartTRUNK became active.

Restrictions

None.

Example

To show the SLR configuration of SmartTRUNK **st.2**:

```
rs# smartrunk show load-redistribution-params st.2 configuration

st.2 configuration:
  Intervals (in seconds):
    Stats Interval      1 seconds
    Redistribute Interval 5 Stats Intervals
  Port Watermarks:
    HWM                 80%
    MWM                 50%
    LWM                 20%
  Options:
    Verbose             True
    Redistribute L2 Flows True
    Redistribute IP Flows False
    Ignore LWM Event    False
    Stats Discard        3 Stats Intervals
    Max Flow Search Attempts 100
```

See [Section , "smartrunk set load-redistribution-params"](#) for descriptions of each field in the configuration display.

Example

To show the SLR related statics for SmartTRUNK **st.1**:

```
rs# smartrunk show load-redistribution-params st.1 statistics
```

st.1 Output Ports	Link Utilization %capacity	Moving Avg Load %capacity	Over Capacity History	Above HWM History	Above MWM History	Below MWM History	Below LWM History	Port Capacity Mb/s
et.1.1	38.46	38.46	0	0	0	141	0	100
et.1.2	57.70	57.70	0	0	139	0	0	100
et.1.3	57.70	58.08	0	0	33	0	0	100
et.1.4	76.92	75.01	0	0	33	0	0	100

```

st.1: 1 redistributions in the last 0 Hr, 7 Min, 25 Sec
```

Table 68-3 Display Field Description

FIELD	DESCRIPTION
Output Ports	A list of ports that comprise the SmartTRUNK.
Link Utilization	Current instantaneous percent of the link's bandwidth being used.
Moving Avg Load	An average in percent of the link's bandwidth utilization.

Table 68-3 Display Field Description (Continued)

FIELD	DESCRIPTION
Over Capacity History	Number of times the link has reached full capacity
Above HWM History	Number of times traffic on the link has exceeded the High Water-mark.
Above MWM History	Number of times traffic on the link has exceeded the Medium Water-mark.
Below MWM History	Number of times traffic on the link has dropped below the Medium Water-mark.
Below LWM History	Number of times traffic on the link has dropped below the Low Water-mark. Can indicate that a link is being under utilized.
Port Capacity	The bandwidth of each port in the SmartTRUNK.

smartrunk show protocol-state

Mode
Enable

Format

smartrunk show protocol-state <smartrunk list>|all-smartrunks

Description

The smartrunk **show protocol-state** command shows information about the control protocol on a SmartTRUNK and the state of its ports.

Parameter	Value	Meaning
protocol-state	<smartrunk list>	The name of one or more SmartTRUNKs.
	all-smartrunks	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None.

Example

To show information about the control protocol for SmartTRUNK **st.1**:

rs# smartrunk show protocol-state st.1				
SmartTRUNK	Protocol	State	Port	Port State
-----	-----	-----	----	-----
st.1	HuntGroup	Up	et.1.1	Forwarding
			et.1.2	Forwarding
			et.1.3	Forwarding
			et.1.4	Forwarding

Table 68-4 Display Field Description

FIELD	DESCRIPTION
SmartTRUNK	The name of the SmartTRUNK(s)
Protocol	The control protocol used by the SmartTRUNK(s).
State	Current state of the SmartTRUNK(s).

Table 68-4 Display Field Description (Continued)

FIELD	DESCRIPTION
Port	A list of the ports that belong to the SmartTRUNK(s)
Port State	The state of the SmartTRUNK ports

smartrunk show trunks

Mode
Enable

Format

smartrunk show trunks <smartrunk list>|all-smartrunks

Description

The smartrunk **show trunks** command shows information about all SmartTRUNKs, including active and inactive ports, and the control protocol used.

Parameter	Value	Meaning
trunks	<smartrunk list>	The name of one or more SmartTRUNKs.
	all-smartrunks	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None.

Example

To display information about all SmartTRUNKs on the RS:

rs# smartrunk show trunks					
Flags: D - Disabled I - Inactive					
SmartTRUNK	Active Ports	Inactive Ports	Primary Port	Protocol	Policy Flags
-----	-----	-----	-----	-----	-----
st.1	et.1.(1-4)		et.1.1	None	RR
st.2	gi.4.(1-2)		gi.4.2	HuntGroup	LU
st.3	et.3.(1-4)		et.3.1	802.3ad	None

Table 68-5 Display Field Description

FIELD	DESCRIPTION
SmartTRUNK	The name of each SmartTRUNK on the RS.
Active Ports	Ports in SmartTRUNK that are active.

Table 68-5 Display Field Description (Continued)

FIELD	DESCRIPTION
Inactive ports	Ports in the SmartTRUNK that are inactive.
Primary Port	The port on the SmartTRUNK that has been elected for sending broadcast and multicast packets.
Protocol	The control protocol being used by the SmartTRUNK: None – No control protocol HuntGroup – DEC HuntGroup control protocol 802.3ad – LACP
Policy	The load policy being used by the SmartTRUNK: RR – Round Robin LU – Link Utilization
Flags	Shows the current state of the SmartTRUNK D – Disabled I – Inactive

69 SNMP COMMANDS

The SNMP commands let you set and show SNMP parameters including SNMP community names and IP host targets for SNMP traps.

69.1 COMMAND SUMMARY

The following table lists the snmp commands. The sections following the table describe the command syntax.

snmp disable trap authentication link-up-down
snmp disable port-trap <port list>
snmp set chassis-id <chassis-name>
snmp set community <community-name> privilege read read-write
snmp set mib name <mib-name> status enable disable
snmp set retro-mib-ifspeed
snmp set target <IP-addr> community <community-name> [owner <name>] [port <number>] [status enable disable]
snmp set trap-source <interface-name> <ipaddr>
snmp show access all chassis-id community statistics trap mibs tftp
snmp stop
snmp test trap type ps-failure ps-recover vrrpNewMaster

snmp disable trap

Mode

Configure

Format

```
snmp disable trap authentication|link-up-down
```

Description

The **snmp disable trap** command controls the types of traps the RS emits. You can disable the following trap types:

- Authentication – use the `authentication` keyword to prevent the RS from sending a trap each time it receives an invalid community string or invalid Telnet password.
- Link-state change – use the `link-up-down` keyword to prevent the RS from sending a trap each time a port changes operational state.

Parameter	Value	Meaning
trap	authentication	Disables authentication traps, which the RS sends when it receives an invalid SNMP community string or Telnet password.
	link-up-down	Disables link-state change traps, which the RS sends when a port's operational state changes.

Restrictions

None.

snmp disable port-trap

Mode

Configure

Format

snmp disable port-trap *<port list>*

Description

The **snmp disable port-trap** command controls the traps the RS emits on specific ports.

Parameter	Value	Meaning
port-trap	<i><port list></i>	Specifies the port(s) on which you wish to disable traps.

Restrictions

None.

snmp set chassis-id

Mode

Configure

Format

```
snmp set chassis-id <chassis-name>
```

Description

The **snmp set chassis-id** command lets you set a string to give the RS an SNMP identity.

Parameter	Value	Meaning
chassis-id	<chassis-name>	Is a string describing the RS.

Restrictions

None.

snmp set community

Mode

Configure

Format

```
snmp set community <community-name> privilege read|read-write
```

Description

The **snmp set community** command sets a community string for SNMP access to the RS. SNMP management stations that want to access the RS must supply a community string that is set on the switch. This command also sets the level of access to the RS to read-only or read-write. Communities that are read-only allow SNMP GETs but not SNMP SETs. Communities that have read-write access allow both SNMP GETs and SNMP SETs.

Parameter	Value	Meaning
community	<community-name>	Character string for the community string.
privilege		Specifies the access level.
	read	Allows SNMP GETs but not SNMP SETs.
	read-write	Allows SNMP GETs and not SNMP SETs.

Restrictions

None.

Example

To set the SNMP community string to “public,” which has read-only access:

```
rs(config)# snmp set community public privilege read
```

snmp set mib

Mode

Configure

Format

```
snmp set mib name <mib-name> status enable| disable
```

Description

The **snmp set mib** command allows you to enable or disable a particular MIB module in the SNMP agent.

Parameter	Value	Meaning
mib name	<mib-name>	Character string for the MIB module you wish to enable or disable. The MIB modules listed are supported by the SNMP agent.
	ATM-MIB	Transmission statistics for ATM
	BGP4-MIB	Border Gateway Protocol Version 4 MIB
	BRIDGE-MIB	Transparent layer 2 bridging protocol MIB
	CAPACITY-MIB	Device capacity usage statistics
	CISCO-BGP-ACCOUNTING_MIB	BGP accounting MIB
	CONFIG-MIB	Configuration control MIB
	DS0-MIB	Transmission statistics for DS0 serial line protocol
	DS0BUNDLE-MIB	Transmission statistics for DS0BUNDLE serial line protocol
	DS1-MIB	Transmission statistics for DS1 serial line protocol
	DS3-MIB	Transmission statistics for DS3 serial line protocol
	DVMRP-MIB	Distance Vector Multicast Routing Protocol
	EtherLike-MIB	IEEE 802.3 detailed ethernet statistics
	FRAME-RELAY-DTE-MIB	Frame Relay mib
	HARDWARE-MIB	Chassis, environmental and inventory statistics
	IF-MIB	Interfaces group: ifTable, ifXTable, ifStackTable
	IGMP-MIB	Internet Group Membership Protocol MIB, Multicast
	IP-MIB	IP group containing global IP statistics
	IP-FORWARD-MIB	IP CIDR Route Table
	LFAP-MIB	Lightweight Flow Accounting Protocol statistics

Parameter	Value	Meaning
	MAU-MIB	IEEE 802.3 ethernet hardware control
	NOVELL-IPX-MIB	Novell IPX MIB
	NOVELL-RIPSAP-MB	Novell RIPSAP MIB
	OSPF-MIB	OSPF Version 2 mib
	POLICY-MIB	Policy Configuration MIB
	PPP-BRIDGE-NCP-MIB	Point to Point Bridge Control Protocol
	PPP-IP-NCP-MIB	Point to Point IP Network Control Protocol
	PPP-LCP-MIB	Point to Point Link Control Protocol mib
	PPP-SEC-MIB	Point to Point Security mib
	RADIUS-AUTH-CLIENT-MIB	Radius client protocol statistics
	RIPv2-MIB	RIP Version 2 mib
	RMON-MIB	Remote Monitoring for Layer 2 traffic
	RMON2-MIB	Remote Monitoring for Layer 3/4 traffic
	RSTONE-ATML2FDBEXT-	Riverstone MAC to VC MIB for ATM interfaces
	SERVICE-STATUS-MIB	Operational protocol statistics
	SNMPv2-MIB	System and snmp group objects
	SONET-MIB	Transmission statistics for SONET
	TCP-MIB	TCP Statistics group
	UDP-MIB	UDP statistics group
	VRRP-MIB	Virtual Router Redundancy Protocol
status		Specifies whether to enable or disable the MIB module:
	enable	Enables the MIB module
	disable	Disables the MIB module

Restrictions

None.

Example

To enable the RMON2-MIB in the SNMP agent:

```
rs(config)# snmp set mib rmon2-mib status enable
```

snmp set retro-mib-ifspeed

Mode

Configure

Format

```
snmp set retro-mib-ifspeed
```

Description

The **snmp set retro-mib-ifspeed** command sets the ifSpeed for IP interface rows. The speed of the first operational port is returned.

Restrictions

None.

snmp set target

Mode

Configure

Format

```
snmp set target <IP-addr> community <community-name> [owner <name>] [port <number>]  
[status enable|disable]
```

Description

The **snmp set target** command specifies the IP address of the target server to which you want the RS to send SNMP traps. Trap targets are enabled by default but you can use the status argument to disable or re-enable a target.



Note In general, community strings sent with traps should not have read-write privileges.

Parameter	Value	Meaning
target	<IP-addr>	Is the IP address of the management station from which you want to be able to access the traps. The target IP address should be locally attached to the RS. Cold start traps might not reach their destination if the target requires dynamic route table entries to be forwarded correctly. The RS will retry every minute up to four minutes on the cold-start trap.
community	<community-name>	Is the name of the SNMP community for which you are setting the trap target.
owner	<name>	Is the administrative owner for this trap destination. The default is monitor.
port	<number>	Is the UDP port to send the trap. Specify a value between 0-65535. The default is UDP port 162.
status	enable	Re-enables the target.
	disable	Disables the target.

Restrictions

None.

snmp set trap-source

Mode

Configure

Format

```
snmp set trap-source <interface-name>|<ipaddr>
```

Description

The **snmp set trap-source** command sets the interface from which traps are reported. Specify either an interface name or an IP address.

Parameter	Value	Meaning
trap-source	<interface-name>	Name of the interface from which traps are reported.
	<ipaddr>	IP address from which traps are reported.

Restrictions

None.

snmp show

Mode

Enable

Format

snmp show access|all|chassis-id|community|statistics|trap|mibs|tftp

Description

The **snmp show** command shows the following SNMP information:

- Community strings set on the RS
- SNMP Statistics
- IP address of SNMP trap target server

Parameter	Value	Meaning
access		Displays the last five SNMP clients to access the RS.
all		Displays all SNMP information (equivalent to specifying all the other keywords)
chassis-id		Displays the RS' SNMP name.
community		Displays the RS' community string.
statistics		Displays SNMP statistics.
trap		Displays the IP address of the trap target server.
mibs		Displays the SNMP MIB registry.
tftp		Displays SNMP TFTP status.

Restrictions

None.

Examples

The following command displays a log of SNMP access to the RS. The host that accessed the RS and the RS system time when the access occurred are listed.

```
rs(config)# snmp show access
SNMP Last 5 Clients:
10.15.1.2 Wed Feb 10 18:42:59 1999
10.15.1.2 Wed Feb 10 18:42:55 1999
10.15.1.2 Wed Feb 10 18:42:56 1999
10.15.1.2 Wed Feb 10 18:42:57 1999
10.15.1.2 Wed Feb 10 18:42:58 1999
```

To display the SNMP identity of the RS:

```
rs(config)# snmp show chassis-id

SNMP Chassis Identity:
s/n 123456
```

To display the IP address of the trap target server:

```
rs(config)# snmp show trap

Trap Table:
IndexTrapTargetAddrCommunity StringStatus
1.10.15.1.2publicenabled
2.1.2.3.4public123disabled
3.5.6.7.8public20disabled
```

snmp stop

Mode

Configure

Format

```
snmp stop
```

Description

The **snmp stop** command stops SNMP access to the RS. The RS will still finish all active requests but will then disregard future requests. When you issue this command, UDP port 161 is closed.

Restrictions

None.

snmp test trap

Mode

Enable

Format

```
snmp test trap type ps-failure| ps-recover| vrrpNewMaster
```

Description

The **snmp test trap** command allows you to test the SNMPv1 notifications to the managers currently configured. You can test the following notification types:

- PS-failure
- PS-recover

Parameter	Value	Meaning
ps-failure		Tests the power supply failure trap notification.
ps-recover		Tests the power supply recover trap notification.
vrrpNewMaster		Tests the Virtual Router Redundancy New Master Trap.

Restrictions

None.

70 SONET COMMANDS

The **sonet** commands allows you to configure and display various parameters for Synchronous Optical Network (SONET) encapsulation. These commands allows you to accommodate Packet-over-SONET (POS) and ATM (asynchronous transfer mode) transmission using the RS.

Packet-over-SONET technology provides the ability to transmit IP packets and ATM cells over a SONET backbone by encapsulating them into a SONET frame. In reference to the OSI Layer model, the SONET layer rests right beneath the IP layer or the ATM layer. Based on the transmission mechanism of SONET frames, the result is larger traffic bandwidth and faster line speed (OC-3), accommodating QoS guarantees as well as the ability to deliver voice/video data over an internet network.

SONET frames carry a large amount of data stored as overhead. This overhead information provide the information for OAM&P (operation, administration, management, and provisioning) capabilities, such as performance monitoring, automatic protection switching, and path tracing.

Riverstone SONET technology features Automatic Protection Switching, performance monitoring capabilities, as well as commercial circuit identification.

70.1 COMMAND SUMMARY

The following table lists the **sonet** commands. The sections following the table describe the command syntax.

sonet set <ports> C2 <num>
sonet set <ports> circuit-id <string>
sonet set <ports> fcs-16-bit
sonet set <ports> framing sonet sdh
sonet set <ports> J0 <num>
sonet set <ports> loopback none line-facility serial-terminal parallel
sonet set <ports> path-trace <string>
sonet set <ports> payload-scramble on off
sonet set <ports> protected-by <port>
sonet set <ports> protection 1+1
sonet set <ports> protection-switch lockoutprot forced manual
sonet set <ports> revertive on off
sonet set <ports> S1S0 <num>

sonet set *<ports>* **sd-ber** *<num>*

sonet set *<ports>* **sf-ber** *<num>*

sonet set *<ports>* **WTR-timer** *<num>*

sonet show alarms *<port-list>*

sonet show aps *<ports>*

sonet show loopback *<ports>*

sonet show medium *<ports>*

sonet show pathtrace *<ports>*

sonet set C2

Mode

Configure

Format

```
sonet set <ports> C2 <num>
```

Description

The **sonet set C2** command allows you to specify a value for the C2 flag. SONET frames carry overhead for path, section and line for easier multiplexing and better OAM&P (operation, administration, management, and provisioning) capabilities.

The SONET frame overhead information is stored in separate bytes, or flags.

There are nine bytes allocated for section overhead labeled A1, A2, B1, D1, D2, D3, E1, F1, J0/Z0.

There are 18 bytes allocated for line overhead labeled H1, H2, H3, B2, K1, K2, D4, D5, D6, D7, D8, D9, D10, D11, D12, S1/Z1, M0/M1, and E2.

There are nine bytes allocated for path overhead labeled J1, B3, C2, H4, G1, P2, Z3, Z4, and Z5.

The **sonet set C2** command set the C2 flag. The C2 flag is the path signal label byte used to indicate the contents of the synchronous payload envelope.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port.
C2	<num>	Specifies the value of the C2 flag. Specify any number between 0 and 255.

Restrictions

None.

Example

To set the C2 flag to 16 on port so.2.1:

```
rs(config)# sonet set so.2.1 C2 16
```

sonet set circuit-id

Mode

Configure

Format

```
sonet set <ports> circuit-id <string>
```

Description

The **sonet set circuit-id** command allows you to set a circuit identifier on a specified port. This command is for administrative purposes, used to identify this line and associate it with a certain customer circuit. Primarily used for service level management.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
circuit-id	<string>	Specifies the circuit identifier. The maximum length must be 64 bytes or less.

Restrictions

None.

Example

To identify the circuit line on port so.2.1 to as 'customer1':

```
rs(config)# sonet set so.2.1 circuit-id customer1
```

sonet set fcs-16-bit

Mode

Configure

Format

sonet set *<ports>* **fcs-16-bit**

Description

The **sonet set fcs-16-bit** command allows you to set the frame check sequence (FCS) field length of the SONET frame to 16 bits. By default, this field length is set to 32 bits (4 octets). Using this command, you can set the frame check sequence field length to 16 bits (2 octets) instead.

The FCS field is used as an error check mechanism during frame transmission. An FCS value is calculated before transmission based on destination address, source address, and other data inside the frame. The FCS field inside the SONET frame carries this value. After the frame arrives to the destination, the FCS value is calculated again and compared with the value in the FCS field. This is done to ensure that there was no errors during transmission.

Parameter	Value	Meaning
set	<i><ports></i>	Specifies the port name(s). Specify a SONET port.

Restrictions

None.

Example

To set the frame check sequence on port so.2.1 to 16 bits:

```
rs(config)# sonet set so.2.1 fcs-16-bit
```

sonet set framing

Mode

Configure

Format

```
sonet set <ports> framing sonet| sdh
```

Description

The **sonet set framing** command allows you to specify the SONET frame type for mapping the data. The two options are SONET (Synchronous Optical Network) which is an ANSI standard, or SDH (Synchronous Digital Hierarchy) which is an ITU standard.

There are minor differences between the two standards. One such difference is that SONET has a basic transmission rate of OC-1 (51.84 Mbps), whereas SDH has a basic transmission rate of OC-3 (155.52 Mbps).

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
framing	sonet	Sets the optical framing standard to SONET.
	sdh	Sets the optical framing standard to SDH.

Restrictions

None.

Example

To set optical framing on port so.2.1 to SONET:

```
rs(config)# sonet set so.2.1 framing sonet
```

sonet set J0

Mode

Configure

Format

sonet set <ports> **J0** <num>

Description

The **sonet set J0** command allows you to specify a value for the J0 flag. SONET frames carry overhead for path, section and line for easier multiplexing and better OAM&P (operation, administration, management, and provisioning) capabilities.

The SONET frame overhead information is stored in separate bytes, or flags.

There are nine bytes allocated for section overhead labeled A1, A2, B1, D1, D2, D3, E1, F1, J0/Z0.

There are 18 bytes allocated for line overhead labeled H1, H2, H3, B2, K1, K2, D4, D5, D6, D7, D8, D9, D10, D11, D12, S1/Z1, M0/M1, and E2.

There are nine bytes allocated for path overhead labeled J1, B3, C2, H4, G1, P2, Z3, Z4, and Z5.

The **sonet set J0** command set the J0 flag. The J0 flag is the section trace byte.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port.
J0	<num>	Specifies the value of the J0 flag. Specify any number between 0 and 255.

Restrictions

None.

Example

To set the J0 flag to 16 on port so.2.1:

```
rs(config)# sonet set so.2.1 J0 16
```

sonet set loopback

Mode

Configure

Format

```
sonet set <ports> loopback none| line-facility| serial-terminal| parallel
```

Description

The **sonet set loopback** command allows you to exercise loopback functionality on a specified port . Loopback is used to verify connectivity between two devices.

Parameter	Value	Meaning
set	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.
loopback	none	Disables loopback functionality. Loopback is disabled by default.
	line-facility	Line or facility loopback connects high speed receive data to high speed transmit data.
	serial-terminal	Serial or terminal loopback connects high speed transmit to high speed receive data.
	parallel	Parallel loopback connects byte wide transmit to receive processor.

Restrictions

None.

Example

To connect high speed receive data to high speed transmit on port so.2.1:

```
rs(config)# sonet set so.2.1 loopback line-facility
```

sonet set path-trace

Mode

Configure

Format

sonet set *<ports>* **path-trace** *<string>*

Description

The **sonet set path-trace** command allows you to set a message in a buffer to be sent as a pathtrace message .

The path trace message is part of the path overhead of the transport overhead in every SONET frame. This path trace byte is a 64 byte (or less) message string that is used by the destination and source to notify each other that they are connected within a path.

Parameter	Value	Meaning
set	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.
path-trace	<i><string></i>	Specifies a character string. The maximum length must be 64 bytes or less.

Restrictions

None.

Example

To send the path trace message 'tracer' on port so.2.1:

```
rs(config)# sonet set so.2.1 path-trace tracer
```

sonet set payload-scramble

Mode

Configure

Format

```
sonet set <ports> payload-scramble on| off
```

Description

The **sonet set payload-scramble** command allows you to enable scrambling or descrambling of the payload encapsulated in the STS frame. Scrambling the STS payload is important in optimizing the transmission density of the data stream. Since all SONET transmission use the same source clock for timing, scrambling the payload using a random number generator converts the data stream to a more random sequence. This ensures optimal transmission density of the data stream.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
payload-scramble	on	Enables scrambling and descrambling of the STS payload.
	off	Disables scrambling and descrambling of the STS payload.

Restrictions

None.

Example

To enable scrambling on port so.2.1:

```
rs(config)# sonet set so.2.1 payload-scramble
```


sonet set protected-by

Mode

Configure

Format

sonet set *<ports>* **protected-by** *<port>*

Description

The **sonet set protecting** command allows you to specify a protecting port for Automatic Protection Switching (APS). APS is used to provide redundancy for transmission between two SONET devices. This ensures that if a link goes down, traffic can be automatically switched to a secondary backup link and the connection remains operational.

With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

This command is used in conjunction with the **sonet set protection** command.

Parameter	Value	Meaning
set	<i><ports></i>	Specifies the port name(s). Specify a SONET port.
protected-by	<i><port></i>	Specifies the APS protecting port. This must be a single port. Only valid for Packet-over-SONET ports.

Restrictions

None.

Example

To set so.1.1 as the APS protecting port for so.2.1:

```
rs(config)# sonet set so.2.1 protection 1+1 protected by so.1.1
```

sonet set protection

Mode

Configure

Format

```
sonet set <ports> protection 1+1
```

Description

The **sonet set protection 1+1** command allows you to configure a working port for Automatic Protection Switching (APS). This working port will be protected by the protecting port. APS is used to provide redundancy for transmission between two SONET devices. This ensures that if a link goes down, traffic can be automatically switched to a secondary backup link and the connection remains operational.

With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

This command is used in conjunction with the **sonet set protected-by** option.

Negate this command to disable APS on the port.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
protection	1+1	Specifies the 1+1 APS scheme, where one working port is matched with one protecting port.

Restrictions

None.

Example

To configure so.2.1 as an APS working port protected by so.1.1:

```
rs(config)# sonet set so.2.1 protection 1+1 protected-by so.1.1
```

sonet set protection-switch

Mode

Configure

Format

```
sonet set <ports> protection-switch lockoutprot| forced| manual
```

Description

The **sonet set protection-switch** command allows you to configure SONET Automatic Protection Switching (APS) on a port. With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

Use this command to configure the APS switching characteristics for a port.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
protection-switch	lockoutprot	Prevents APS switching from a working port to a protecting port in the case of signal failure or signal degrade. This command is configured only on the protecting port.
	forced	Allows protection switching to occur. Switches service from this port to the other port, even when there are errors on the other port.
	manual	Allows you to manually switch service from a port to the other APS port. This is provided that there are no errors on the protecting port. This command can be configured on either the working port or the protecting port.

Restrictions

None.

Example

To configure APS switching for the working port so.2.1:

```
rs(config)# sonet set so.2.1 protection-switch forced
```

sonet set revertive

Mode

Configure

Format

```
sonet set <ports> revertive on|off
```

Description

The **sonet set revertive** command allows you to select whether traffic will be switched back to the working port from the protecting port after the signal degrade or failure condition has been corrected. Once the condition has been corrected, APS waits for a specified time period (WTR-timer) before switching back to the working port.

With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
revertive	on	Allows traffic to switch back from the protecting port to the working port after the signal degrade or failure condition has been corrected and after the Wait-to-Restore timer has expired.
	off	Prevents automatic switch back to the working port from the protecting port after the signal degrade or failure condition has been corrected.

Restrictions

None.

Example

To set APS switching to revertive mode for the protecting port so.2.1:

```
rs(config)# sonet set so.2.1 revertive on
```

sonet set S1S0

Mode

Configure

Format

```
sonet set <ports> S1S0 <num>
```

Description

The **sonet set S1S0** command allows you to specify a value for the S1/S0 flag. SONET frames carry overhead for path, section and line for easier multiplexing and better OAM&P (operation, administration, management, and provisioning) capabilities.

The SONET frame overhead information is stored in separate bytes, or flags.

There are nine bytes allocated for section overhead labeled A1, A2, B1, D1, D2, D3, E1, F1, J0/Z0.

There are 18 bytes allocated for line overhead labeled H1, H2, H3, B2, K1, K2, D4, D5, D6, D7, D8, D9, D10, D11, D12, S1/Z1, M0/M1, and E2.

There are nine bytes allocated for path overhead labeled J1, B3, C2, H4, G1, P2, Z3, Z4, and Z5.

The **sonet set S1S0** command set the S1/S0 flag. The S1/S0 flag is the line synchronization status byte used to indicate synchronization state of the line terminating devices.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port.
S1S0	<num>	Specifies the value of the S1/S0 flag. Specify any number between 0 and 3.

Restrictions

None.

Example

To set the S1/S0 flag to 1 on port so.2.1:

```
rs(config)# sonet set so.2.1 S1S0 1
```

sonet set sd-ber

Mode

Configure

Format

sonet set *<ports>* **sd-ber** *<num>*

Description

The **sonet set sd-ber** command allows you to specify a signal degrade threshold level. There are two threshold levels based on the Bit Error Rate: signal degrade and signal failure. These two threshold levels act as a two stage alarm system, where the signal degrade threshold is always met first before the signal failure threshold.

Once the BER reaches the signal degrade threshold level, then a signal degrade alarm occurs and the receive is considered to be in signal degrade condition. Based upon the APS configuration, all traffic is switched from the working port to the protecting port.

Parameter	Value	Meaning
set	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.
sd-ber	<i><num></i>	Specifies the Bit Error Rate signal degrade threshold level in 10^{-n} . Specify any number for n between 5 to 9. The default is 6, indicating a threshold level of 10^{-6} . This means that a signal degrade alarm occurs if the Bit Error Rate rises past the 1/1000000 level.

Restrictions

None.

Example

To set the BER signal degrade threshold level to 10^{-6} or 1/1000000:

```
rs(config)# sonet set so.2.1 sd-ber 6
```

sonet set sf-ber

Mode

Configure

Format

```
sonet set <ports> sf-ber <num>
```

Description

The **sonet set sf-ber** command allows you to specify a signal failure threshold level. There are two threshold levels based on the Bit Error Rate: signal degrade and signal failure. These two threshold levels act as a two-stage alarm system, whereby the signal degrade threshold is always met first before the signal failure threshold.

Once the BER reaches the signal failure threshold level, then a signal failure alarm occurs and the receive is considered to be in signal failure condition. Based upon the APS configurations, all traffic is switched from the working port to the protecting port.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
sf-ber	<num>	Specifies the Bit Error Rate signal failure threshold level in 10^{-n} . Specify any number for n between 3 to 5. The default is 3, indicating a threshold level of 10^{-3} . This means that a signal failure alarm occurs if the Bit Error Rate rises past the 1/1000 level.

Restrictions

None.

Example

To set the BER signal failure threshold level to 10^{-3} or 1/1000:

```
rs(config)# sonet set so.2.1 sf-ber 3
```

sonet set WTR-timer

Mode

Configure

Format

```
sonet set <ports> WTR-timer <num>
```

Description

The **sonet set WTR-timer** command allows you to set the Wait-to-Restore timer. The WTR-timer specifies a time period that must expire before traffic is switched back to the working port from the protecting port. Once the signal degrade or failure condition has been corrected, APS waits until the WTR-timer expires before switching back to the working port.

Parameter	Value	Meaning
set	<ports>	Specifies the port name(s). Specify a SONET port or an ATM port.
WTR-timer	<num>	Specifies the WTR timer (in minutes). Specify any number between 5 and 12 minutes. The default is 5 minutes.

Restrictions

None.

Example

To set the WTR-timer to 6 minutes on port so.2.1:

```
rs(config)# sonet set so.2.1 WTR-timer 6
```


sonet show alarms

Mode

Enable

Format

sonet show alarms *<port-list>*

Description

The **sonet show alarms** command allows you to display all alarms and errors (such as a loss of signal or loss of frames) that occur on the specified SONET ports.

Parameter	Value	Meaning
alarms	<i><port-list></i>	Specifies the ports for which the alarms will be displayed. Specify an ATM port.

Restrictions

This command applies the ATM OC-12 module only.

Examples

Following is sample output generated by the **sonet show alarms** command:

```
rs# sonet show alarms
WORKING PORT
Section
  Alarms:
    BIP = 65535
Line
  Alarms:
    BIP = 258  FEBE = 105
Path
  Alarms:
    BIP = 65535  FEBE = 79
    Corrected HCS errors = 0  Uncorrected HCS errors = 0

PROTECTION PORT
Section
  Alarms:
    BIP = 65535
Line
  Alarms:
    BIP = 295  FEBE = 108
Path
  Alarms:
    BIP = 65535  FEBE = 80
    Corrected HCS errors = 0  Uncorrected HCS errors = 0
```

It displays information about the alarms that occurred in the working port and in the protection port. The alarms can be any of the following:

- LOS - loss of signal
- LOF - loss of frame
- OOF - out of frame
- RDI - remote defect indication
- AIS - alarm indication signal
- LOP - loss of pointer
- SLM - signal lable mismatch
- LCD - loss of cell delineation
- SDBER - signal degrade bit error rate
- SFBER - signal failure bit error rate

The errors can be any of the following:

- BIP - Bit Interleaved Parity
- FEBE - Far End Block Error
- HCS - Header Check Sequence

sonet show aps

Mode

Enable

Format

sonet show aps *<ports>*

Description

The **sonet show aps** command allows you to display APS (automatic protection switching) status. This command allows you to display such APS parameters as protection level, working or protecting port, directionality, and switch status.

Parameter	Value	Meaning
aps	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.

Restrictions

None.

Example

To display the APS status for port so.2.1:

```
rs# sonet show aps so.2.1
```

sonet show loopback

Mode

Enable

Format

sonet show loopback *<ports>*

Description

The **sonet show loopback** command allows you to display loopback status for a specified port. Loopback is used to verify connectivity between two devices.

Parameter	Value	Meaning
loopback	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.

Restrictions

None.

Example

To display the loopback status for port so.2.1:

```
rs# sonet show loopback so.2.1
```

sonet show medium

Mode

Enable

Format

sonet show medium *<ports>*

Description

The **sonet show medium** command allows you to display the various SONET optical line values associated with a port. This command will allow you to display values such as framing status, line type, and administrator-specified circuit identifier.

Parameter	Value	Meaning
medium	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.

Restrictions

None.

Example

To display optical line values for port so.2.1:

```
rs# sonet show medium so.2.1
```

sonet show pathtrace

Mode

Enable

Format

sonet show pathtrace *<ports>*

Description

The **sonet show pathtrace** command allows you to display path trace messages received on a specified port.

Parameter	Value	Meaning
pathtrace	<i><ports></i>	Specifies the port name(s). Specify a SONET port or an ATM port.

Restrictions

None.

Example

To display the path trace messages for port so.2.1:

```
rs# sonet show pathtrace so.2.1
```

71 SSH COMMANDS

The **ssh** commands allow you to configure the Secure Shell (SSH) server on the RS.

71.1 COMMAND SUMMARY

The following table lists the **ssh** commands. The sections following the table describe the command syntax.

<code>ssh server eliminate_key rsa</code>
<code>ssh server generate_key rsa</code>
<code>ssh server options listen-port <port></code>

ssh server eliminate_key

Mode

Enable

Format

```
ssh server eliminate_key rsa
```

Description

The **ssh server eliminate_key** command eliminates an SSH server host key which has previously been created with the **ssh server generate_key** command.

Parameter	Value	Meaning
eliminate_key	rsa	Eliminates an RSA host key.

Restrictions

None.

Examples

To eliminate the SSH server host key:

```
rs# ssh server eliminate_key rsa
```


ssh server generate_key

Mode

Enable

Format

```
ssh server generate_key rsa
```

Description

The **ssh server generate_key** command generates an SSH server host key. Use the **ssh server eliminate_key** command to eliminate the generated host key.

Parameter	Value	Meaning
generate_key	rsa	Generates an RSA host key.

Restrictions

None.

Examples

To generate an SSH server host key:

```
rs# ssh server generate_key rsa
Your identification has been saved in /int-flash/cfg/ssh/ssh_host_key.
Your public key has been saved in /int-flash/cfg/ssh/ssh_host_key.pub.
```

ssh server options

Mode

Configure

Format

ssh server options listen-port <port>

Description

The **ssh server options** command allows you to set the port on which the SSH server listens for connections.

Parameter	Value	Meaning
listen-port	<port>	The port on which the SSH server should listen for connections. Specify a value between 1-65535. The default value is 22.

Restrictions

None.

Examples

To set the SSH server listen port:

```
rs(config)# ssh server options listen-port 21
```

72 STATISTICS COMMANDS

The **statistics** commands let you display statistics for various RS features. You also can clear some statistics.

72.1 COMMAND SUMMARY

The following table lists the statistics commands. The sections following the table describe the command syntax.

<code>statistics clear <statistic-type> <port-list></code>
<code>statistics show arp <string> all</code>
<code>statistics show framer <port-list></code>
<code>statistics show icmp</code>
<code>statistics show ip</code>
<code>statistics show ip-interface <string> all [packets] [bytes] [errors] [input] [output] verbose</code>
<code>statistics show ip-routing</code>
<code>statistics show ipx</code>
<code>statistics show ipx-interface <string> all packets bytes errors input output verbose</code>
<code>statistics show ipx-routing</code>
<code>statistics show multicast</code>
<code>statistics show phy-errors <port list> all-ports [interval <seconds>]</code>
<code>statistics show port-errors <port/SmartTRUNK-list> all-ports</code>
<code>statistics show port-packets <port-list> all-ports</code>
<code>statistics show port-stats <port/SmartTRUNK-list> all-ports</code>
<code>statistics show rarp <string> all</code>
<code>statistics show summary-stats</code>
<code>statistics show tcp</code>
<code>statistics show udp</code>
<code>statistics show top</code>

statistics clear

Mode
Enable

Format

```
statistics clear <statistic-type> <port-list>
```

Description

The **statistics clear** command clears port statistics, error statistics, IP, IPX, or ICMP statistics. When you clear statistics, the RS sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

Parameter	Value	Meaning
clear	<statistic-type>	Type of statistics you want to clear.
	phy-errors	Clears potential physical error statistics for the specified port. ^a
	port-errors	Clears all error statistics for the specified port.
	port-packets	Clears all packet statistics for the specified port.
	port-stats	Clears all normal (non-error) statistics for the specified port.
	ip	Clears all IP statistics for the specified port.
	ipx	Clears all IPX statistics for the specified port.
	icmp	Clears ICMP statistics for the specified port.
	all	
	input	
	output	
	disabled	
	<port-list>	The ports for which you are clearing statistics. You can specify a single port or a comma-separated list of ports. Specify all-ports to clear statistics for all RS ports.

a. You cannot use this command to clear physical layer errors for WAN ports or ports on the following line cards: POS OC-12, ATM OC-12, serial line cards, CMTS line cards.

Restrictions

None.

statistics show arp

Mode

Enable

Format

```
statistics show arp <string> |all
```

Description

Displays address resolution protocol (ARP) statistics.

Parameter	Value	Meaning
arp	<string>	Specifies the name of an interface.
	all	Specify all to display ARP statistics for all interfaces.

Restrictions

None.

Example

To display ARP statistics on interface 'en0':

```
rs# statistics show arp en0

Interface en0:
  1 requests sent
 19 replies sent
  0 proxy replies sent
Last 5 Requests Sent
----- no arp requests sent -----
Last 5 Replies Sent
134.141.179.129 | Yago      16:BF:21      |2000-04-17 13:12:49
134.141.179.129 | Yago      16:BF:21      |2000-04-17 13:50:15
134.141.179.129 | Yago      16:BF:21      |2000-04-17 15:32:32
134.141.179.129 | Yago      16:BF:21      |2000-04-17 16:17:19
134.141.179.129 | Yago      16:BF:21      |2000-04-17 11:12:44

Last 5 ARP packets received on wrong interface
----- no arp packets received on wrong interface -----
```

The following describes the output:

requests sent	Displays how many ARP requests have been sent out to an ARP server for address resolution.
replies sent	Displays how many ARP replies have been sent out to an ARP client in response to request packets.
proxy replies sent	Displays how many proxy ARP replies have been sent out in response to request packets. A proxy router serving as a gateway to a subnet would respond with a proxy reply.
Last 5 Requests sent	Displays the last five ARP requests sent, including the following information: target MAC address, date and time sent.
Last 5 Replies sent	Displays the last five ARP replies sent, including the following information: target IP address, date and time sent.
Last 5 ARP packets received on wrong interface	Displays the last five ARP packets that has been received on the wrong interface.

statistics show framer

Mode

Enable

Format

statistics show framer *<port list>*

Description

Displays framer statistics.

Parameter	Value	Meaning
framer	<i><port list></i>	Specifies the port or group of ports.

Restrictions

None.

statistics show icmp

Mode
Enable

Format

statistics show icmp

Description

Displays internet control message protocol (ICMP) statistics.

Restrictions

None.

Example

To display ICMP statistics:

```
rs# statistics show icmp
icmp:
    0 messages with bad code fields
    0 messages smaller than minimum length
    0 bad checksums
    0 messages with bad length
    0 message responses generated
```

The following describes the output:

messages with bad code fields	Displays the number of ICMP messages processed by the router with a bad code field. The code field within the ICMP header uses a number to specify the message content of the ICMP message. An invalid number within the code field would show in this statistic parameter.
messages smaller than min length	Displays the number of ICMP messages processed by the router that didn't meet a minimum length requirement.
bad checksums	Displays the number of ICMP messages processed by the router with bad checksums. The checksum field within the ICMP header is used to verify that the message was transmitted error-free. A bad checksum indicates an ICMP message with errors.
messages with bad length	Displays the number of ICMP messages processed by the router with bad or invalid length.
message responses generated	Displays the number of ICMP responses that have been generated by the router in response to ICMP messages.

statistics show ip

Mode

Enable

Format

statistics show ip

Description

Displays internet protocol (IP) statistics.

Restrictions

None.

Example

To display IP statistics:

```
rs# statistics show ip
ip:
    78564 total packets received
    0 bad header checksums
    0 packets with size smaller than minimum
    0 packets with data size < data length
    0 packets with header length < data size
    0 packets with data length < header length
    0 packets with bad options
    0 packets with incorrect version number
    0 fragments received
    0 fragments dropped (dup or out of space)
    0 fragments dropped after timeout
    0 packets reassembled ok
    2984 packets for this host
    0 packets for unknown/unsupported protocol
    0 packets forwarded
    75580 packets not forwardable
    0 redirects sent
    2120 packets sent from this host
    0 packets sent with fabricated ip header
    0 output packets dropped due to no bufs, etc.
    0 output packets discarded due to no route
    0 output datagrams fragmented
    0 fragments created
    0 datagrams that can't be fragmented
```

The following describes the output:

total packets received	Displays the total number of IP packets received by the router, including all forwarded and dropped packets.
bad header checksums	Displays the number of IP packets received by the router with bad checksums. The checksum field within the IP header is used to verify that the packet was transmitted error-free. A bad checksum indicates an IP packet with errors.
packets w/size smaller than min	Displays the number of IP packets received by the router that didn't meet a minimum length requirement.
packets w/data size<data length	Displays the number of IP packets received by the router containing a data size smaller than the specified data length. The data length field in the IP header specifies the data length contained within the packet.
packets w/header length<data size	Displays the number of IP packets received by the router containing a IP header length smaller than the data size within the packet.
packets w/data length<header length	Displays the number of IP packets received by the router containing a data length smaller than the IP header length.
packets w/incorrect version number	Displays the number of IP packets received by the router with an incorrect IP version number. The IP version number field in the IP header is used to specify whether the packet is formatted for IPv4 or IPv6.
fragments received	Displays the number of datagram fragments received by the router. A datagram that does not fit into an IP packet must be fragmented into two or more packets.
fragments dropped	Displays the number of datagram fragments dropped by the router. A datagram that does not fit into an IP packet must be fragmented into two or more packets.
fragments dropped after timeout	Displays the number of datagram fragments dropped by the router after a certain time period. A datagram that does not fit into an IP packet must be fragmented into two or more packets.
packets reassembled ok	Displays the number of IP packets containing fragmented datagrams that were reassembled successfully at the destination.
packets for this host	Displays the total number of IP packets received that were intended for the router as the destination.
packets for unknown protocol	Displays the number of IP packets received by the router that is of an unknown or unsupported routed protocol.
packets forwarded	Displays the number of IP packets received by the router that were forwarded onto another host.
packets not forwardable	Displays the total number of IP packets received by the router that could not be forwarded onto another host.
redirects sent	Displays the number of redirects sent by the router.
packets sent from this host	Displays the total number of IP packets sent out by the router.

packets sent w/fabricated ip header	Displays the total number of IP packets sent out by the router after attaching an IP header onto the packet.
output packets dropped due to no bufs	Displays the total number of IP packets dropped before being sent out by the router because of lack of output buffer space.
output packets discarded due to no route	Displays the total number of IP packets dropped before being sent out by the router because of no IP routing information.
output datagrams fragmented	Displays the total number of datagrams that were fragmented into two or more IP packets before being sent out by the router.
fragments created	Displays the total number of datagram fragments created.
datagrams that can't be fragmented	Displays the total number of datagrams that was not successfully fragmented into two or more IP packets.

statistics show ip-interface

Mode
Enable

Format

statistics show ip-interface <string>|all [packets] [bytes] [errors] [input]
[output]|verbose

Description

Displays IP interface statistics.

Parameter	Value	Meaning
ip-interface	<string>	Specifies the name of an interface.
	all	Specify all to display IP statistics for all interfaces.
packets		Specify this optional parameter to display the number of packets that have passed through the interface.
bytes		Specify this optional parameter to display the number of bytes that have passed through the interface.
errors		Specify this optional parameter to display the number of packets with errors detected through the interface.
input		Specify this optional parameter to display interface statistics for the input side.
output		Specify this optional parameter to display interface statistics for the output side.
verbose		Specify this optional parameter to display statistics on the number of packets, bytes, and errors on both the input and output sides of the interface.

Restrictions

None.

Example

To display interface statistics on interface ‘en0’:

```
rs# statistics show ip-interface en0 verbose

Name In-frames Out-frames In-bytes Out-bytes In-errors Out-errors
en0 0 0 0 0 0 0
```

The following describes the output:

In-frames	Displays the number of packets that have entered the interface.
Out-frames	Displays the number of packets that have exited the interface.
In-bytes	Displays the number of bytes that have entered the interface.
Out-bytes	Displays the number of bytes that have exited the interface.
In-errors	Displays the number of packets with errors detected entering the interface.
Out-errors	Displays the number of packets with errors detected exiting the interface.

statistics show ip-routing

Mode
Enable

Format

statistics show ip-routing

Description

Displays unicast IP routing statistics.

Restrictions

None.

Example

To display routing statistics:

```
rs# statistics show ip-routing
routing:
    0 bad routing redirects
    0 dynamically created routes
    0 new gateways due to redirects
    1141 destinations found unreachable
    0 uses of a wildcard route
```

The following describes the output:

bad routing redirects	Displays the number of bad redirects have occurred. A redirect occurs in the case where the destination interface is the same as the source interface.
dynamically created routes	Displays the number of IP routes have been created using a routing protocol, as opposed to static routes which are user-defined.
new gateways due to redirects	Displays the number of new gateways have been added into the routing table due to redirects.
destinations found unreachable	Displays the number of destination addresses that have been found to be unreachable in the routing table. A destination may be unreachable due to the route being expired or being unavailable due to network changes.
uses of a wildcard route	Displays the number of times that a wildcard route has been used to forward a packet onto the next-hop destination.

statistics show ipx

Mode

Enable

Format

```
statistics show ipx
```

Description

Displays internetwork packet exchange (IPX) statistics.

Restrictions

None.

Example

To display IPX statistics:

```
rs# statistics show ipx
ipx:
    0 total packets received
    0 packets with bad checksums
    0 packets smaller than advertised
    0 packets smaller than a header
    0 packets forwarded
    0 packets not forwardable
    0 packets for this host
    0 packets sent from this host
    0 packets dropped due to no bufs, etc.
    0 packets discarded due to no route
    0 packets too big
    0 packets with too many hops
    0 packets of type 20
    0 packets discarded due to infiltering
    0 packets discarded due to outfiltering
    0 packets with misc protocol errors
    0 rip packets discarded due to socket buffer full
    0 sap packets discarded due to socket buffer full
    0 rip req packets discarded due to socket buffer full
    0 sap gns packets discarded due to socket buffer full
    0 packets discarded due to port of entry zero
    0 packets discarded due to sourced by us
```

The following describes the output:

total packets received	Displays the total number of IPX packets received by the router, including all forwarded and dropped packets.
bad header checksums	Displays the number of IPX packets received by the router with bad checksums. The checksum field within the IPX header is used to verify that the packet was transmitted error-free. A bad checksum indicates an IPX packet with errors.
packets smaller than advertised	Displays the number of IPX packets received by the router that are smaller than what the header indicates as the size.
packets smaller than a header	Displays the number of IPX packets received by the router that are smaller than the IPX header.
packets forwarded	Displays the number of IPX packets received by the router that have been forwarded onto the next-hop destination.
packets not forwardable	Displays the total number of IPX packets received by the router that could not be forwarded onto another host.
packets for this host	Displays the total number of IPX packets received that were intended for the router as the destination.
packets sent from this host	Displays the total number of IPX packets sent out by the router.
packets dropped due to no bufs	Displays the total number of IPX packets dropped before being sent out by the router because of lack of buffer space.
packets discarded due to no route	Displays the total number of IPX packets dropped before being sent out by the router because of no IPX routing information.
packets too big	Displays the total number of IPX packets that exceed a size threshold.
packets with too many hops	Displays the total number of IPX packets that exceed a number of hops threshold.
packets of type 20	Displays the total number of NetBIOS packets.
packets discarded due to infiltering	Displays the total number of incoming IPX packets that have been discarded due to filtering. Filtering is based upon various access control lists (ACL) such as IPX ACL, SAP ACL, and RIP ACL.
packets discarded due to outfiltering	Displays the total number of outgoing IPX packets that have been discarded due to filtering. Filtering is based upon various access control lists (ACL) such as IPX ACL, SAP ACL, and RIP ACL.
packets with misc protocol errors	Displays the total number of IPX packets containing routing protocol errors.
rip packets discarded	Displays the total number of Routing Information Protocol (RIP) packets that have been discarded due to the socket buffer being full.
sap packets discarded	Displays the total number of Server Advertisement Protocol (SAP) packets that have been discarded due to the socket buffer being full.

rip req packets discarded	Displays the total number of Routing Information Protocol (RIP) request packets that have been discarded due to the socket buffer being full.
sap gns packets discarded	Displays the total number of Service Advertisement Protocol (SAP) Get Nearest Server (GNS) packets that have been discarded due to the socket buffer being full.

statistics show ipx-interface

Mode

Enable

Format

```
statistics show ipx-interface <string>|all [packets] [bytes] [errors] [input]  
[output]|verbose
```

Description

Displays IPX interface statistics.

Parameter	Value	Meaning
ipx-interface	<string>	Specifies the name of an interface.
	all	Specify all to display IPX statistics for all interfaces.
packets		Specify this optional parameter to display the number of packets that have passed through the interface.
bytes		Specify this optional parameter to display the number of bytes that have passed through the interface.
errors		Specify this optional parameter to display the number of packets with errors detected through the interface.
input		Specify this optional parameter to display interface statistics for the input side.
output		Specify this optional parameter to display interface statistics for the output side.
verbose		Specify this optional parameter to display statistics on the number of packets, bytes, and errors on both the input and output sides of the interface.

Restrictions

None.

Example

To display interface statistics on interface 'en0':

```
rs# statistics show ipx-interface en0 verbose  
  
Name In-frames Out-frames In-bytes Out-bytes In-errors Out-errors  
en0 0 0 0 0 0 0
```

The following describes the output:

In-frames	Displays the number of packets that have entered the interface.
Out-frames	Displays the number of packets that have exited the interface.
In-bytes	Displays the number of bytes that have entered the interface.
Out-bytes	Displays the number of bytes that have exited the interface.
In-errors	Displays the number of packets with errors detected entering the interface.
Out-errors	Displays the number of packets with errors detected exiting the interface.

statistics show ipx-routing

Mode
Enable

Format

statistics show ipx-routing

Description

Display IPX routing statistics.

Restrictions

None.

Example

To display routing statistics:

```
rs# statistics show ipx-routing
routing:
    0 bad routing redirects
    0 dynamically created routes
    0 new gateways due to redirects
    1141 destinations found unreachable
    0 uses of a wildcard route
```

The following describes the output:

bad routing redirects	Displays the number of bad redirects have occurred. A redirect occurs in the case where the destination interface is the same as the source interface.
dynamically created routes	Displays the number of IPX routes have been created using a routing protocol, as opposed to static routes which are user-defined.
new gateways due to redirects	Displays the number of new gateways have been added into the routing table due to redirects.
destinations found unreachable	Displays the number of destination addresses that have been found to be unreachable in the routing table. A destination may be unreachable due to the route being expired or being unavailable due to network changes.
uses of a wildcard route	Displays the number of times that a wildcard route has been used to forward a packet onto the next-hop destination.

statistics show multicast

Mode

Enable

Format

```
statistics show multicast
```

Description

Displays multicast statistics.

Restrictions

None.

Example

To display multicast statistics:

```
rs# statistics show multicast
multicast forwarding:
    0 multicast forwarding cache lookups
    0 multicast forwarding cache misses
    0 upcalls to mrouterd
    0 upcall queue overflows
    0 upcalls dropped due to full socket buffer
    0 cache cleanups
    0 datagrams with no route for origin
    0 datagrams arrived with bad tunneling
    0 datagrams could not be tunneled
    0 datagrams arrived on wrong interface
    0 datagrams selectively dropped
    0 datagrams dropped due to queue overflow
    0 datagrams dropped for being too large
```

statistics show phy-errors

Mode

Enable

Format

```
statistics show phy-errors <port list>|all-ports [interval <seconds>]
```

Description

The **statistics show phy-errors** command measures and displays potential physical layer errors. You can use this command to relate a performance issue on a network segment with a possible physical problem on that segment.

Parameter	Value	Meaning
phy-errors	<port list>	Specifies the ports for which you want potential physical layer errors shown.
	all-ports	Specify all-ports to display physical layer errors for all ports.
interval	<seconds>	Specifies the interval, in seconds, for measurement of errors. Specify a value between 1-10. Default is 1 second.

This command returns the same information as the **port show phy-errors** command.

Restrictions

You *cannot* use this command to show physical layer errors for WAN ports or ports on the following line cards:

- POS OC-12
- ATM OC-12
- Serial line cards
- CMTS line cards

This command provides a reasonable estimate of potential degradation problems with the physical medium and is not intended to be a substitute for bit error rate testing of the physical line.

Example

To display potential physical layer errors for the port 'et.2.1':

```
rs# statistics show phy-errors et.2.1

Port: et.2.1
-----
Physical Error Stats
-----
RX frames Okay                100
Correlated Layer 1 Errors     10
Average bytes per frame       64
Errors gathered since 2000-11-01 11:22:4
Error stats cleared 2000-11-01 11:12:4
```

The display shows:

- The number of frames successfully received.
- The number of “suspected” physical layer errors.
- The average number of bytes per frame.
- The time when error statistics measurement and collection began and the time when the statistics were last cleared with the **statistics clear phy-errors** command.

statistics show port-errors

Mode

Enable

Format

```
statistics show port-errors <port/SmartTRUNK-list>|all-ports
```

Description

Display port error statistics.

Parameter	Value	Meaning
port-errors	<port/SmartTRUNK-list>	Specifies the port.
	all-ports	Specify all-ports to display port error statistics for all physical and logical ports.

Restrictions

None.

Example

To display port error statistics on port et.2.1:

```
rs# statistics show port-errors et.2.1

Port: et.2.1
----
Error Stats                                Error Stats
-----                                -----
CRC errors                                0      Carrier sense errors            0
Single collision (tx OK)                  0      Many collisions (tx OK)        0
Many collisions (drop)                    0      Late collisions                  0
Long frames >1518 bytes                   0      Invalid long frames             0
Short frames <64 bytes                    0      Alignment errors                0
Deferred transmissions                    0      Transmit underruns              0
IP - bad version                          0      IP - bad checksum                0
IP - bad header                           0      IP - small datagram             0
IP - expand TTL ring                      0      IPX - bad header                 0
Non-IP/IPX protocol                      0      Invalid MAC encap.              0
Internal frame tx error                   0      Internal frame rx error          0
Input buffer overflow                     0      Packet request overflow          0
Out buffer (low) ovflow                    0      Out buffer (med) ovflow          0
Out buffer (high) ovflow                  0      Out buffer (ctrl) ovflow         0
Input VLAN drop frame                     0
Error stats cleared * Never Cleared *
```

statistics show port-packets

Mode

Enable

Format

statistics show port-packets *<port-list>* | all-ports

Description

Displays port packet statistics.

Parameter	Value	Meaning
port-packets	<i><port-list></i>	Specifies the port.
	all-ports	Specify all-ports to display port packet statistics for all physical and logical ports.

Restrictions

None.

Example

To display port packet statistics on port et.2.1:

```
rs# statistics show port-packets et.2.1

Port: et.2.1
----
RMON Stats                Received                Transmitted
-----
Unicast frames            0                    0
Multicast frames          0                    0
Broadcast frames          0                    0
64 byte frames            0                    0
65-127 byte frames        0                    0
128-255 byte frames        0                    0
256-511 byte frames        0                    0
512-1023 byte frames        0                    0
1024-1518 byte frames      0                    0
RMON stats cleared      * Never Cleared *
```

statistics show port-stats

Mode

Enable

Format

```
statistics show port-stats <port/SmartTRUNK-list>|all-ports
```

Description

Displays normal (non-error) port statistics.

Parameter	Value	Meaning
port-stats	<port/SmartTRUNK-list>	Specifies the port.
	all-ports	Specify all-ports to display port statistics for all physical and logical ports.

Restrictions

None.

Example

To display port statistics on port et.2.1:

```
rs# statistics show port-stats et.2.1

Port: et.2.1
-----
Port Stats                Received                Transmitted
-----                -
Frames/Packets            0                    0
. Switched frames (bridging) 0                    0
. Local frames (bridging)    0                    N/A
. Routed packets            0                    0
. Switched (data)           0                    N/A
. Consumed by CPU           0                    N/A
Bytes                     0                    0
. Bridged bytes             0                    0
. Routed bytes              0                    0
L2 table misses            0                    N/A
IP table misses            0                    N/A
IPX table misses           0                    N/A
IP TTL expirations         0                    N/A
IPX TC expirations         0                    N/A
1 minute traffic rates
. Average bits/sec          0                    0
. Packet discards           0                    0
. Packet errors             0                    0
. Unicast packets           0                    0
. Multicast packets         0                    0
. Broadcast packets         0                    0
Port stats cleared * Never Cleared *
```

The following describes the output:

Frames/Packets	
Switched frames	Shows the number of frames that have been bridged or forwarded.
Local frames	Shows the number of local frames (frames destined for a port that is the same as the port of entry) that was dropped.

Routed packets	
Switched (data)	Shows the number of packets forwarded by the hardware.
Consumed by CPU	Shows the number of packets sent to the control module to be forwarded.
Bytes	
Bridged bytes	Shows the total number of bytes that have been bridged.
Routed bytes	Shows the total number of bytes that have been routed.
L2 table misses	Shows the number of times that a Layer-2 frame could not be resolved by the L2 Table.
IP table misses	Shows the number of times that an IP packet could not be resolved by the IP Routing Table.
IPX table misses	Shows the number of times that an IPX packet could not be resolved by the IPX Routing Table.
IP TTL expirations	Shows the number of IP packets that have been received by the port with a Time-to-Live (TTL) header with a value of 1. The IP packet will then be expired at this point.
IPX TC expirations	Shows the number of IPX packets that have been received by the port with a TC header with a value of 1. The IPX packet will then be expired at this point.
1 minute traffic rates	
Average bits/sec	Shows an average traffic rate in bits/second for a one-minute time period for a port.
Packet discards	Shows the number of packets discarded by a port within a one-minute time period.
Packet errors	Shows the number of packets containing errors that was seen by the port within a one-minute time period.
Unicast packets	Shows the number of unicast packets that was seen by the port within a one-minute time period.
Multicast packets	Shows the number of multicast packets that was seen by the port within a one-minute time period.
Broadcast packets	Shows the number of broadcast packets that was seen by the port within a one-minute time period.
Port stats Cleared	Shows the date and time when the port stats were last cleared.

statistics show rarp

Mode

Enable

Format

statistics show rarp <string>|all

Description

Displays reverse ARP statistics.

Parameter	Value	Meaning
rarp	<string>	Specifies the interface name.
	all	Specify all to display reverse ARP statistics for all interfaces.

Restrictions

None.

Example

To display reverse ARP statistics on interface 'en0':

```
rs# statistics show rarp en0
Interface en0:
  0 requests received
  0 replies sent
  0 requests received on interface with rarpd disabled
  0 requests received that failed sanity check
  0 requests received that did not result in a match
  Last 5 Requests Received
  ----- no rarp requests received -----
  Last 5 Replies Sent
  ----- no rarp replies sent -----
```

statistics show summary-stats

Mode

Enable

Format

```
statistics show summary-stats
```

Description

Displays recent traffic summary statistics.

Restrictions

None.

statistics show tcp

Mode

Enable

Format

```
statistics show tcp
```

Description

Displays transmission control protocol (TCP) statistics.

Restrictions

None.

Example

To display TCP statistics:

```
rs# statistics show tcp
tcp:
    235 packets sent
        232 data packets (22777 bytes)
        1 data packet (494 bytes) retransmitted
        0 resends initiated by MTU discovery
        2 ack-only packets (5 packets delayed)
        0 URG only packets
        0 window probe packets
        0 window update packets
        0 control packets
    320 packets received
        227 acks (for 22776 bytes)
        3 duplicate acks
        0 acks for unsent data
        158 packets (185 bytes) received in-sequence
        0 completely duplicate packets (0 bytes)
        0 old duplicate packets
        0 packets with some dup. data (0 bytes duped)
        0 out-of-order packets (0 bytes)
        0 packets (0 bytes) of data after window
        0 window probes
        0 window update packets
        0 packets received after close
        0 discarded for bad checksums
        0 discarded for bad header offset fields
        0 discarded because packets too short
    0 connection requests
    1 connection accept
    1 bad connection attempt
    0 listen queue overflows
    1 connection established (including accepts)
    0 connections closed (including 0 drops)
        0 connections updated cached RTT on close
        0 connections updated cached RTT variance on close
        0 connections updated cached ssthresh on close
    0 embryonic connections dropped
    226 segments updated rtt (of 228 attempts)
    0 retransmit timeouts
        0 connections dropped by rexmit timeout
    0 persist timeouts
        0 connections dropped by persist timeout
    0 keepalive timeouts
        0 keepalive probes sent
        0 connections dropped by keepalive
    0 correct ACK header predictions
    88 correct data packet header predictions
```

statistics show udp

Mode

Enable

Format

```
statistics show udp
```

Description

Displays user datagram protocol (UDP) statistics.

Restrictions

None.

Example

To display UDP statistics:

```
rs# statistics show udp
udp:
    0 datagrams received
    0 datagrams with incomplete header
    0 datagrams with bad data length field
    0 datagrams with bad checksum
    0 datagrams dropped due to no socket
    0 broadcast/multicast datagrams dropped due to no socket
    0 datagrams dropped due to full socket buffers
    0 datagrams not for hashed pcb
    0 delivered
    0 datagrams output
```

statistics show top

Mode

Enable

Format

statistics show top

Description

Displays active tasks.

Restrictions

None.

Example

To display active tasks:

```
rs# statistics show top

Timestamp: 2000-04-25 17:56:32
CPU Idle : 98% (since system startup 441751425.0 sec ago)
NAME      USAGE %    RELATIVE %
-----
STP_T      0.2        47.65
PHY_POLL   0.0        17.57
L2_AGE_T   0.0        7.90
L3_AGE_T   0.0        7.10
IPC        0.0        4.60
CONS_T     0.0        4.25
STATS_T    0.0        3.96
TNTASK     0.0        2.41
SYSTEM H   0.0        0.88
HBT_T      0.0        0.82
SNMP       0.0        0.67
GATED      0.0        0.58
IPXROUTE   0.0        0.48
CONS2T     0.0        0.33
LOWEST     0.0        0.25
PPP_TASK   0.0        0.24
PINGER_T   0.0        0.11
L2_LRN_T   0.0        0.07
CDP_T      0.0        0.02
LFAP_CN    0.0        0.00
LGRP_T     0.0        0.00
MPS        0.0        0.00
TNETD      0.0        0.00
ETHH       0.0        0.00
NI H       0.0        0.00
ARP_T      0.0        0.00
HSWAP      0.0        0.00
IPRED_T    0.0        0.00
SYS_TK     0.0        0.00
SNMP_CF    0.0        0.00
WAN_TOD_   0.0        0.00
DHCP       0.0        0.00
BOUNCE     0.0        0.00
IP_T       0.0        0.00
IPX_T      0.0        0.00
PHX_T      0.0        0.00
NTP        0.0        0.00
ERROR_LO   0.0        0.00
L3_ACL_T   0.0        0.00
MCAST     0.0        0.00
PROFILE    0.0        0.00
PRI_L3MD   0.0        0.00
L3_RL_T    0.0        0.00
```


73 STP COMMANDS

The stp commands let you display and change settings for the default Spanning Tree.

73.1 COMMAND SUMMARY

The following table lists the **stp** commands. The **stp** commands let you display and change settings for the default Spanning Tree. The sections following the table describe the command syntax.

stp enable port <i><port-list></i>
stp filter-bpdu <i><port-list></i>
stp set bridging [forward-delay <i><num></i>] [hello-time <i><num></i>] [max-age <i><num></i>] [priority <i><num></i>] [damp-monitor-time <i><num></i>] [damp-bpdu-count <i><num></i>]
stp set port <i><port-list></i> priority <i><num></i> port-cost <i><num></i> dampening enable disable
stp set protocol-version rstp
stp set vlan-disable
stp show bridging-info
stp show dampening-info
stp show protocol-version

stp enable port

Mode

Configure

Format

stp enable port *<port-list>*

Description

The **stp enable port** command enables STP on the specified ports.

Parameter	Value	Meaning
port	<i><port-list></i>	The ports on which you are enabling STP. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8)

Restrictions

None

stp filter-bpdu

Mode

Configure

Format

stp filter-bpdu <port-list>

Description

The **stp filter-bpdu** command is used to filter out BPDUs on a port, when STP is disabled.

Parameter	Value	Meaning
port	<port-list>	The ports on which BPDUs will be filtered out when STP is disabled.

Restrictions

None

stp set bridging

Mode

Configure

Format

```
stp set bridging [forward-delay <num>] [hello-time <num>] [max-age <num>]  
[priority <num>] [damp-monitor-time <num>] [damp-bpdu-count <num>]
```

Description

The **stp set bridging** command lets you configure STP operating parameters.

Parameter	Value	Meaning
forward-delay	<num>	Sets the STP forward delay for the RS. The forward delay is measured in seconds. Specify a number from 4– 30. The default is 15.
hello-time	<num>	Sets the STP hello time for the RS. The hello time is measured in seconds. Specify a number from 1– 10. The default is 2.
max-age	<num>	Sets the STP maximum age for the RS. Specify a number from 6–40. The default is 20.
priority	<num>	Sets the STP bridging priority for the RS. Specify a number from 0 – 65535. The default is 32768.
damp-monitor-time	<num>	Factor of hello time during which a port is monitored to determine if it is stable or unstable. Enter a value between 1 and 20, inclusive. The default is 10.
damp-bpdu-count	<num>	The number of BPDUs that need to be received within the damp-monitor-time for the link to be considered stable. Enter a value between 1 and 60, inclusive. The default is 10.

Restrictions

None.

Examples

To set the bridging priority of Spanning Tree for the entire RS to 1:

```
rs(config)# stp set bridging priority 1
```

stp set port

Mode

Configure

Format

```
stp set port <port-list> priority <num> port-cost <num> dampening enable|disable
```

Description

The **stp set port** command sets the STP priority and port cost for individual ports.

Parameter	Value	Meaning
port	<port-list>	The port(s) for which you are setting STP parameters. You can specify a single port or a comma-separated list of ports. Example: et . 1.3,et . (1-3) , (4,6-8) .
priority	<num>	The priority you are assigning to the port(s). Specify a number from 0– 255. The default is 128.
port-cost	<num>	The STP cost you are assigning to the port(s). Specify a number from 1– 65535. The default depends on the port speed: 1 for Gigabit (100-Mbps) ports, 10 for 100-Mbps ports, and 100 for 10-Mbps ports.
dampening	enable	Enables dampening on the port.
	disable	Disables dampening on the port. This is the default.

Restrictions

STP dampening cannot be used in conjunction with RSTP.

stp set protocol-version

Mode

Configure

Format

```
stp set protocol-version rstp
```

Description

The **stp set protocol-version** command sets the protocol to be used by STP.

Parameter	Value	Meaning
rstp		The Rapid STP protocol (also known as “Fast Spanning Tree”), defined by IEEE 802.1w.

Restrictions

This command is not supported with per VLAN spanning tree.

This command works only on ports where STP is already enabled (with the **stp enable port** command).

stp set vlan-disable

Mode

Configure

Format

```
stp set vlan-disable
```

Description

The **stp set vlan-disable** command specifies that if the port does not belong to a certain VLAN, then the port should block all traffic coming from that VLAN.

Restrictions

None

stp show bridging-info

Mode

Enable

Format

```
stp show bridging-info
```

Description

The **stp show bridging-info** command displays STP bridging information for the RS.

Restrictions

None.

stp show dampening-info

Mode

Enable

Format

```
stp show dampening-info
```

Description

The **stp show dampening-info** command displays the state of ports on which dampening is enabled.

Restrictions

None.

Example

Following is sample output from the **stp show dampening-info** command. It displays the port's state, the period of time it is supposed to be monitored (dampening period), and the number of BPDUs it should receive within the dampening period.

```
rs# stp show dampening-info

Port Monitor Time (Factor to Hello Time) : 10
Bpdu Count : 10

Port      Port State
----      -
et.5.1    STABLE
```

stp show protocol-version

Mode

Enable

Format

```
stp show protocol-version
```

Description

The **stp show protocol-version** command displays the spanning tree protocol being used: either regular STP or fast STP. Fast STP, defined by IEEE 802.1w, is set with the **stp set protocol-version** command in Configure mode.

Restrictions

None.

74 SYSTEM COMMANDS

Use the **system** commands to change and display system parameters.

74.1 COMMAND SUMMARY

The following table lists the **system** commands. The sections following the table describe the command syntax.

system disable inputport level-rate-limiting slot <number>
system disable nat slot <number>
system disable telnet server
system enable aggregate-rate-limiting slot <number>
system hotswap {out slot <number> fabric <number>} {in slot <number>}
system image add <IPaddr-or-hostname> <filename> [primary-cm backup-cm] [slot0 slot1]
system image choose <filename> none [primary-cm backup-cm] [slot0 slot1]
system image copy slot0 slot1 <filename> slot0 slot1 [<filename>]
system image list primary-cm backup-cm all
system image delete <filename> primary-cm backup-cm slot0 slot1
system kill ssh-session <session-id>
system kill telnet-session <session-id>
system l3-deep-buckets module <number> set on
system promimage upgrade <hostname-or-IPaddr> <filename> primary-cm backup-cm
system set backup-cm-timeout seconds <seconds>
system set bootprom netaddr <IPaddr> netmask <IPnetmask> tftp-server <IPaddr> [tftp-gateway <IPaddr>]
system set console level fatal error warning info
system set contact <system-contact>

system set cpu-traffic-priority priority low medium high control
system set date year <year> month <month> day <day> hour <hour> min <min> second <sec>
system set dns server <IPaddr>[,<IPaddr>[,<IPaddr>]] domain <name>
system set dst-changing [s-wk <num>] [s-dow <num>] [s-mo <num>] [s-hr <num>] [s-min <num>] [e-wk <num>] [e-dow <num>] [e-mo <num>] [e-hr <num>] [e-min <num>] dst-fixed [s-mo <num>] [s-day <num>] [s-hr <num>] [s-min <num>] [e-mo <num>] [e-day <num>] [e-hr <num>] [e-min <num>] dst-manual
system set extended-debug inhibit-master-reboot enable-intr-monitor enable-pkt-capture
system set idle-timeout serial ssh telnet <num>
system set location <location>
system set login-banner <string> none file-name name <string>
system set name <system-name>
system set password <mode> <string> none
system set poweron-selftest [on quick]
system set show-config alphabetical
system set syslog [server <hostname-or-IPaddr>] [level <level-type>] [facility <facility-type>] [buffer-size <size>] [source <source-IPaddr>]
system set terminal autobaud baud <baud-rate> columns <num> rows <num>
system set timezone <timezone> <minutes>
system show active-config
system show bootlog
system show bootprom
system show capacity all chassis task cpu memory
system show contact
system show cpu-utilization
system show date
system show dns
system show environmental-info
system show hardware verbose summary slot <num>
system show idle-timeout serial ssh telnet
system show location
system show login-banner
system show name

system show nat-state
system show poweron-selftest-mode
system show scratchpad
system show serial-number
system show ssh-access
system show startup-config
system show syslog
system show syslog buffer
system show telnet access
system show terminal
system show timezone
system show uptime
system show users
system show version

system disable inputportlevel-rate-limiting

Mode

Configure

Format

```
system disable inputportlevel-rate-limiting slot <number>
```

Description

The **system disable inputportlevel-rate-limiting** command disables input port level rate limiting on a line card. The types of rate limiting available on the RS are:

- Per-flow rate limiting
- Port level rate limiting
- Aggregate rate limiting

By default, the per-flow rate limiting mode is enabled.

By using this command, you are enabling port level rate limiting for a specified line card.

Parameter	Value	Meaning
slot	<number>	The slot where the line card resides.

Restrictions

None.

Example

To enable aggregate rate limiting in slot 8 on the RS:

```
rs(config)# system enable aggregate-rate-limiting slot 8
```

system disable nat

Mode

Configure

Format

system disable nat slot *<number>*

Description

The **system disable nat** command disables Network Address Translation (NAT) on a line card.

Parameter	Value	Meaning
slot	<i><number></i>	The slot where the line card resides.

Restrictions

None.

system disable telnet-server

Mode

Configure

Format

system disable telnet-server

Description

The **system disable telnet-server** command disables the Telnet server on the RS. By default, the Telnet server is enabled.

This command causes the Telnet server to stop listening for and accepting Telnet connections to the RS. If you reboot the RS with this command in the Startup configuration, the Telnet server will not listen for connections. Negate this command to have the server start listening for connections again.

Restrictions

None.

Example

To disable the Telnet server on the RS:

```
rs(config)# system disable telnet-server
```

system enable aggregate-rate-limiting

Mode

Configure

Format

system enable aggregate-rate-limiting slot *<number>*

Description

The **system enable aggregate-rate-limiting** command enables port level and aggregate rate limiting on a line card. The types of rate limiting available on the RS are per-flow rate limiting, port level rate limiting, and aggregate rate limiting. By default, per-flow rate limiting is enabled.

By using this command, you are disabling per-flow rate limiting and enabling aggregate rate limiting and port level rate limiting for a line card.

To revert back to per-flow rate limiting, negate this command.

Parameter	Value	Meaning
slot	<i><number></i>	The slot where the line card resides.

Restrictions

None.

Example

To enable aggregate rate limiting in slot 8 on the RS:

```
rs(config)# system enable aggregate-rate-limiting slot 8
```

system hotswap

Mode
Enable

Format

system hotswap {out slot <number> fabric <number>} | {in slot <number>}

Description

The **system hotswap out** command deactivates a line card in a specified slot on the RS, causing it to go offline. The command performs the same function as pressing the Hot Swap button on the line card.

The **system hotswap in** command causes a line card that was deactivated with the **system hotswap out** command to go online again. The command performs the same function as removing the card from it’s slot and inserting it in again.

See the *Riverstone Networks RS Switch Router User Guide* for more information on hot swapping line cards.

Parameter	Value	Meaning
out slot	<number>	Causes the line card in the specified slot to be deactivated
fabric	<number>	Causes the specified switching fabric to be deactivated
in slot	<number>	Causes an inactive line card in the specified slot to be reactivated.



Note The **system hotswap in** command works only on a line card that was deactivated with the **system hotswap out** command.

Restrictions

None.

Example

To deactivate the line card in slot 7 on the RS:

```
rs# system hotswap out slot 7
```


system image add

Mode

Enable

Format

system image add <IPaddr-or-hostname> <filename> [primary-cm | backup-cm] [slot0 | slot1]

Description

The **system image add** command copies a system software image from a TFTP server to a PC card in a Control Module. By default, if the RS has two Control Modules, the image is copied to both Control Modules. If a Control Module has two PC cards, the image is copied to the card in slot 0. Optionally specify the Control Module, primary or backup, and the slot where the image is to be copied.

Parameter	Value	Meaning
add	<IPaddr-or-hostname>	The IP address or host name of the TFTP server or a TFTP URL.
	<filename>	The name of the system software image file.
primary-cm		Copies the system software image to the primary Control Module.
backup-cm		Copies the system software image to the backup Control Module.
slot0		Copies the system software image to the PC card in slot 0.
slot1		Copies the system software image to the PC card in slot 1.

Restrictions

None.

Examples

To download the software image file named **img.tar.gz** from the TFTP server 10.1.2.3 enter:

```
rs# system image add tftp://10.1.2.3/images/img.tar.gz
```

If the RS contains a primary and backup Control Module with PC cards in slot0, the above command copies the system software image into both PC cards.

To download the software image file named **img.tar.gz** from the TFTP server 10.1.2.3 onto the primary Control Module:

```
rs# system image add 10.1.2.3 /images/img.tar.gz primary-cm
```

The above command copies the system software image into the PC card in slot0 in the primary Control Module.

system image choose

Mode

Enable

Format

system image choose <filename> | none [primary-cm | backup-cm] [slot0 | slot1]

Description

The **system image choose** command specifies the system software image file on the PC card that you want the RS to use the next time you reboot the system. You can specify an image file on a PC card in either slot 0 or slot 1. You can also specify if the image file is on the primary or backup control module.

Parameter	Value	Meaning
choose	<filename>	The name of the system software image file.
	none	This parameter specifies that no image file is chosen for the next bootup.
primary-cm		This parameter specifies that the image file is on the primary control module.
backup-cm		This parameter specifies that the image file is on the backup control module.
slot0		This parameter specifies that the image file is on the PC card in slot 0.
slot1		This parameter specifies that the image file is on the PC card in slot 1.

Restrictions

None.

Examples

To specify a software image file on *slot0* in the backup Control Module for the next bootup:

```
rs# system image choose ros70 backup-cm
```

To specify a software image file on *slot1* in the primary Control Module for the next bootup:

```
rs# system image choose ros70 primary-cm slot1
```

system image copy

Mode

Enable

Format

```
system image copy slot0 | slot1 <filename> slot0 | slot1 [<filename>]
```

Description

The **system image copy** command copies a system software image file from one PC card to another in the primary Control Module. The file in either slot 0 or slot 1 can be specified. Additionally, files can be copied from primary to backup Control Modules.

Parameter	Value	Meaning
copy	<filename>	The name of the system software image file. The first occurrence of <filename> in the command is the source file, and the second is the destination file.
slot0		This parameter specifies that the image file is copied from or to the PC card in slot 0.
slot1		This parameter specifies that the image file is copied from or to the PC card in slot 1.

Restrictions

None.

Examples

To copy a software image file from *slot0* to *slot1*:

```
rs# system image copy slot0 ros71 slot1
```

To copy a software image file from *slot0* to a different filename on *slot1*:

```
rs# system image copy slot0 ros71 slot1 ros71.bak
```

system image delete

Mode

Enable

Format

system image delete <filename> primary-cm | backup-cm slot0 | slot1

Description

The **system image delete** command deletes a system software image file from the PC card on the Control Module.

Parameter	Value	Meaning
delete	<filename>	The name of the system software image file you want to delete.
primary-cm		This parameter deletes the image file from the primary control module.
backup-cm		This parameter deletes the image file from the backup control module.
slot0		This parameter deletes the image file on the PC card in slot 0.
slot1		This parameter deletes the image file on the PC card in slot 1.

Restrictions

None.

Examples

To delete a software image file in *slot0* in the backup Control Module:

```
rs# system image delete ros70 backup-cm
```

To delete a software image file in *slot1* in the primary Control Module:

```
rs# system image delete ros70 primary-cm slot1
```

system image list

Mode
Enable

Format

system image list primary-cm | backup-cm

Description

The **system image list** command lists the system software image files contained in the PC card on the Control Module. If there is a PC flash card in both slots on a Control Module, this command lists the image files from both cards.

Parameter	Value	Meaning
primary-cm		This parameter lists the image files on the primary control module.
backup-cm		This parameter lists the image files on the backup control module.

Restrictions

None.

Examples

To lists the system image files in the primary Control Module:

```
rs# system image list primary-cm  
Images currently available on Master CM  
slot0:  
  ros70A6    (version 7.0.A.6)  
slot1:  
  ros70A6    (version 7.0.A.6)
```

To list the system image files in the primary and backup Control Modules:

```
rs# system image list all  
Images currently available on Master CM  
slot0:  
  ros70A6    (version 7.0.A.6)  
slot1:  
  ros70A6    (version 7.0.A.6)
```

system kill ssh-session

Mode
Enable

Format

system kill ssh-session <session-id>

Description

The **system kill ssh-session** command ends the secure shell (SSH) session specified by the session ID. Use the **system show users** command to display the list of current SSH users and session IDs.

Parameter	Value	Meaning
ssh-session	<session-id>	The SSH session ID number, which can be 0, 1, 2, or 3. The system show users command displays the session ID number in the first column. You can only specify one session ID per system kill ssh-session command.

Restrictions

None.

Example

To show the active SSH sessions.

rs# system show users			
Current Terminal User List:			
## Login ID	Mode	From	Login Timestamp
--	----	----	-----
guest	guest	console	2001-02-28 10:32:42
0T	enabled	134.141.173.239	2001-02-28 10:53:49
1T	enabled	134.141.173.215	2001-02-28 13:35:32

Then, to kill SSH session 2:

rs# system kill ssh-session 2
SSH session 2 (from 10.9.0.1) killed

system kill telnet-session

Mode

Enable

Format

system kill telnet-session <session-id>

Description

The **system kill telnet-session** command ends the Telnet session specified by the session ID. Use the **system show users** command to display the list of current Telnet users and session IDs.

Parameter	Value	Meaning
telnet-session	<session-id>	The Telnet session ID number, which can be 0, 1, 2, or 3. The system show users command displays the session ID number in the first column. You can only specify one session ID per system kill telnet-session command.

Restrictions

None.

Example

To show the active Telnet sessions.

```
rs# system show users
Current Terminal User List:
# Login ID      Mode           From           Login Timestamp
- - - - -
0               enabled        console        Thu Feb 25 13:07:411999
2               login-prompt   10.9.0.1       Thu Feb 25 13:07:591999
3               login-prompt   10.9.0.1
```

Then, to kill Telnet session 2:

```
rs# system kill telnet-session 2
Telnet session 2 (from 10.9.0.1) killed
```

system l3-deep-hashing

Mode

Configure

Format

system l3-deep-buckets module *<num>* | all set on

Description

Use the **system l3-deep-buckets** command to enable deep hashing on a specified module.

Deep hashing allows for more than four hash buckets (levels within a particular entry for a hash value) within an entry in the L3 lookup table. Although hashing should provide an even distribution across the lookup table, there is still a possibility that more than four flows may end up at a particular entry in the lookup table.

Allowing for more than four entries through deep hashing will prevent thrashing, but may cause less-than-wirespeed performance due to the extra amount of entries. This is because thrashing reduces performance to a greater extent than deep hashing. But although deep hashing may result in less-than-wirespeed performance, it still performs much better than if it were thrashing.

Parameter	Value	Meaning
module	<i><num></i>	Specify a slot number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot.
	all	Enables deep hashing on all slots.
set	on	Enables deep hashing on the module. Negate this command from active configuration to disable l3 deep hashing.

Restrictions

None.

Example

To enable deep hashing on slot 7:

```
rs(config)# system l3-deep-buckets module 7 set on
```

system promimage upgrade

Mode

Enable

Format

system promimage upgrade <IPaddr-or-hostname> <filename> primary-cm | backup-cm

Description

The **system promimage upgrade** command copies and installs a bootPROM software image from a TFTP server onto the internal memory in the Control Module. The bootPROM software image is loaded when the RS is powered on.

Parameter	Value	Meaning
upgrade	<IPaddr-or-hostname>	The IP address or host name of the TFTP server or a TFTP URL.
	<filename>	The name of the boot PROM software image file.
	primary-cm	Specifies an upgrade for the primary control module.
	backup-cm	Specifies an upgrade for the backup control module.



Note If neither **primary-cm** or **backup-cm** is specified, then both control modules will be upgraded.

Restrictions

None.

Example

The command in the following example downloads a boot PROM image file from the TFTP server 10.50.89.88.

```
rs# system promimage upgrade tftp://10.50.89.88/qa/prom-upgrade  
Downloading image 'qa/prom-upgrade' from host '10.50.89.88'  
tftp complete  
checksum valid. Ready to program.  
flash found at 0xbfc00000  
erasing...  
programming...  
verifying...  
programming successful.  
Programming complete.
```

system set backup-cm-timeout

Mode

Configure

Format

system set backup-cm-timeout seconds <seconds>

Description

The **system set backup-cm-timeout** command sets the timeout used by the secondary Control Module to determine failure of the primary Control Module. If the secondary Control Module does not receive any heartbeats from the primary Control Module for a time equal to or greater than the timeout, then the secondary Control Module takes over as the primary Control Module. For example, if the primary Control Module becomes too busy to send heartbeats to the secondary Control Module, you can use this command to increase the timeout.

Parameter	Value	Meaning
seconds	<seconds>	The number of seconds that the secondary Control Module waits to receive heartbeats from the primary Control Module before taking over as the primary Control Module. Enter a value between 20-1000. The default is 20 seconds.

Restrictions

None.

Example

The command in the following example sets the timeout period to 30 seconds.

```
rs(config)# system set backup-cm-timeout seconds 30
```

system set bootprom

Mode

Configure

Format

```
system set bootprom netaddr <IPaddr> netmask <IPnetmask> tftp-server <IPaddr>
[tftp-gateway <Ipaddr>]
```

Description

The **system set bootprom** command sets parameters to aid in booting the system software image remotely over the network. Use this command to set the IP address, subnet mask, TFTP boot server address, and gateway address.



Note These parameters apply only to the Control Module's en0 Ethernet interface.

Parameter	Value	Meaning
netaddr	<IPaddr>	The IP address the RS uses during the boot exchange with the TFTP boot server.
netmask	<IPnetmask>	The subnet mask the RS uses during the boot exchange.
tftp-server	<IPaddr>	The TFTP boot server's IP address.
tftp-gateway	<Ipaddr>	The gateway that connects the RS to the TFTP boot server.

Restrictions

None.

Example

The command in the following example configures the RS to use IP address 10.50.88.2 to boot over the network from TFTP boot server 10.50.89.88.

```
rs(config)# system set bootprom netaddr 10.50.88.2 netmask 255.255.0.0
tftp-server 10.50.89.88
```

system set console level

Mode

Configure

Format

system set console level fatal | error | warning | info

Description

The **system set console level** command specifies the type of messages displayed on the console terminal.

Parameter	Value	Meaning
	fatal	Displays fatal messages only.
	error	Displays fatal and error messages only
	warning	Displays fatal, error, and warning messages only.
	info	Displays all messages.

Restrictions

None.

system set console limit

Mode

Configure

Format

system set console limit *<seconds>*

Description

The **system set console limit** command sets the time interval for displaying INFO, WARNING, or ERROR messages on the console screen. By default messages are displayed as soon as they are generated. Use the **system set console level** command to reset the time interval. For example, this command can be used to limit the console display to one message every three seconds.

Parameter	Value	Meaning
limit	<i><seconds></i>	Specifies the number of seconds a message is displayed before another message is printed to the screen

Restrictions

None.

system set contact

Mode

Configure

Format

system set contact <system-contact>

Description

The **system set contact** command specifies the name and contact information for the network administrator responsible for the RS.

Parameter	Value	Meaning
contact	<system-contact>	A string listing the name and contact information for the network administrator responsible for the RS. If the string contains blanks or commas, you must use the quotation marks around the string. (Example: "Jane Doe, janed@corp.com, 408-555-5555 ext. 555")

Restrictions

None.

system set cpu-traffic-priority

Mode

Configure

Format

```
system set cpu-traffic-priority priority low | medium | high | control
```

Description

The **system set cpu-traffic-priority** sets the priority level for all non-control traffic coming from and going into of the CPU. Non-control traffic is non-routed protocol traffic, such as SNMP traffic and Telnet traffic.

Parameter	Value	Meaning
cpu-traffic priority		Specifies the priority level for the CPU traffic.
	low	Specifies low priority. This is default.
	medium	Specifies medium priority.
	high	Specifies high priority.
	control	Specifies control priority.

Restrictions

None.

system set date

Mode

Enable

Format

system set date year <year> month <month> day <day> hour <hour> min <min> second <sec>

Description

The **system set date** command sets the system time and date for the RS. The RS keeps time with a battery-backed realtime clock. To display the time and date, enter the **system show date** command.

Parameter	Value	Meaning
year	<year>	Four-digit number for the year. (Example: 1998)
month	<month>	Name of the month. You must spell out the month name. (Example: March)
day	<day>	Number from 1 – 31 for the day.
hour	<hour>	Number from 0 – 23 for the hour. (The number 0 means midnight.)
min	<min>	Number from 0 – 59 for the hour.
second	<sec>	Number from 0 – 59 for the second.

Restrictions

None.

system set dns

Mode

Configure

Format

```
system set dns server ["<IPaddr> [<IPaddr> [<IPaddr>]]"] domain <name>
```

Description

Use the **system set dns** command to configures DNS servers for the RS. Additionally specify the domain name to use for each DNS query.

Parameter	Value	Meaning
dns server	<IPaddr>	The IP address of the DNS server. Specify the address in dotted-decimal notation. You can specify up to three DNS servers separated by single spaces in the command line. If you specify more than one IP address, you must surround the IP address with a set of quotes.
domain	<name>	The domain name over which the server is an authority.

Restrictions

None.

Examples

To configure a single DNS server and make the DNS domain name *mrB.com* enter:

```
rs(config)# system set dns server 10.1.2.3 domain mrB.com
```

To configure three DNS servers and make the DNS domain name *mrB.com* enter:

```
rs(config)# system set dns server "10.1.2.3 10.2.10.12 10.3.4.5" domain mrB.com
```

system set dst

Mode

Configure

Format

```
system set dst-changing [s-wk <num>] [s-dow <num>] [s-mo <num>] [s-hr <num>] [s-min <num>] [e-wk <num>] [e-dow <num>] [e-mo <num>] [e-hr <num>] [e-min <num>] | dst-fixed [s-mo <num>] [s-day <num>] [s-hr <num>] [s-min <num>] [e-mo <num>] [e-day <num>] [e-hr <num>] [e-min <num>] | dst-manual
```

Description

Use the **system set dst** command to set the RS clock for daylight savings time. When **s-mo** (start month) is reached, the clock automatically moves forward one hour. When **e-mo** (end month) is reached, the clock automatically moves backward one hour. The UCT offset remains constant. Disable the **system set dst** command by negating it.

Parameter	Value	Meaning
dst-changing		This parameter allows the user to set up daylight saving time according to specific days.
s-wk	<num>	This optional parameter specifies the starting week of the month. Specify a number between 1 and 5. The following is a description of the values: 1-first week, 2-second week, 3-third week, 4-fourth week, 5-last week. The default value is 1.
s-dow	<num>	This optional parameter specifies the starting day of the week. Specify a number between 1 and 7. The following is a description of the values: 1-Sunday, 2-Monday, 3-Tuesday, 4-Wednesday, 5-Thursday, 6-Friday, 7-Saturday. The default value is 1.
s-mo	<num>	This optional parameter specifies the starting month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1.
s-hr	<num>	This optional parameter specifies the starting hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.
s-min	<num>	This optional parameter specifies the starting minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.

Parameter	Value	Meaning
e-wk	<num>	This optional parameter specifies the ending week of the month. Specify a number between 1 and 5. The following is a description of the values: 1-first week, 2-second week, 3-third week, 4-fourth week, 5-last week. The default value is 1.
e-dow	<num>	This optional parameter specifies the ending day of the week. Specify a number between 1 and 7. The following is a description of the values: 1-Sunday, 2-Monday, 3-Tuesday, 4-Wednesday, 5-Thursday, 6-Friday, 7-Saturday. The default value is 1.
e-mo	<num>	This optional parameter specifies the ending month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1.
e-hr	<num>	This optional parameter specifies the ending hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.
e-min	<num>	This optional parameter specifies the ending minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.
dst-fixed		This parameter allows the user to set up daylight saving time according to specific dates.
s-mo	<num>	This optional parameter specifies the starting month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1.
s-day	<num>	This optional parameter specifies the starting day of the month. Specify a number between 1 and 31. This is based upon a 31-day month, where 1-first day and 31-thirty first day for that month. The default value is 1.
s-hr	<num>	This optional parameter specifies the starting hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.
s-min	<num>	This optional parameter specifies the starting minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.
e-mo	<num>	This optional parameter specifies the ending month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1.

Parameter	Value	Meaning
e-day	<num>	This optional parameter specifies the ending day of the month. Specify a number between 1 and 31. This is based upon a 31-day month, where 1-first day and 31-thirty first day for that month. The default value is 1.
e-hr	<num>	This optional parameter specifies the ending hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.
e-min	<num>	This optional parameter specifies the ending minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.
dst-manual		This parameter allows the user to set the system time forward by one hour after the command is saved into active configuration. Negating this command will set the system time back one hour.

Restrictions

None.

Examples

Set daylight saving time to start at midnight on the last Sunday of March and end at 2:00 A.M on the first Saturday of October every year:

```
rs(config)# system set dst-changing s-wk 5 s-dow 1 s-mo 3 e-wk 1
e-dow 7 e-mo 10 e-hr 2
```

Set daylight saving time to start at 3:00 a.m. on April 1st and end at midnight on the 15th of September every year:

```
rs(config)# system set dst-fixed s-mo 4 s-day 1 s-hr 3 e-mo 9 e-day
15
```

system set extended-debug

Mode
Configure

Format

system set extended-debug inhibit-master-reboot | enable-intr-monitor | enable-pkt-capture

Description

The **system set extended -debug** command enables various troubleshooting functions.



Note Use this command only when directed to do so by Riverstone technical support.

Parameter	Value	Meaning
extended-debug	inhibit-master-reboot	If this parameter is set, after a failover the new primary Control Module will not reboot the old primary Control Module. This parameter is useful for troubleshooting a Control Module crash.
	enable-intr-monitor	If this parameter is set, interrupt disables are logged. The log of interrupts is displayed with the diagnostic mode command debug interrupt -check log .
	enable-pkt-capture	If this parameter is set, the last ten packets received by the RS are stored in memory. In the case of a system crash, the packet information is printed to the Console as well as appended to the core file on the PC card.

Restrictions

None.

system set idle-timeout

Mode

Configure

Format

```
system set idle-timeout serial | ssh | telnet <num>
```

Description

The **system set idle-timeout** command sets the time (in minutes) the console can remain idle before the communication session is terminated by the control module.

Parameter	Value	Meaning
serial		Use this parameter to set the timeout value for a serial console connection.
ssh		Use this parameter to set the timeout value for a secure shell (SSH) connection.
telnet		Use this parameter to set the timeout value for a telnet console connection.
	<num>	Use this parameter to set the idle-timeout value in minutes. Specify any value between 0 and 60. The default is 5 minutes. Specifying 0 disables the timeout.

Restrictions

None.

system set location

Mode

Configure

Format

system set location <location>

Description

The **system set location** command creates a string describing the location of the RS. The system name and location can be accessed by SNMP managers.

Parameter	Value	Meaning
location	<location>	A string describing the location of the RS. If the string contains blanks or commas, you must use quotation marks around the string. Example: "Bldg C, network control room".

Restrictions

None.

system set login-banner

Mode

Configure

Format

```
system set login-banner <string> | none | file-name name <string>
```

Description

The **system set login-banner** command configures the initial login banner that displays when logging into the RS. The banner may span multiple lines by adding line-feed characters in the string.

Parameter	Value	Meaning
login-banner	<string>	Is the text of the login banner for the RS. The banner may span multiple lines by adding the line-feed character, \n , in the string.
	none	Specifies that no login-banner will be used on the RS.
name	<string>	Specifies the name of the file containing the login banner.

Restrictions

None.

Example

The following example configures a multi-line login banner:

```
rs(config)# system set login-banner "Server network  
RS\nUnauthorized Access Prohibited"
```

The next person to log into the RS would see the following:

```
Server network RS  
Unauthorized Access Prohibited  
  
Press RETURN to activate console...
```

If you do not want any login-banner at all, enter the following:

```
rs(config)# system set login-banner none
```

system set name

Mode

Configure

Format

system set name <system-name>

Description

Use the **system set name** command to name the RS. This name will appear in the CLI command prompt.

Parameter	Value	Meaning
name	<system-name>	The hostname of the RS. If the string contains blanks or commas, you must use quotation marks around the string. Example: Mega-Corp RS #27

Restrictions

None.

system set password

Mode

Configure

Format

system set password *<mode>* *<string>* | none

Description

The **system set password** command sets or changes the passwords for the Login and Enable modes.



Note

If a password is configured for the Enable mode, the RS prompts for the password when you enter the **enable** command. Otherwise, the RS displays a message advising you to configure an Enable password, then enters the Enable mode. From the Enable mode, you can enter the Configure mode to make configuration changes.

Parameter	Value	Meaning
password	<i><mode></i>	The access mode for which you are setting a password. Use either login or enable .
	login	The password required to start a CLI session. The RS prompts for this password when the system finishes booting.
	enable	The password for entering the Enable mode.
	<i><string></i>	The password.
	none	If you specify none , no password is required.



Note

You cannot use the string **none** as a password.

Restrictions

The RS stores passwords in the Startup configuration file. If you copy a configuration file from one RS to another, the passwords in the file also are copied and will be required on the new RS.

When you activate a new password by copying the **password set** command to the active configuration, the RS replaces the command with a **system set hashed-password** command, which hides the password text in the configuration file so that the password is not visible to others if they examine the configuration file.

Example

To remove a password, enter the following command while in Configure mode:

```
rs(config)# system set password <mode> none
```

system set poweron-selftest

Mode

Configure

Format

system set poweron-selftest on | quick

Description

Use the **system set poweron-selftest** command to set the type of Power-On-Self-Test (POST) the RS will perform during the next system bootup. By default, no POST is performed during system bootup. To perform POST, use this command to specify which type of test to run, **on** or **quick**. Turn off POST by negating the command.

Parameter	Value	Meaning
poweron-selftest	on	The RS will perform a full test during the next system bootup.
	quick	The RS will perform a quick test during the next system bootup.

Restrictions

None.

system set show-config

Mode

Configure

Format

system set show-config alphabetical

Description

The **show** and **system show active-config** commands normally display the configuration commands in the order that they are executed. The **system set show-config** command changes the way the configuration commands are displayed.

Parameter	Value	Meaning
alphabetical		Shows the configuration commands in alphabetical order.

Restrictions

None.

Example

To display the configuration commands in alphabetical order:

```
rs(config)# system set show-config alphabetical
```


system set syslog

Mode

Configure

Format

```
system set syslog [server <hostname-or-IPaddr>] [level <level-type>] [facility <facility-type>]  
[source <source-IPaddr>] [buffer-size <size>]
```

Description

Use the **system set syslog** command to identify which Syslog servers the RS will send system messages to. You can identify one or multiple Syslog servers. To identify multiple servers, enter the command in full once for each server.



Note The maximum number of servers that can be set on one RS is 4.

Additionally, the type of messages to send as well as the facility under which the message is sent can be controlled. The type of messages to send is based on the severity of the message, controlled by the option **level**. Messages can also be sent under a specific facility. There are 11 facilities supported by the RS. On the Syslog server or servers, decide what to do with these messages based on the level as well as the facility. For example, choose to discard the messages, write them to a file, or send them out to the console. Further identify the source of the system messages sent to the Syslog server by specifying a source IP address for the Syslog on the RS.

The RS keeps the last *n* messages in a local circular buffer. By default, this buffer keeps the last 10 Syslog messages. You can change the buffer size to hold anywhere from 10 to 50 messages. To view the current buffer size, enter the **system show syslog buffer** command.

Parameter	Value	Meaning
server	<hostname-or-IPaddr>	Hostname or IP address of the SYSLOG server.
level	<level-type>	Level of Syslog message logged.
	fatal	Log only fatal messages.
	error	Log fatal messages and error messages.
	warning	Log fatal messages, error messages, and warning messages. This is the default.
	info	Logs all messages, including informational messages.
facility	<facility-type>	Type of facility under which you want messages to be sent. By default, messages are sent under facility local7 .
	kern	kernel messages

Parameter	Value	Meaning
	user	user messages
	daemon	daemon messages
	local0	Reserved for local use
	local1	Reserved for local use
	local2	Reserved for local use
	local3	Reserved for local use
	local4	Reserved for local use
	local5	Reserved for local use
	local6	Reserved for local use
	local7	Reserved for local use
source	<source-IPaddr>	Source IP address of the messages sent to the Syslog server. You must specify a Unicast IP address in the form a.b.c.d.
buffer-size	<size>	The Syslog message buffer size. The size specifies how many messages the Syslog buffer can hold. You can specify a number from 10 – 50, giving the buffer a capacity to hold from 10– 50 Syslog messages. The default is 10.

Restrictions

None.

Example

To log only fatal and error level messages to the syslog server on 10.1.43.77:

```
rs(config)# system set syslog server 10.1.43.77 level error
```

system set terminal

Mode

Configure

Format

```
system set terminal autobaud | baud <baud-rate> | columns <num> | rows <num>
```

Description

The **system set terminal** command globally sets parameters for a serial console's baud rate, output columns, and output rows.

Parameter	Value	Meaning
autobaud		Enables the console port to automatically detect the baud rate of the connected terminal.
baud	<baud-rate>	Sets the baud rate.
	300	300 baud.
	600	600 baud.
	1200	1200 baud.
	2400	2400 baud.
	4800	4800 baud.
	9600	9600 baud.
	19200	19200 baud.
	38400	38400 baud.
columns	<num>	Sets the number of columns displayed at one time.
rows	<num>	Sets the number of rows displayed at one time.

Restrictions

None.

Example

The command in the following example sets the baud rate, number of columns, and number of rows for the management terminal connected to the System Control module.

```
rs(config)# system set terminal baud 38400 columns 132 rows 50
```

system set timezone

Mode

Configure

Format

```
system set timezone <timezone> | <minutes>
```

Description

The **system set timezone** command sets the local time zone for the RS. Use one of the time zone keywords to specify the local time zone or specify the time offset in minutes. Configure the time zone in order to use NTP (Network Time Protocol) to synchronize the real time clock.

Parameter	Value	Meaning
timezone	<timezone>	Sets the time zone.
	est	Eastern Standard Time (UCT -05:00)
	cst	Central Standard Time (UCT -06:00)
	mst	Mountain Standard Time (UCT -07:00)
	pst	Pacific Standard Time (UCT -08:00)
	uct -12	Eniwetok, Kawajalein (UCT -12:00)
	uct -11	Midway Island, Samoa (UCT -11:00)
	uct -10	Hawaii (UCT -10:00)
	uct -9	Alasaka (UCT -09:00)
	uct -8	Pacific Standard Time (UCT -08:00)
	uct -7	Mountain Standard Time (UCT -07:00)
	uct -6	Central Standard Time (UCT -06:00)
	uct -5	Eastern Standard Time (UCT -05:00)
	uct -4	Caracas, La Paz (UCT -04:00)
	uct -3	Buenos Aires, Georgetown (UCT -03:00)
	uct -2	Mid-Atlantic (UCT -02:00)
	uct -1	Azores, Cape Verde Island (UCT -01:00)
	uct	Greenwich, London, Dublin (UCT)
	uct+1	Berlin, Madrid, Middle European Time, Paris (UCT +01:00)
	uct+2	Athens, Helsinki, Istanbul, Cairo (UCT +02:00)

Parameter	Value	Meaning
	uct+3	Moscow, Nairobi, Riyadh (UCT +03:00)
	uct+4	Abu Dhabi, Kabul(UCT +05:00)
	uct+5	Pakistan (UCT +05:00)
	uct+5:30	India (UCT +05:30)
	uct+6	Bangladesh (UCT +06:00)
	uct+7	Bangkok, Jakarta (UCT +07:00)
	uct+8	Beijing, Hong Kong, Singapore(UCT +08:00)
	uct+9	Japan, Korea (UCT +09:00)
	uct+10	Sydney, Guam (UCT +10:00)
	uct+11	Solomon Is. (UCT +11:00)
	uct+12	Fiji, Marshall Is. Auckland (UCT +12:00)
<minutes>	Between -720 to + 720.	Specify the time zone offset in minutes. .

Restrictions

None.

Example

To set the local time zone to Pacific Standard Time (UCT -8:00).

```
rs(config)# system set timezone pst
```

system show active-config

Mode

Enable

Format

system show active-config

Description

The **system show active-config** command shows the CLI configuration of the running system.

Restrictions

None.

Example

To display the active configuration:

```
rs# system show active-config
Running system configuration:
!
! Last modified from Console on 2000-06-06 15:10:29
!
1E: atm create vcl port at.9.1.1.200
!
2 : vlan create VLANA port-based
3 : vlan create VLAN_A port-based
!
4E: interface create ip pos11 address-netmask 12.1.1.3/24 peer-address
20.11
.11.21 type point-to-point port so.13.1
5E: interface create ip atm1 address-netmask 12.1.1.1/24 port
at.9.1.1.200
6 : system set idle-timeout telnet 0
!
7 : system set idle-timeout serial 0
```

system show bootlog

Mode

Enable

Format

system show boot log

Description

The **system show boot log** command displays the contents of the boot log file, which contains all the system messages generated during bootup. The display includes status information on the hardware, such as the control module(s) and power supplies. It also lists the modules on the RS, which slots and ports were initialized, and displays the status of the ports.

Restrictions

None.

Example

To display the bootlog information:

```
rs# system show bootlog
-----
RS 8000 System Software, Version 4.1.
Copyright (c) 1998-2000, Riverstone Networks, Inc.
Built by mhaydt@sage on Mon Jun  5 10:42:23 2000
Processor: R5000, Rev 2.1, 197.99 MHz
System started on 2000-06-06 11:07:20
-----
2000-06-06 11:07:21 %SYS-I-FLASHCRD, Mounting 8MB Flash card
2000-06-06 11:07:29 %SYS-E-FLASHMNTFAIL, 8MB Flash card could not be
mounted
2000-06-06 11:07:29 %SYS-E-VFSBADBLKNUM, vfs_initialize_pcmcia: flash
mount: bad
    block number
2000-06-06 11:07:38 %SYS-I-INITSYS, initializing system RS 8000
2000-06-06 11:07:38 %SYS-I-DSCVMOD, discovered 'Control Module (CM2)'
module in
slot CM
2000-06-06 11:07:43 %SYS-I-MULTICPU, additional CPU Module(s) detected
in slot C
M/1
2000-06-06 11:07:43 %SYS-I-INITSLOTS, Initializing system slots -
please wait
2000-06-06 11:07:50 %SYS-I-MODPROBE, Detecting installed media modules
- please
wait
2000-06-06 11:07:52 %SYS-I-DSCVMOD, discovered '10/100-TX' module in
slot 2
2000-06-06 11:07:52 %SYS-I-DSCVMOD, discovered '10/100-TX' module in
slot 3
2000-06-06 11:07:52 %SYS-I-DSCVMOD, discovered '100-FX-M' module in
slot 4
2000-06-06 11:07:52 %SYS-I-DSCVMOD, discovered 'Dual HSSI' module in
slot 6
2000-06-06 11:07:52 %SYS-I-DSCVMOD, discovered 'Quad Serial-CE' module
in slot 7
2000-06-06 11:07:59 %SYS-I-INITPORT, initialized slot 2, port 1
2000-06-06 11:07:59 %SYS-I-INITPORT, initialized slot 2, port 2
2000-06-06 11:07:59 %SYS-I-INITPORT, initialized slot 2, port 3
--- More: m,<space> --- Quit: q --- One line: <return> ---
```


system show bootprom

Mode

Enable

Format

system show bootprom

Description

The **system show bootprom** command displays the boot PROM parameters for a TFTP download of the system image. The display includes the network address and mask of the RS, the IP address of the TFTP server, and the gateway to the TFTP server. This information is useful only if the system has been configured to download the image via TFTP.

Restrictions

None.

Example

To display the boot prom parameters:

```
rs# system show bootprom
Boot Prom's parameters for TFTP network booting:
(Current values were set from boot prompt, not config file)
Network address      : 123.132.111.155
Network mask         : 222.222.222.136
TFTP server          : 123.132.121.23
Gateway to reach TFTP server: 123.132.111.129
```

system show capacity

Mode

Enable

Format

system show capacity all | chassis | task | cpu | memory

Description

The **system show capacity** command displays information about the resources of the RS.

Restrictions

None.

Example

To display usage information for all the RS' resources:

```
rs# system show capacity all
```

Capacity MIB Chassis Information: ❶									
Total Slots	Used Slots	Free Slots	CPU Redundancy	Power Supply Redundancy	Switch Fabric Redundancy				
8	7	1	Present	Present	No Support				

Capacity MIB Task Information: ❷									
Index	Name	Count	Task Status	Memory Used					
1	CONS_T	2	Suspended (event)	8096					
6	IPX_T	16996	Suspended (event)	8096					
11	STATS_T	169939	Suspended (event)	8096					
16	PHY_POLL	339892	Suspended (event)	16384					
21	L3_ACL_T	1	Suspended (event)	16192					
26	IPC	2	Suspended (event)	8096					
31	PINGER_T	7623	Suspended (event)	8096					
36	BOUNCE	2	Suspended (event)	8096					
41	CONS2T	2	Suspended (event)	8096					

Capacity MIB Storage Information: ❸									
Type	Description	Size	Free	Used	Block	Remov	Fail	CPU	
Internal CPU	4194304	3837935	356369	16	True	0			
FLASH	Internal Flash	756	745	11	64	True	0		
L2HW	port et.2.1	5888	5887	1	64	True	0		
L2HW	port et.2.2	5888	5887	1	64	True	0		
L2HW	port et.2.3	5888	5887	1	64	True	0		
L2HW	port et.2.4	5888	5887	1	64	True	0		
L2HW	port et.2.5	5888	5887	1	64	True	0		
L2HW	port et.2.6	5888	5887	1	64	True	0		
L2HW	port et.2.7	5888	5887	1	64	True	0		
L2HW	port et.2.8	5888	5887	1	64	True	0		
L2HW	port et.3.1	5888	5887	1	64	True	0		
L2HW	port et.3.2	5888	5887	1	64	True	0		
L2HW	port et.3.3	5888	5887	1	64	True	0		
L2HW	port et.3.4	5888	5887	1	64	True	0		
.									

Capacity MIB CPU Information: ❹									
Slot	Util	L3 Learned/Aged	L2 Learned/Aged	NIA Received/Xmt					
-----0									
1	0	/0	0	/0	0	/75684			

```
rs#
```

Legend:

1. Capacity MIB Chassis Information displays information about the chassis:

- the total number of slots in the chassis, including the slot for the CPU,
 - the number of slots used, including that used by the CPU, and
 - the number of available slots.
 - It also indicates if there is a redundant control module, power supply, and switch fabric (for the 8600 only) installed on the chassis.
2. Capacity MIB Task Information displays information about the tasks scheduled for the CPU:
- *Index* is the unique index assigned to the task.
 - *Name* is the encrypted name assigned to the task. This is unique for each different type of task.
 - *Count* is the number of times the task was scheduled to run. It is a cumulative count from the time the RS was started.
 - *Task Status* is the current status of the task. The task status can be Ready (task is scheduled and ready), Suspended (task is waiting for something, such as a queue or memory), Finished, or Terminated
 - *Memory Used* is the size of the memory consumed by the task. This can be used to monitor the excess memory used by a particular task and is expressed in bytes.
3. Capacity Storage Information provides information about the non-volatile memory devices in the RS:
- *Type* indicates the type of storage device.
 - *Description* describes the storage device.
 - *Size* is the total memory capacity of the device, expressed in blocks.
 - *Free* is the amount of free memory in the device, expressed in blocks.
 - *Used* is the size of the used memory on the device, expressed in blocks. This includes blocks of memory that are partially used.
 - *Block* is the size of the memory blocks in the memory device. This is the minimum block size of memory returned when memory is requested. It is expressed in bytes.
 - *Remove* indicates if the memory is removable.
 - *Fail* is the number of times a memory allocation in the memory device has failed. For L2 and L3 hardware, it is the number of times a full hash bucket condition has been met.
4. Capacity MIB CPU Information displays information about the various hardware tables:
- *Slot* is the slot number of the CPU.
 - *Utilization* is the CPU utilization expressed as an integer percentage. This is calculated over the last 5 seconds at a 0.1 second interval as a simple average.
 - *L3 Learned* is the total number of new L3 flows the CPU has processed and programmed into the L3 hardware flow tables. L3 flows are IP or IPX packets that are routed from one subnet to another.
 - *L3 Aged* is the total number of L3 flows that were removed from the L3 hardware flow table across all modules.
 - *L2 Learned* is the total number of L2 flows or addresses learned.
 - *L2 Aged* is the total number of L2 flows or addresses that were removed from the L2 lookup tables.
 - *NIA Received* is the total number of packets received by the NIA chip. This is useful in gauging how many packets are forwarded to the CPU for processing.

- *NIA XMT* is the total number of packets transmitted by the NIA chip. This is useful in seeing how much the CPU is communicating directly with management stations and other routes.

system show contact

Mode

Enable

Format

system show contact

Description

The **system show contact** command displays contact information about the administrator of the RS.

Restrictions

None.

Example

To display contact information:

```
rs# system show contact  
Administrative contact: IT_dept.
```

system show cpu-utilization

Mode

Enable

Format

system show cpu-utilization

Description

The **system show cpu-utilization** command displays the percentage of the CPU being used. It is expressed as an integer percentage. This is calculated as a simple average over the last 5 seconds and the last 60 seconds at a 0.1 second interval.

Restrictions

None.

Example

To display CPU information:

```
rs# system show cpu-utilization
CPU Utilization (5 seconds): 1%    (60 seconds): 1%
rs#
```

system show date

Mode

Enable

Format

system show date

Description

The **system show date** command displays the system date and time.

Restrictions

None.

Example

To display the system time and date:

```
rs# system show date  
Current time: 2000-06-07 14:17:28  
rs#
```


system show dns

Mode

Enable

Format

system show dns

Description

The **system show dns** command displays the IP address(es) and domain name of the DNS servers the RS can use.

Restrictions

None.

Example

To display the IP address(es) and domain name of DNS servers:

```
rs# system show dns  
DNS domain: mktg_a  
DNS server: 16.50.11.12  
rs#
```

system show environmental-info

Mode

Enable

Format

system show environmental-info

Description

The **system show environmental-info** command displays environmental information, such as temperature and power supply status.

Restrictions

None.

Example

To display environmental information:

```
rs# system show environmental-info
Environmental Status
Temperature: normal
Fan Tray: normal
Power Supply 1: normal  2: normal
rs#
```

system show hardware

Mode

Enable

Format

system show hardware verbose | summary | slot <num>

Description

The **system show hardware** command displays information about hardware. The display includes the primary and redundant CPUs, the primary and backup power supplies, and the PC flash card. The information displayed includes cache size, memory size, MAC addresses, and status. It also lists each line card installed and its associated ports.

Parameter	Value	Meaning
hardware	verbose	Displays more detailed information about the system hardware.
	summary	Displays summarized information about the system hardware.
slot	<num>	Displays information about the module in the specified slot number.

Restrictions

None.

Example

To display hardware information:

```
rs# system show hardware

Hardware Information
  System type       : RS 8000, Rev. 0
  CPU Module type   : CPU-Elan, Rev. 0
  Processor         : R5000, Rev 2.1, 197.99 MHz
    Icache size     : 32 Kbytes, 32 bytes/line
    Dcache size     : 32 Kbytes, 32 bytes/line
  CPU Board Frequency: 65.99 MHz
  PCMCIA card       : 8MB flash memory card (corrupt filesystem, not mounted)
  System Memory size : 64 MBytes
  Network Memory size: 8 MBytes
  MAC Addresses
    System          : 00c034:21d32e
    10Base-T CPU Port: 00c034:21d32f
    Internal Use     : 00c034:21d320 -> 00c034:21d5cd
  CPU Mode          : Active
  Redundant CPU slot : CM/1 (not operational)

Power Supply Information

  PS1: present
  PS2: present

Redundant CPU Information
  CPU Module type   : (unknown)
  System Memory size : 0 MBytes
  Network Memory size: 0 MBytes
  CPU Mode          : Stand-by
  Redundant CPU slot : not operational

Slot Information
  Slot    CM,  Module: Control Module (CM2)  Rev. 0

  Slot    CM/1,  Module: Control Module (CM2)  Rev. 0.0

  Slot     2,  Module: 10/100-TX  Rev. 0.2
    Port:  et.2.1,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 33
    Port:  et.2.2,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 34
    Port:  et.2.3,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 35
    Port:  et.2.4,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 36
    Port:  et.2.5,  Media Type: 10/100-Mbit Ethernet,  Physical Port:  Port:
et.3.5,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 53
    Port:  et.3.6,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 54
    Port:  et.3.7,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 55
  Port: et.3.8, Media Type: 10/100-Mbit Ethernet, Physical Port: 56
```

system show idle-timeout

Mode

Enable

Format

system show idle-timeout serial | ssh | telnet

Description

The **system show idle-timeout** command displays the timeout value (in minutes). If a session remains idle longer than the **idle-timeout** value, the session is closed by the system. Specify a timeout value for a serial, secure shell (SSH), or a Telnet connection.

Restrictions

None.

Example

To display the timeout value:

```
rs# system show idle-timeout serial ssh telnet
Serial console idle timeout = 5 minute(s)
SSH console idle timeout = 5 minute(s)
Telnet console idle timeout disabled.
rs#
```

system show location

Mode

Enable

Format

system show location

Description

The **system show location** command displays the location of the RS.

Restrictions

None.

Example

To display the location:

```
rs# system show location  
System location: Santa_Clara  
rs#
```

system show login-banner

Mode

Enable

Format

system show login-banner

Description

The **system show login-banner** command displays the login banner. The login banner is configured using the **system set login-banner** command.

Restrictions

None.

Example

To display the login-banner:

```
rs# system show login-banner
Login banner:  system default
rs#
```

system show name

Mode

Enable

Format

system show name

Description

The **system show name** command displays the system name of the RS.

Restrictions

None.

Example

To display the system name:

```
RS-8000# system show name  
System name: RS-8000  
RS-8000#
```


system show nat-state

Mode

Enable

Format

system show nat-state

Description

The **system show nat-state** command displays the enable/disable state of NAT/load balancing on RS modules.

Restrictions

None.

Example

To display the NAT/load balancing enable/disable state:

rs# system show nat-state	
Module	NAT/LSNAT state
-----	-----
3	Enabled
5	Enabled
10	Enabled
12	Enabled
14	Enabled

system show poweron-selftest-mode

Mode

Enable

Format

system show poweron-selftest-mode

Description

The **system show poweron-selftest-mode** command displays the type of Power-On Self Test (POST) that is performed at bootup.

Restrictions

None.

Example

To display the self test mode:

```
rs# system show poweron-selftest-mode
%SYS-I-POST, Power-On Self Test mode: quick
rs#
```

system show scratchpad

Mode

Enable

Format

system show scratchpad

Description

The **system show scratchpad** command displays the configuration changes in the scratchpad that have not yet been activated.

Restrictions

None.

Example

To display the contents of the scratchpad:

```
rs# system show scratchpad

***** Non-committed changes in Scratchpad *****
1*: vlan add ports et.3.1 to vlan1
rs#
```

system show serial-number

Mode

Enable

Format

system show serial-number

Description

The **system show serial-number** command displays the serial number of the Control Module.

Restrictions

None.

Example

To display a serial number:

```
rs2100# system show serial-number  
Primary   CM serial number id is 7233b90e000000b4
```

system show ssh-access

Mode

Enable

Format

system show ssh-access

Description

The **system show ssh-access** command displays the last five secure shell (SSH) connections to the RS.

Restrictions

None.

Example

To display SSH access:

```
rs# system show ssh-access
SSHD Last 5 Clients:
      123.152.165.215 2000-06-07 12:07:01
      123.152.165.213 2000-06-07 13:15:13
      123.152.165.213 2000-06-07 14:48:55
      123.152.165.215 2000-06-06 17:06:07
      123.152.165.213 2000-06-07 09:20:54
rs#
```

system show startup-config

Mode

Enable

Format

system show startup-config

Description

The **system show startup-config** command displays the contents of the startup configuration file.

Restrictions

None.

Example

To display the startup configuration file:

```
rs# system show startup-config
!
! Startup configuration for the next system reboot
!
! Last modified from Telnet (123.111.121.143) on 2000-06-07 15:14:57
!
version 4.1
atm create vcgroup et.2.1 slot 2
atm set vcgroup port et.3.2 forced-bridged
vlan make trunk-port et.2.1
vlan make trunk-port et.3.1
vlan create trunk1 port-based
vlan create trunk2 port-based
vlan create trunk3 ip
vlan create ipx1 ipx
vlan create blue bridged-protocols
vlan add ports et.2.1 to trunk3
vlan add ports et.2.2 to trunk3
vlan add ports et.3.2 to trunk3
vlan add ports et.3.3 to trunk3
vlan add ports et.2.1 to trunk2
vlan add ports et.2.2 to trunk2
vlan add ports et.2.3 to trunk2
system set idle-timeout serial 5 telnet 5
rs#
```

system show syslog

Mode

Enable

Format

system show syslog

Description

The **system show syslog** command displays the IP address or hostname of Syslog server and the Syslog message level.

Restrictions

None.

Example

To display information about the syslog servers:

```
rs# system show syslog  
Syslog host: 123.122.143.137, Facility: LOG_LOCAL0  
Minimum syslog level: INFO, Buffer Size: 10 messages  
Source IP address: none configured  
rs#
```

system show syslog buffer

Mode

Enable

Format

system show syslog buffer

Description

The **system show syslog buffer** command displays the messages in the Syslog message buffer.

Restrictions

None.

Example

To display information about the Syslog buffers:

```
rs# system show syslog buffer
2000-06-08 10:26:39 <132>Jun 08 10:26:39 %SYS-W-NOPASSWD, no password
for enable
, use 'system set password' in Config mode
2000-06-08 10:26:35 <132>Jun 08 10:26:35 %SYS-W-NOPASSWD, no password
for login,
  use 'system set password' in Config mode
2000-06-08 09:47:38 <131>Jun 08 09:47:38 %SNMP-E-TRAP, send trap pdu to
host "123.122.167.132" failed : No route to host
2000-06-08 09:45:30 <131>Jun 08 09:45:30 %SNMP-E-TRAP, send trap pdu to
host "123.133.167.132" failed : No route to host
2000-06-08 09:43:22 <131>Jun 08 09:43:22 %SNMP-E-TRAP, send trap pdu to
host "123.122.167.132" failed : No route to host
2000-06-08 09:41:14 <131>Jun 08 09:41:14 %SNMP-E-TRAP, send trap pdu to
host "123.122.167.132" failed : No route to host
2000-06-07 09:33:45 <132>Jun 07 09:33:45 %SYS-W-NOPASSWD, no password
for login,use 'system set password' in Config mode
rs#
```


system show telnet-access

Mode

Enable

Format

system show telnet-access

Description

The **system show telnet-access** command displays the last five telnet connections to the RS.

Restrictions

None.

Example

To display telnet access:

```
rs# system show telnet-access
TELNETD Last 5 Clients:
      123.152.165.215 2000-06-07 12:07:01
      123.152.165.213 2000-06-07 13:15:13
      123.152.165.213 2000-06-07 14:48:55
      123.152.165.215 2000-06-06 17:06:07
      123.152.165.213 2000-06-07 09:20:54
rs#
```

system show terminal

Mode

Enable

Format

system show terminal

Description

The **system show terminal** command displays the default terminal settings:

- Number of rows
- Number of columns
- Baud rate

Restrictions

None.

Example

To display terminal settings:

```
rs# system show terminal

System default terminal settings (console & telnet):
  Number of rows      : 24
  Number of columns   : 80

Terminal settings for current login session
  Number of rows      : 24
  Number of columns   : 80

Console baud rate     : 0
rs#
```

system show timezone

Mode

Enable

Format

system show timezone

Description

The **system show timezone** command displays the timezone offset from UCT in minutes.

Restrictions

None.

Example

To display time zone settings:

```
rs# system show timezone  
Daylight saving = OFF  
UCT Time offset = 0 hours 0 minutes  
rs#
```

system show uptime

Mode

Enable

Format

system show uptime

Description

The **system show uptime** command displays the time that has elapsed since the RS was rebooted, and the system time and date when the last reboot occurred.

Restrictions

None.

Example

To display the uptime:

```
rs# system show uptime
System started 2000-06-06 11:07:20
System up 1 day, 5 hours, 48 minutes, 15 seconds.
rs#
```

system show users

Mode
Enable

Format

system show users

Description

The **system show users** command displays the current Console, telnet, and secure shell (SSH) connections.

Restrictions

None.

Example

To display the current users:

rs# system show users
Current Terminal User List:

1	2	3	4	5
##	Login ID	Mode	From	Login Timestamp
--	-----	----	----	-----
	guest	enabled	console	2000-09-26 18:10:49
0T		enabled	134.141.173.224	2000-10-01 21:57:41
1S		configuration	134.141.173.226	2000-10-01 21:58:02

- Legend:
- 1. Session ID. T indicates a Telnet session. S indicates an SSH session.
 - 2. The login ID of the session user.
 - 3. The current CLI command mode for this user.
 - 4. The address from which the session originated.
 - 5. The time that this user logged in to the RS.

system show version

Mode

Enable

Format

system show version

Description

The **system show version** command displays the software version running on the RS.

Restrictions

None.

Example

To display the software version:

```
rs# system show version
Software Information
  Software Version   : 4.1.
  Copyright          : Copyright (c) 1998-2000 Riverstone Networks, Inc.
  Image Information  : Version 4.1, built on Mon Jun  5 10:42:23 2000
  Image Boot Location: file:/pc-flash/boot/img
  Boot Prom Version  : prom-1.1.0.8
rs#
```

75 TACACS COMMANDS

The **tacacs** commands let you secure access to the RS using the Terminal Access Controller Access Control System (TACACS) protocol. When TACACS authentication is activated on the RS, the user is prompted for a password when he or she tries to access Enable mode. The RS queries a TACACS server to see if the password is valid. If the password is valid, the user is granted access to Enable mode.

75.1 COMMAND SUMMARY

The following table lists the **tacacs** commands. The sections following the table describe the command syntax.

tacacs enable
tacacs set last-resort password succeed
tacacs set server <IPaddr>
tacacs set timeout <number>
tacacs show stats all

tacacs enable

Mode

Configure

Format

tacacs enable

Description

The **tacacs enable** command starts TACACS authentication on the RS. TACACS authentication is disabled by default on the RS. When you issue this command, the TACACS-related parameters set with **tacacs set** commands become active.

Restrictions

None.

Example

The following commands set TACACS-related parameters on the RS. The commands are then activated with the **tacacs enable** command:

```
rs(config)# tacacs set host 207.135.89.15
rs(config)# tacacs set timeout 30
rs(config)# tacacs enable
```


tacacs set last-resort

Mode

Configure

Format

tacacs set last-resort password|succeed

Description

The **tacacs set last-resort** command allows you to define the action to take if a TACACS server does not reply within the time specified by the **tacacs set timeout** parameter.

Parameter	Value	Meaning
last-resort	password	The user is prompted for the Enable mode password set with system set password command (if one exists).
	succeed	Access to the RS is granted.

Restrictions

None.

Example

The following commands specify that if a response from a TACACS server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the RS **system set password** command.

```
rs(config)# tacacs set timeout 30
rs(config)# tacacs set last-resort password
```

tacacs set server

Mode

Configure

Format

tacacs set server <IPaddr>

Description

The **tacacs set sever** command allows you to set the IP address of a TACACS server. You can enter up to five TACACS servers. Enter one server per **tacacs set server** command

Parameter	Value	Meaning
server	<IPaddr>	The IP address of a TACACS server.

Restrictions

None.

Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are TACACS servers.

```
rs(config)# tacacs set server 137.72.5.9
rs(config)# tacacs set server 137.72.5.41
```

tacacs set timeout

Mode

Configure

Format

tacacs set timeout *<number>*

Description

The **tacacs set timeout** command allows you to set the maximum time, in seconds, to wait for a TACACS server to reply. The default is 3 seconds.

Parameter	Value	Meaning
timeout	<i><number></i>	The maximum time (in seconds) to wait for a TACACS server to reply.

Restrictions

None.

Example

The following command specifies that the RS should wait no more than 30 seconds for a response from one of the TACACS servers. If a response from a TACACS server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the RS **system set password** command.

```
rs(config)# tacacs set timeout 30
rs(config)# tacacs set last-resort password
```

tacacs show

Mode

Enable

Format

```
tacacs show stats|all
```

Description

The **tacacs show** command displays statistics and configuration parameters related to the TACACS configuration on the RS. The statistics displayed include:

- **accepts:** Number of times each server responded and validated the user successfully.
- **rejects:** Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied.
- **timeouts:** Number of times each server did not respond.

Parameter	Value	Meaning
stats		Displays the number of accepts, rejects, and timeouts for each TACACS server.
all		Displays the configuration parameters set with the tacacs set command, in addition to the number of accepts, rejects, and timeouts for each TACACS server.

Restrictions

None.

Example

To display configuration parameters and TACACS server statistics:

```
rs# tacacs show all
```

76 TACACS-PLUS COMMANDS

The **tacacs-plus** commands let you secure access to the RS using the TACACS+ protocol. When a user logs in to the RS or tries to access Enable mode, he or she is prompted for a password. If TACACS+ authentication is enabled on the RS, it will contact a TACACS+ server to verify the user. If the user is verified, he or she is granted access to the RS.



Note The RS currently supports the Password Authentication Protocol (PAP) method of authentication but not the Challenge Handshake Authentication Protocol (CHAP) method.

76.1 COMMAND SUMMARY

The following table lists the **tacacs-plus** commands. The sections following the table describe the command syntax.

tacacs-plus accounting command level <i><level></i>
tacacs-plus accounting shell start stop all
tacacs-plus accounting snmp active startup
tacacs-plus accounting system fatal error warning info
tacacs-plus authentication login enable system
tacacs-plus enable
tacacs-plus set deadline <i><minutes></i>
tacacs-plus set key <i><string></i>
tacacs-plus set last-resort password succeed deny
tacacs-plus set retries <i><number></i>
tacacs-plus set server <i><IPaddr></i>
tacacs-plus set single-connect
tacacs-plus set source <i><ipaddr></i> <i><interface></i>
tacacs-plus set timeout <i><seconds></i>
tacacs-plus show stats all

tacacs-plus accounting command level

Mode

Configure

Format

tacacs-plus accounting command level *<level>*

Description

The **tacacs-plus accounting command level** command allows you specify the types of commands that are logged to the TACACS+ server. The user ID and timestamp are also logged.

Parameter	Value	Meaning
level	<i><level></i>	Specifies the type(s) of commands that are logged to the TACACS+ server.
	5	Log Configure commands.
	10	Log all Configure and Enable commands.
	15	Log all Configure, Enable, and User commands.

Restrictions

None.

Example

To cause Configure, Enable, and User mode commands to be logged on the TACACS+ server:

```
rs(config)# tacacs-plus accounting command level 15
```

tacacs-plus accounting shell

Mode

Configure

Format

tacacs-plus accounting shell start|stop|all

Description

The **tacacs-plus accounting shell** command allows you to track shell usage on the RS. It causes an entry to be logged on the TACACS+ server when a shell is started or stopped. You can specify that an entry be logged when a shell is started, when a shell is stopped, or when a shell is either started or stopped.

Parameter	Value	Meaning
shell	start	Logs an entry when a shell is started.
	stop	Logs an entry when a shell is stopped
	all	Logs an entry when a shell is either started or stopped

Restrictions

None.

Example

To cause an entry to be logged on the TACACS+ server when a shell is either started or stopped on the RS:

```
rs(config)# tacacs-plus accounting shell all
```

tacacs-plus accounting snmp

Mode

Configure

Format

```
tacacs-plus accounting snmp active|startup
```

Description

The **tacacs-plus accounting snmp** command allows you to track changes made to the active or startup configuration through SNMP. It causes an entry to be logged on the TACACS+ server whenever a change is made to the ACL configuration. You can specify that an entry be logged to the active or startup configuration.

Parameter	Value	Meaning
snmp	active	Logs an entry when a change is made to the active configuration.
	startup	Logs an entry when a change is made to the startup configuration.

Restrictions

None.

Example

To cause an entry to be logged on the TACACS+ server whenever an ACL configuration change is made via SNMP to the active configuration:

```
rs(config)# tacacs-plus accounting snmp active
```


tacacs-plus accounting system

Mode

Configure

Format

tacacs-plus accounting system fatal|error|warning|info

Description

The **tacacs-plus accounting system** command allows you to specify the types of messages that are logged on the TACACS+ server.

Parameter	Value	Meaning
system	fatal	Logs only fatal messages.
	error	Logs fatal messages and error messages.
	warning	Logs fatal messages, error messages, and warning messages.
	info	Logs all messages, including informational messages.

Restrictions

None.

Example

To log only fatal and error messages on the TACACS+ server:

```
rs(config)# tacacs-plus accounting system error
```

tacacs-plus authentication

Mode

Configure

Format

tacacs-plus authentication login|enable|system

Description

The **tacacs-plus authentication** command allows you to specify when TACACS+ authentication is performed: either when a user logs in to the RS, or tries to access Enable mode.

Parameter	Value	Meaning
authentication	login	Authenticates users at the RS login prompt.
	enable	Authenticates users when they try to access Enable mode.
	system	Authenticates \$enab<n>\$ user when they try to access Enable mode.

Restrictions

None.

Example

To perform TACACS+ authentication at the RS login prompt:

```
rs(config)# tacacs-plus authentication login
```

tacacs-plus enable

Mode

Configure

Format

tacacs-plus enable

Description

TACACS+ authentication is disabled by default on the RS. The **tacacs-plus enable** command causes TACACS+ authentication to be activated on the RS. You set TACACS+-related parameters with the **tacacs-plus set**, **tacacs-plus accounting shell**, and **tacacs-plus authorization** commands, then use the **tacacs-plus enable** command to activate TACACS+ authentication.

Restrictions

None.

Example

The following commands set TACACS+-related parameters on the RS. The commands are then activated with the **tacacs-plus enable** command:

```
rs(config)# tacacs-plus set server 207.135.89.15
rs(config)# tacacs-plus set timeout 30
rs(config)# tacacs-plus authentication login
rs(config)# tacacs-plus accounting shell all
rs(config)# tacacs-plus enable
```

tacacs-plus set deadtime

Mode

Configure

Format

tacacs-plus set deadtime *<minutes>*

Description

The **tacacs-plus set deadtime** command allows you to set the length of time that a TACACS+ server is ignored after it has failed. This command sets a global value that is applicable to all configured TACACS+ servers. You can set a deadtime value for a specific server with the **tacacs-plus set server** command.



Note The deadtime value set for a specific server with the **tacacs-plus set server** command takes precedence over the value specified with the **tacacs-plus set deadtime** command.

Parameter	Value	Meaning
deadtime	<i><minutes></i>	Number of minutes that any TACACS+ server is ignored after it has failed. Specify a value between 0 and 1440. The default is 0 minutes.

Restrictions

None.

Example

The following commands configure three TACACS+ servers. The RS will ignore hosts 137.72.5.41 and 137.72.5.25 for 10 minutes if either server fails, and it will ignore host 137.72.5.9 for 2 minutes if that server fails.

```
rs(config)# tacacs-plus set server 137.72.5.9 deadtime 2
rs(config)# tacacs-plus set server 137.72.5.41
rs(config)# tacacs-plus set server 137.72.5.25
rs(config)# tacacs-plus set deadtime 10
```

tacacs-plus set key

Mode

Configure

Format

tacacs-plus set key <string>

Description

The **tacacs-plus set key** command allows you to set the authentication key for TACACS+ servers. This command sets a global key that is applicable to all configured TACACS+ servers. You can set a key for a specific server with the **tacacs-plus set server** command.



Note The key set for a specific server with the **tacacs-plus set server** command takes precedence over the key specified with the **tacacs-plus set key** command.

Parameter	Value	Meaning
key	<string>	Authentication key to be shared with a configured TACACS+ server. Specify a string up to 128 characters.

Restrictions

None.

Example

The following commands configure three TACACS+ servers. The RS will use the authentication key 'pome4' for hosts 137.72.5.41 and 137.72.5.25, and the key 'b456' for host 137.72.5.9.

```
rs(config)# tacacs-plus set server 137.72.5.9 key b456
rs(config)# tacacs-plus set server 137.72.5.41
rs(config)# tacacs-plus set server 137.72.5.25
rs(config)# tacacs-plus set key pome4
```

tacacs-plus set last-resort

Mode

Configure

Format

```
tacacs-plus set last-resort password|succeed |deny
```

Description

The **tacacs-plus set last-resort** command allows you to specify what the RS does if the TACACS+ server does not reply by a given time. If this command is not specified, the RS tries the next configured authentication method (including RADIUS configuration commands). Otherwise, if the TACACS+ server does not reply within the configured timeout period for the configured number of retries, user authentication will fail.

Parameter	Value	Meaning
last-resort		The action to take if a TACACS+ server does not reply within the configured timeout for the configured number of retries.
	password	The password set with system set password command is used. This keyword is <i>recommended</i> for optimal security, however, note that you must set a password with the system set password command.
	succeed	Access to the RS is granted.
	deny	Access to the RS is denied.

Restrictions

None.

Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are TACACS+ servers, and the RS should wait no more than 30 seconds for a response from one of these servers. If a response from a TACACS+ server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the RS **system set password** command.

```
rs(config)# tacacs-plus set server 137.72.5.9
rs(config)# tacacs-plus set server 137.72.5.41
rs(config)# tacacs-plus set timeout 30
rs(config)# tacacs-plus set retries 1
rs(config)# tacacs-plus set last-resort password
```

tacacs-plus set retries

Mode

Configure

Format

tacacs-plus set retries *<number>*

Description

The **tacacs-plus set retries** command allows you to set the maximum number of times that the RS will try to contact a TACACS+ server for authentication. This command sets a global value that is applicable to all configured TACACS+ servers. You can set a retries value for a specific server with the **tacacs-plus set server** command.



Note The retries value set for a specific server with the **tacacs-plus set server** command takes precedence over the retries specified with the **tacacs-plus set retries** command.

Parameter	Value	Meaning
retries	<i><number></i>	The maximum number of times that the RS will try to contact a TACACS+ server. Specify a value between 1 and 10. The default is 3 times.

Restrictions

None.

Example

The following commands configure three TACACS+ servers. The RS will try up to four times for a response from hosts 137.72.5.41 and 137.72.5.25, but will try up to six times for a response from host 137.72.5.9.

```
rs(config)# tacacs-plus set server 137.72.5.9 retries 6
rs(config)# tacacs-plus set server 137.72.5.41
rs(config)# tacacs-plus set server 137.72.5.25
rs(config)# tacacs-plus set retries 4
```

tacacs-plus set server

Mode

Configure

Format

```
tacacs-plus set server <IPaddr> [port <port-no>] [timeout <seconds>] [retries <number>]
[deadtime <minutes>] [key <string>] [source <ipaddr> | <interface>]
```

Description

The **tacacs-plus set server** command allows you to identify a TACACS+ server and configure parameters for the server. These parameters include the port number for accounting and authentication, how long to wait for the server to authenticate the user, and number of times to try contacting the server for authentication. You can configure up to five TACACS+ servers for use with the RS. Specify one server per **tacacs-plus set server** command.

Parameter	Value	Meaning
server	<IPaddr>	Is the IP address of a TACACS+ server.
port	<port-no>	Port number to use for this TACACS+ server. Specify a value between 1-65535. The default is port 49.
timeout	<seconds>	The maximum time (in seconds) to wait for this TACACS+ server to reply. Specify a value between 1-30. If this parameter is not defined, the global timeout value defined with the tacacs-plus set timeout command is used. If a tacacs-plus set timeout value is not configured, the default is 3 seconds.
retries	<number>	The number of times to try contacting this TACACS+ server. Specify a value between 1-10. If this parameter is not defined, the global retries value defined with the tacacs-plus set retries value is used. If a tacacs-plus set retries value is not configured, the defaults is 3 times.
deadtime	<minutes>	Number of minutes that this TACACS+ server is ignored after it has failed. Specify a value between 0-1440. If this parameter is not defined, the global deadtime value defined with the tacacs-plus set deadtime command is used. If a tacacs-plus set deadtime value is not configured, the default is 0 minutes.
key	<string>	Authentication key to be shared with this TACACS+ server. Specify a string up to 128 characters. If this parameter is not defined, the global key defined with the tacacs-plus set key command is used.
source	<ipaddr>	IP address to use with this server.
	<interface>	Name of interface to use with this server.

Restrictions

None.

Example

The following commands configure hosts 137.72.5.9 and 137.72.5.41 as TACACS+ servers, each with different operating parameters.

```
rs(config)# tacacs-plus set server 137.72.5.9 timeout 30 retries 4
rs(config)# tacacs-plus set server 137.72.5.41 timeout 20 retries 6
deadtime 5
```

tacacs-plus set single-connect

Mode

Configure

Format

```
tacacs-plus set single-connect
```

Description

When a user logs onto the RS, it opens a TCP connection to the TACACS+ server, sends the authentication request and closes the connection after it receives a response. The **tacacs-plus set single-connect** command enables the RS to keep the TCP connection open so the RS can continue to send authorization or accounting requests to the TACACS+ server without having to re-open the TCP connection with each request.

Restrictions

None

tacacs-plus set source

Mode

Configure

Format

tacacs-plus set source <ipaddr> | <interface>

Description

The **tacacs-plus set source** command allows you to set a source IP address or interface to use with a TACACS+ server. This command sets a global value that is applicable to all configured TACACS+ servers. You can set a source value for a specific server with the **tacacs-plus set server** command.



Note The source value set for a specific server with the **tacacs-plus set server** command takes precedence over the source specified with the **tacacs-plus set source** command.

Parameter	Value	Meaning
source	<ipaddr> <interface>	IP address or the name of the interface to use with the TACACS+ server.

Restrictions

None.

Example

The following commands configure three TACACS+ servers. The RS will use the IP address 101.100.100.102 for hosts 137.72.5.41 and 137.72.5.25, but will use 10.10.10.10 for host 137.72.5.9.

```
rs(config)# tacacs-plus set server 137.72.5.9 source 10.10.10.10
rs(config)# tacacs-plus set server 137.72.5.41
rs(config)# tacacs-plus set server 137.72.5.25
rs(config)# tacacs-plus set source 101.100.100.102
```

tacacs-plus set timeout

Mode

Configure

Format

tacacs-plus set timeout *<seconds>*

Description

The **tacacs-plus set timeout** command allows you to set how long to wait for the TACACS+ server to respond to client requests. This command sets a global value that is applicable to all configured TACACS+ servers. You can set a timeout value for a specific server with the **tacacs-plus set server** command.

 **Note** The timeout value set for a specific server with the **tacacs-plus set server** command takes precedence over the timeout specified with the **tacacs-plus set timeout** command.

Parameter	Value	Meaning
timeout	<i><seconds></i>	The maximum time (in seconds) to wait for a TACACS+ server to reply. Specify a value between 1 and 30. The default is 3 seconds.

Restrictions

None.

Example

The following commands configure three TACACS+ servers. The RS will wait no more than 10 seconds for a response from hosts 137.72.5.41 and 137.72.5.25, but will wait up to 30 seconds for a response from host 137.72.5.9.

```
rs(config)# tacacs-plus set server 137.72.5.9 timeout 30
rs(config)# tacacs-plus set server 137.72.5.41
rs(config)# tacacs-plus set server 137.72.5.25
rs(config)# tacacs-plus set timeout 10
```

tacacs-plus show

Mode

Enable

Format

tacacs-plus show stats|all

Description

The **tacacs-plus show** command displays statistics and configuration parameters related to TACACS+ configuration on the RS. The statistics displayed include:

- **accepts:** Number of times each server responded and validated the user successfully.
- **rejects:** Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied.
- **timeouts:** Number of times each server did not respond.

Parameter	Value	Meaning
show	stats	Displays the accepts, rejects, and timeouts for each TACACS+ server.
	all	Displays the configuration parameters set with the tacacs-plus set command, in addition to the accepts, rejects, and timeouts for each TACACS+ server.

Restrictions

None.

Example

To display configuration parameters and TACACS+ server statistics:

```
rs# tacacs-plus show all
TACACS+ status: ACTIVE 1
TACACS+ last resort: Deny access when server fails 2
Default TACACS+ timeout (seconds): 3 3
Default TACACS+ retries: 4 4
Default TACACS+ deadtime (minutes): 5 5
Default TACACS+ source IP address: Let system decide 6 6

TACACS+ servers listed in order of priority:

Server: 10.50.7 7
Port: 4949
Timeout (seconds): 30
Retries: 1
Deadtime (minutes): 60
Source IP: <Default>

Server: 192.168.1.78
Port: 49
Timeout (seconds): <Default>
Retries: <Default>
Deadtime (minutes): <Default>
Source IP: <Default>

Server: 192.168.2.33
Port: 49
Timeout (seconds): <Default>
Retries: <Default>
Deadtime (minutes): <Default>
Source IP: <Default>

TACACS+ server statistics:

8      9      10     11
Host    Accepts  Rejects  Timeouts
10.50.7.45    0        0        0
192.168.1.78  0        0        0
192.168.2.33  0        0        0
```

Legend:

1. Shows “ACTIVE” if TACACS+ has been enabled with the **tacacs-plus enable** command.
2. Action to be taken if there is no response from the TACACS+ server, as configured with the **tacacs-plus set last-resort** command. If this command is not configured, the action shown is “None set.”
3. Value set with the **tacacs-plus set timeout** command. Default is 3 seconds.
4. Value set with the **tacacs-plus set retries** command. Default is 3 retries.
5. Value set with the **tacacs-plus set deadtime** command. Default is 0 minutes.

6. IP address set with the **tacacs-plus set source** command. “Let system decide” means that no source IP address is configured with this command and the RS performs a lookup in its routing table to set the source IP address for client requests.
7. Shows server-specific parameter values for each configured TACACS+ server. Server-specific parameters are configured with the **tacacs-plus set server** command. “<Default>” means that the default value is used for the parameter.
8. IP address of TACACS+ server.
9. Number of times server responded and successfully validated the user.
10. Number of times server responded and denied the user access, either because the user was not known or the wrong password was supplied.
11. Number of times server did not respond before the timeout expired.

77 TELNET COMMAND

telnet

Mode

User or Enable

Format

telnet <hostname-or-IPaddr> [socket <socket-number>]

Description

The telnet command allows you to open a Telnet session to the specified host.

Parameter	Value	Meaning
telnet	<hostname-or-IPaddr>	The host name or IP address of the remote computer that you want to access.
socket	<socket-number>	The TCP port through which the Telnet session will be opened. If this parameter is not specified, the Telnet port (socket number 23) is assumed. This parameter can be used to test other ports; for example, socket number 21 is the port for FTP.

Restrictions

None.

Example

To open a Telnet session on the host “rs4”:

```
rs# telnet rs4
```


78 TRACEROUTE COMMAND

The **traceroute** command traces the path a packet takes to reach a remote host.

Format

```
traceroute <host> [max-ttl <num>] [probes <num>] [size <num>] [source <host>] [tos <num>] [wait-time <secs>] [verbose] [noroute]
```

Mode

User

Description

The **traceroute** command traces the route taken by a packet to reach a remote IP host. The **traceroute** command examines the route taken by a packet traveling from a source to a destination. By default, the source of the packet is the RS. However, one can specify a different source and track the route between it and a destination. The route is calculated by initially sending a probe (packet) from the source to the destination with a TTL of 1. Each intermediate router that is not able to reach the final destination directly will send back an ICMP Time Exceeded message. Subsequent probes from the source will increase the TTL value by 1. As each Time Exceeded message is received, the program keeps track of the address of each intermediate gateway. The probing stops when the packet reaches the destination or the TTL exceeds the **max-ttl** value.

Parameter	Value	Meaning
	<host>	Hostname or IP address of the destination
max-ttl	<num>	Maximum number of gateways (“hops”) to trace
probes	<num>	Number of probes to send
size	<num>	Packet size of each probe
source	<host>	Hostname or IP address of the source
tos	<num>	Type of Service value in the probe packet
wait-time	<secs>	Maximum time to wait for a response

Parameter	Value	Meaning
verbose		Displays results in verbose mode
noroute		Ignores the routing table and sends a probe to a host on a directly attached network. If the destination is not on the local network, an error is returned.

Restrictions

None.

Example

To display the route from the RS to the host *othello* in verbose mode:

```
rs# traceroute othello verbose
```

79 VLAN COMMANDS

The vlan commands let you perform the following tasks:

- Create VLANs
- List VLANs
- Add ports to VLANs
- Specify ports that cannot be added to a specific VLAN
- Change the port membership of VLANs
- Make a VLAN port either a trunk port, an access port, or a metropolitan area network (MAN) tunnel port

79.1 COMMAND SUMMARY

The following table lists the vlan commands. The sections following the table describe the command syntax.

<code>vlan add ports <port-list> to <vlan-name></code>
<code>vlan create <vlan-name> <type> id <num></code>
<code>vlan enable l4-bridging on <vlan-name></code>
<code>vlan enable stackable-vlan on <port-list> backbone-vlan <vlan-name></code>
<code>vlan forbid ports <port-list> from <vlan-name></code>
<code>vlan make access-port <port-list> [stackable-vlan]</code>
<code>vlan make trunk-port <port-list> [stackable-vlan] [exclude-default-vlan] [untagged]</code>
<code>vlan show [stackable-vlan]</code>

vlan add ports

Mode

Configure

Format

```
vlan add ports <port-list> to <vlan-name>
```

Description

The **vlan add ports** command adds ports to an existing VLAN. You do not need to specify the VLAN type when you add ports. You specify the VLAN type when you create the VLAN (using the **vlan create** command).

Parameter	Value	Meaning
ports	<port-list>	The ports you are adding to the VLAN. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8)
to	<vlan-name>	Name of the VLAN to which you are adding ports.

Restrictions

The VLAN to which you add ports must already exist. To create a VLAN, use the **vlan create** command. An access port can be added to only one IP VLAN, one IPX VLAN, and one bridged-protocols VLAN.

The ATM modules do not support Spanning Tree Protocol. Take precautions to not create loops into the VLAN.

vlan create

Mode

Configure

Format

```

vlan create <vlan-name> <type> id <num>

```

Description

The **vlan create** command creates a VLAN definition. You can create a port-based VLAN or a protocol-based VLAN.

Parameter	Value	Meaning
create	<vlan-name>	The VLAN name is a string up to 32 characters long. The VLAN name cannot begin with an underscore (_) or the word “SYS_”. The names “control”, “default”, “blackhole”, “reserved”, and “learning” cannot be used.
	<type>	The type of VLAN you are adding. The VLAN type determines the types of traffic the RS will forward on the VLAN. Specify any combination of the first seven types that follow or specify port-based .
	ip	Create this VLAN for IP traffic
	ipx	Create this VLAN for IPX traffic
	appletalk	Create this VLAN for AppleTalk traffic
	dec	Create this VLAN for DECnet traffic
	sna	Create this VLAN for SNA traffic
	ipv6	Create this VLAN for IPv6 traffic
	bridged-protocols	Create this VLAN for extended VLAN types (DEC, SNA, Appletalk, IPv6), and non-IP and non-IPX protocols
	port-based	Create this VLAN for all the traffic types listed above (port-based VLAN)
id	<num>	ID of this VLAN. The ID must be unique. You can specify a number from 2 – 4094. If more than one RS will be configured with the same VLAN, you must specify the same VLAN ID on each RS.



Note You can specify a combination of **ip**, **ipx**, **appletalk**, **dec**, **sna**, **ipv6**, and **bridged-protocols**. If you specify *any* of the extended VLAN types (**sna**, **dec**, **appletalk**, **ipv6**) with the **bridged-protocols** option, then all the other extended VLAN types are removed from the VLAN. See the following table:

Configuration Command	Protocols Included in VLAN	Protocols Excluded from VLAN
<code>vlan create <vlan-name> ip</code>	IP	IPX, SNA, IPv6, DECnet, Appletalk, Other
<code>vlan create <vlan-name> ip bridged-protocols</code>	IP, SNA, DECnet, IPv6, Appletalk, Other	IPX
<code>vlan create <vlan-name> ip bridged-protocols sna</code>	IP, SNA, Other	IPX, IPv6, DECnet, Appletalk
<code>vlan create <vlan-name> ip bridged-protocols sna ipv6</code>	IP, SNA, IPv6, Other	IPX, DECnet, Appletalk



Note You can specify a combination of **ip**, **ipx**, **appletalk**, **dec**, **sna**, **ipv6**, and **bridged-protocols** or you can specify **port-based**; you cannot specify **port-based** with any of the other options.

Restrictions

The following *cannot* be used for VLAN names:

- control
- default
- blackhole
- reserved
- learning
- names starting with an underscore (_) or “sys_”



Note Specify both **sna** and **bridged-protocols** to successfully create an SNA based VLAN. The SNA-protocol-based VLAN (implemented in version 3.0 and later) needs to be configured with the following command:
vlan create sna bridged-protocols id <id#>
 in order to forward all SNA protocol types. Refer to the following Technical Bulletin for more detail: TB0973-1

Examples

The following command creates a VLAN 'blue' for IP, SNA, non-IPX, non-DECnet, non-Appletalk, non-IPv6 protocols.:

```
rs(config)# vlan create blue ip bridged-protocols sna
```

The following command creates a VLAN 'red' for IP, non-IPX, and extended VLAN types SNA, DECnet, Appletalk, and IPv6:

```
rs(config)# vlan create red ip bridged-protocols
```

vlan enable l4-bridging

Mode

Configure

Format

```
 vlan enable l4-bridging on <vlan-name>
```

Description

The **vlan enable l4-bridging** command allows you to enable Layer-4 bridging. Layer-4 bridging can be enabled on VLANs that support only IP traffic or only IPX traffic.

Parameter	Value	Meaning
on	<vlan-name>	The name of the VLAN on which Layer-4 bridging will be enabled.

Restrictions

You cannot enable L4 bridging on VLAN ports that are already mapped to backbone VLANs, and vice versa. That is, you cannot use the **vlan enable stackable-vlans** command on any port that is part of a VLAN on which the **vlan enable l4-bridging** command has already been issued. Conversely, you cannot use the **vlan enable l4-bridging** command on any VLAN whose ports are already specified with the **vlan enable stackable-vlans** command.

vlan enable stackable-vlan

Mode

Configure

Format

```
vlan enable stackable-vlan on <port-list> backbone-vlan <vlan-name>
```

Description

The **vlan enable stackable-vlan** command allows you to map VLAN access ports to a backbone VLAN. This allows traffic on the access ports to be switched through a MAN on the backbone VLAN.

Parameter	Value	Meaning
on	<port-list>	The ports you are mapping to the backbone VLAN. You can specify a single port of a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8)
backbone-vlan	<vlan-name>	The name of the VLAN on which VLAN packets will be tunneled through the MAN. The port(s) in the backbone VLAN must be designated as tunnel backbone ports with the stackable-vlan parameter of the vlan make trunk-port command.

Restrictions

You can specify only one backbone VLAN per input port. The VLAN access ports that are to be mapped to the backbone VLAN must receive packets with 802.1q tags.

You cannot enable L4 bridging on VLAN ports that are already mapped to backbone VLANs, and vice versa. That is, you cannot use the **vlan enable stackable-vlans** command on any port that is part of a VLAN on which the **vlan enable l4-bridging** command has already been issued. Conversely, you cannot use the **vlan enable l4-bridging** command on any VLAN whose ports are already specified with the **vlan enable stackable-vlans** command.

vlan forbid ports

Mode

Configure

Format

```
vlan forbid ports <port-list> from <vlan-name>
```

Description

The **vlan forbid ports** command allows you to specify those ports which are *not* to be added to a VLAN.



Note

This command prevents the specified port from being added to a VLAN, either through the CLI **vlan add ports** command or through a facility such as the GARP VLAN Registration Protocol (GVRP), which allows dynamic VLAN creation.

Parameter	Value	Meaning
ports	<port-list>	The ports that should not be added to the VLAN. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8)
to	<vlan-name>	Name of the VLAN to which the ports should not be added.

Restrictions

None.

vlan make access-port

Mode

Configure

Format

```
vlan make access-port <port-list> [stackable-vlan]
```

Description

The **vlan make access-port** command turns a port into a VLAN access port. The port will forward traffic only for the VLANs to which you have added the ports and the traffic will be untagged. This is the default.

Parameter	Value	Meaning
access-port	<port-list>	The ports you are configuring. You can specify a single port or a comma-separated list of ports. Example: et . 1 . 3 , et . (1 - 3) . (4 , 6 - 8) .
stackable-vlan		Specifies that this port is a tunnel entry or exit port for traffic to be tunneled on a stackable VLAN. This parameter allows the port to belong to more than one VLAN of the same protocol type. If this parameter is not specified, the access port can only belong to one VLAN of a particular protocol type.

Restrictions

None.

vlan make trunk-port

Mode

Configure

Format

```
vlan make trunk-port <port-list> [stackable-vlan] [exclude-default-vlan] [untagged]
```

Description

The **vlan make trunk-port** command turns a port into a VLAN trunk port. A VLAN trunk port can forward traffic for multiple VLANs. Use trunk ports when you want to connect RS switches together and send traffic for multiple VLANs on a single network segment connecting the switches. Specify the **stackable-vlan** option to designate this trunk port as a tunnel backbone port on which VLAN packets will be tunneled through the metropolitan area network (MAN).

Parameter	Value	Meaning
trunk-port	<port-list>	The ports you are configuring. You can specify a single port or a comma-separated list of ports. Example: et . 1.3,et . (1-3) . (4,6-8).
stackable-vlan		Specifies that this port is a tunnel backbone port on which VLANs will be tunneled through the MAN.
exclude-default-vlan		Specifies that this trunk port does not belong to the default VLAN.
untagged		Specifies that this trunk port will send out untagged frames instead of 802.1Q tagged frames.

Restrictions

Packet-over-SONET (PoS) ports must be configured for bridged encapsulation in order to be a VLAN trunk port. Use the **ppp set ppp-encaps-bgd** command to set one or more PoS ports for bridged encapsulation.

vlan show

Mode

User or Enable

Format

vlan show [stackable-vlan]

Description

The **vlan show** command lists all the VLANs that have been configured on the RS. It provides the following information about each VLAN:

- the VLAN ID
- the name of the VLAN
- the type of VLAN (determines the types of traffic the RS forwards on the VLAN)
- the ports included in the VLAN

The **vlan show stackable-vlan** command lists all the stackable VLANs that have been configured on the RS. It provides the following information:

- the ID of the VLAN to be tunneled and the ID of the backbone VLAN
- tunnel entry/exit ports
- ports on which multicast, broadcast, or unknown unicast packets are flooded
- tunnel backbone ports
- stackable VLAN access ports

Restrictions

None.

Example

To display all the VLANs that have been configured on the RS:

rs# vlan show			
VID	VLAN Name	Used for	Ports
---	-----	-----	----
1	DEFAULT	IP, IPX, ATALK, DEC, SNA, IPv6, L2	et.2.(1,4-8)
2	trunk1	IP, IPX, ATALK, DEC, SNA, IPv6, L2	et.2.1
3	trunk2	IP, IPX, ATALK, DEC, SNA, IPv6, L2	et.2.(1,3)
4	trunk3	IP	et.2.(1-2)
5	ipx1	IPX	et.2.(1-2)
6	blue	L2	
rs#			

To display information about the stackable VLANs that have been configured on the RS:

```
rs# vlan show stackable-vlan
Stackable VLAN Information
=====

(20, 222): ❶
  Applied On: et.6.1 ❷
  Flooded On: et.3.8,et.6.1 ❸

Stackable VLAN Trunk Ports: et.3.8 ❹

Stackable VLAN Access Ports: ❺
```

1. The ID number of the VLAN, followed by the ID number of the backbone VLAN.
2. The tunnel entry/exit ports, configured with the **vlan enable stackable-vlan** command.
3. The ports on which multicast, broadcast, or unknown unicast packets are flooded.
4. The tunnel backbone ports, configured with the **stackable-vlan** option of the **vlan make trunk-port** command.
5. Tunnel entry ports that have also been configured (with the **stackable-vlan** option of the **vlan make access-port** command) as access ports that can belong to more than one VLAN of the same protocol type. This allows multiple VLANs to use the same tunnel entry port.

80 WAN COMMANDS

The WAN rate shaping commands are used to perform the following tasks:

- Create WAN rate shaping policies
- Apply WAN rate shaping policies to ports
- Clear WAN rate shaping statistics
- List WAN rate shaping policies and statistics

80.1 COMMAND SUMMARY

The following table lists the WAN rate shaping commands. The sections following the table describe the command syntax.

wan apply rate-shape-parameters <i><name></i> [port <i><port></i> destination-ip-address <i><ipaddr></i> source-ip-address <i><ipaddr></i> vlan <i><name></i> traffic-source-port <i><port></i>] burst-queue-depth <i><number></i> shape-control-priority no-shape-high-priority
wan clear rate-shape-statistics port <i><port></i>
wan define rate-shape-parameters <i><name></i> cir <i><value></i> bc <i><value></i> be <i><value></i>
wan show rate-shape-parameters <i><name></i> all
wan show rate-shape-policies port <i><port></i>
wan show rate-shape statistics port <i><port></i>

wan apply rate-shape-parameters

Mode

Configure

Format

```
wan apply rate-shape-parameters <name> [port <port> | destination-ip-address <ipaddr> |  
source-ip-address <ipaddr> | vlan <name> | traffic-source-port <port>] burst-queue-depth  
<number> | shape-control-priority | no-shape-high-priority
```

Description

The **wan apply rate-shape-parameters** command applies a named rate shaping template to a specified WAN port. The rate shaping template must first be created using the **wan define rate-shape-parameters** command.

You can limit rates using one of the following criteria:

- The destination IP address in the packet.
- The source IP address in the packet.
- The VLAN to which the packet belongs.
- The port from which the packet originated.

This criteria, together with the rate shaping template, form the rate shaping policy for the specified port. Only one of these criteria can be specified for each policy, although more than one policy can be applied to a specific port.

For each policy, you can optionally specify whether or not control traffic and high priority traffic is shaped, and the size of the queue where packets exceeding the configured rate for the stream will be placed.

For IP address qualifiers, you can specify subnets using the CIDR notation. (e.g. 10.1.1.2/16 represents subnet 10.1.0.0).



Caution

If you do not specify a subnet mask with the IP address, then the address is treated as a specific IP address. For example, 10.1.0.0 is treated as a unique IP address and not as the network 10.1.

Parameter	Value	Meaning
rate-shape-parameters	<name>	The name of a previously created rate shaping policy.
port	<port>	A port name for one of the following: PPP, CHDLC, Multilink PPP, Channelized T1, Channelized E1, Channelized T3, Clear Channel T3, or Clear Channel E3.
destination-ip-address	<ipaddr>	The IP address of a LAN interface to which the traffic is destined.

Parameter	Value	Meaning
source-ip-address	<i><ipaddr></i>	The IP address of a LAN interface from which the traffic originates.
vlan	<i><name></i>	A VLAN name.
traffic-source-port	<i><port></i>	The LAN port from which the traffic originates.
burst-queue-depth	<i><number></i>	The size of the queue where packets exceeding the configured rate for the stream will be queued up. You can choose a value of 0 to allow for rate-limiting. The maximum value is 256. The default is 32.
shape-control-priority		Controls what happens to control priority traffic. By default control priority traffic is not shaped. During normal operation control priority traffic like STP/ARP/OSPF packets is never shaped. Using this parameter also forces the shaping of control traffic. This control should be used sparingly.
no-shape-high-priority		Controls what happens to high priority traffic. By default high priority traffic is shaped. If you want to configure some kinds of traffic as high priority traffic such as VoIP packets, and want to prevent them being dropped due to shaping actions, then configure this parameter to not shape high priority traffic.

Restrictions

Valid for PPP, Cisco HDLC and Multilink PPP encapsulations on the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3.
- Clear Channel T3 and Clear Channel E3

Examples

To apply the rate shaping parameters from the policy *rs1* to the HSSI link in slot 5, port 1, in VLAN red:

```
rs(config)# wan apply rate-shape-parameters rs1 port hs.5.1 vlan red
```

To apply the rate shaping parameters from policy *rs1* to the HSSI link in slot 5, port 1, in VLAN red and a burst queue depth of zero:

```
rs(config)# wan apply rate-shape-parameters rs1 port hs.5.1 vlan red  
burst-queue-depth 0
```

To apply the rate shaping parameters from policy *rs1* to the HSSI link in slot 5, port 1, in VLAN red and a burst queue depth of 64:

```
rs(config)# wan apply rate-shape-parameters rs1 port hs.5.1 vlan red  
burst-queue-depth 64
```

To apply the rate shaping parameters from policy *rs1* to the first T1 line of the T3 in slot 1, port 1, and a source IP address of 10.1.1.1:

```
rs(config)# wan apply rate-shape-parameters rs1 port t3.1.1:1 source-ip-address  
10.1.1.1
```

To apply the rate shaping parameters from policy *rs1* to the first T1 line of the T3 in slot 1, port 1, and a source network address of 10.1.1.0:

```
rs(config)# wan apply rate-shape-parameters rs1 port t3.1.1:1 source-ip-address  
10.1.1.1/24
```

wan clear rate-shape-statistics

Mode

Configure

Format

wan clear rate-shape-statistics port <port>

Description

The **wan clear rate-shape-statistics** command clears rate shaping statistics for a particular port. Repeatedly showing and clearing statistics at regular intervals allows you to get a snapshot of how the rate shaping feature is working. Some of the statistics columns include:

Curr Queue – The current number of packets in the shaping burst queue.

Max Queue – The maximum number of packets queued so far in the burst queue.

Peak Burst – The peak number of bytes sent in any sampling interval.

Restrictions

Valid for PPP, Cisco HDLC and Multilink PPP encapsulations on the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3.
- Clear Channel T3 and Clear Channel E3

Example

To clear the rate shaping statistics for the HSSI link in slot 2, port 1:

```
rs# wan clear rate-shape-statistics port hs.2.1
```

wan define rate-shape-parameters

Mode

Configure

Format

```
wan define rate-shape-parameters <name> cir <value> bc <value> be <value>
```

Description

The **wan define rate-shape-parameters** command creates a WAN rate shaping template that you can later apply to specific WAN ports.

Parameter	Value	Meaning
rate-shape-parameters	<name>	An ASCII string that you can use to refer to this template. The string can have a maximum length of 15 characters.
cir	<value>	The Committed Information Rate (CIR) in bits-per-second. The CIR is the rate to which you want to restrict the users use of the total bandwidth. CIR can be zero, in which case a Burst Exceed (BE) value must be configured.
 Caution The sum of the CIRs on a link must be less than or equal to the total bandwidth available for that link. If the sum is greater than the total bandwidth, the link is oversubscribed and congestion can occur.		
bc	<value>	The Burst Commit value, in number of bits. This signifies the number of bits that will be sent out in the sampling interval. Using this parameter, a sampling interval Tc of BC / CIR is computed internally. Tc is the interval of time in which the Burst Commit is transmitted. This parameter is optional. If not provided, a Tc value of 1/16th of a second will be used and the BC computed internally as CIR * Tc. If CIR is zero, then BC must be zero.
 Note You get better results the smaller the sampling interval (less than 1/8th of a second). Choose the BC values such that BC / CIR is less than 1.		
be	<value>	The BE value, in number of bits. This signifies the number of excess bits that can be sent in the above computed interval. Excess bits are sent only if there is some bandwidth available to send. This parameter is optional. If not specified, the value is zero. If CIR is configured to be zero then a non-zero BE must be specified. Note that BE is a value that represents the extra number of bits above how much is allowed by BC.

Restrictions

Valid for PPP, Cisco HDLC and Multilink PPP encapsulations on the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3.
- Clear Channel T3 and Clear Channel E3

Example

To define a CIR of 256Kbits, with the BC internally computed as CIR/16:

```
rs(config)# wan define rate-shape_parameters rs1 cir 256000
```

To define a CIR of 256Kbits and BC of 16Kbits:

```
rs(config)# wan define rate-shape_parameters rs1 cir 256000 bc 16000
```

To define a CIR of 256Kbits, a BC of 16Kbits and BE of 8K bits:

```
rs(config)# wan define rate-shape_parameters rs1 cir 256000 bc 16000 be 8000
```

To define a CIR of 0, BC of 0 and BE of 8K bits. Use this for best-effort delivery. If there is bandwidth available, then packets will be sent out:

```
rs(config)# wan define rate-shape_parameters rs1 cir 0 bc 0 be 8000
```

The previous example could also be defined using the command:

```
rs(config)# wan define rate-shape_parameters rs1 be 8000
```

wan show rate-shape-parameters

Mode
Enable

Format

wan show rate-shape-parameters <name> | all

Description

The **wan show rate-shape-parameters** command displays the list of configured policies. You can list each policy by name, or list all the policies.

Parameter	Value	Meaning
rate-shape-parameters	<name>	The name of the rate shaping policy to display.
all		Indicates that all rate shaping policies are to be listed.

Restrictions

Valid for PPP, Cisco HDLC and Multilink PPP encapsulations on the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3.
- Clear Channel T3 and Clear Channel E3

Example

To display the rate shaping parameters for the HSSI link in slot 2, port 1:

rs# wan show rate-shape-parameters port hs.2.1			
Template	CIR	BC	BE
-----	-----	-----	-----
rs1	524288	32768	16384
rs#			

wan show rate-shape-policies

Mode

Enable

Format

wan show rate-shape-policies port *<port>*

Description

The **wan show rate-shape-policies** command displays the list of rate shaping policies applied to a particular port.

Parameter	Value	Meaning
port	<i><port></i>	The port for which the applied rate shaping policies are to be listed.

Restrictions

Valid for PPP, Cisco HDLC and Multilink PPP encapsulations on the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3.
- Clear Channel T3 and Clear Channel E3

Example

To display the rate shaping policies applied to the HSSI link in slot 2, port 1:

rs# wan show rate-shape-policies port hs.2.1							
Port	Template	CIR	Bc	Be	Type	Type Info	Queue
-----	-----	-----	-----	-----	-----	-----	-----
hs.2.1	rs1	524288	32768	16384	DST-IP	123.45.67.0/24	32
rs#							

wan show rate-shape-statistics

Mode

Enable

Format

```
wan show rate-shape statistics port <port>
```

Description

The **wan show rate-shape-statistics** command displays the following rate shaping statistics for a particular port:

Curr Queue – The current number of packets in the shaping burst queue.

Max Queue – The maximum number of packets queued so far in the burst queue.

Peak Burst – The peak number of bytes sent in any sampling interval.

Parameter	Value	Meaning
port	<port>	The port for which the rate shaping statistics are to be displayed.

Restrictions

Valid for PPP, Cisco HDLC and Multilink PPP encapsulations on the following port types:

- HSSI
- Serial
- Channelized T1, Channelized E1 and Channelized T3.
- Clear Channel T3 and Clear Channel E3

Example

To display the rate shaping statistics for the HSSI link in slot 2, port 1:

rs# wan show rate-shape statistics port hs.2.1							
Template	Type	Type Info	Curr Queue (Packets)	Max Queue (Packets)	Peak Burst (Bytes)	Num Exceeded (Packets)	
rs1	DST-IP	123.45.67.0/24	0	0	0	0	
rs#							

81 WEB-CACHE COMMANDS

The **web-cache** commands allow you to transparently redirect HTTP request to a group of local cache servers. This feature can provide faster user responses and reduce demands for WAN bandwidth.



Note Certain web sites require authentication of source IP addresses for user access. Requests to these sites cannot be sent to the cache servers.

81.1 COMMAND SUMMARY

The following table lists the web-cache commands. The sections following the table describe the syntax for each command.

<code>web-cache <cache-name> apply interface <interface-name></code>
<code>web-cache <cache-name> apply port <port-number> [vlan <string>]</code>
<code>web-cache <cache-name> create bypass-list range <ipaddr-range> list <ipaddr-list> acl <acl-name></code>
<code>web-cache <cache-name> create filter interface <interface-name> ports <port-number></code>
<code>web-cache <cache-name> create server-list <server-list-name> range <ipaddr-range> list <ipaddr-list> [status backup]</code>
<code>web-cache <cache-name> permit deny hosts range <ipaddr-range> list <ipaddr-list> acl <acl-name></code>
<code>web-cache <cache-name> selection-policy {round-robin range <ipaddr-range> list <ipaddr-list>} {weighted-round-robin range <ipaddr-range> list <ipaddr-list>} {weighted-hash range <ipaddr-range> list <ipaddr-list>}</code>
<code>web-cache <cache-name> set http-port <port number></code>
<code>web-cache <cache-name> set maximum-connections <server-list> <max-connections></code>
<code>web-cache <cache-name> set redirect-protocol tcp udp protocol <protocol number></code>

web-cache <cache-name> set server-options <server-list> [ping-int <num>] [ping-tries <num>] [app-int <num>] [app-tries <num>] [app-check-on] [backup <string>] [backup policy backup-pool one-to-one] [hashbucket-weight <num>] [wrr-weight <num>]
web-cache show all [server-options]
web-cache show cache-name <cache-name> all [server-options]
web-cache show servers cache <cache-name> all [server-options]
web-cache show statistics {cache-block <cache-name> all} {server <IPAddr>}

web-cache apply interface

Mode

Configure

Format

web-cache <cache-name> apply interface <interface-name>

Description

The **web-cache apply** command lets you apply a configured cache policy to an outbound interface. The interface to which the cache policy is applied is typically the interface that physically connects to the internet. This command is used to redirect outbound HTTP traffic to the cache servers.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache policy configured with the web-cache create server-list command.
interface	<interface-name>	This is the interface that connects to the internet.

Restrictions

None.

Example

To apply the caching policy *websrv1* to the interface *inet2*:

```
rs(config)# web-cache websrv1 apply interface inet2
```

web-cache apply port

Mode

Configure

Format

```
web-cache <cache-name> apply port <port-number> [vlan <string>]
```

Description

The **web-cache apply** command lets you apply a configured cache policy to the port leading to the web server. This command is used to redirect outbound HTTP traffic to the cache servers. Use this command when redirecting bridged traffic. When you do so, L4 bridging must be enabled, and the clients, servers, and ports must belong to the same VLAN.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache policy configured with the web-cache create server-list command.
port	<port-number>	The port that leads to the web server.
vlan	<string>	If the specified port is an 802.1Q trunk port, you can also specify the VLAN to which the policy will be applied.

Restrictions

None.

Example

To apply the caching policy *websrv1* to the BLUE VLAN on port et.3.1:

```
rs(config)# web-cache websrv1 apply port et.3.1 vlan blue
```

web-cache create bypass-list

Mode

Configure

Format

```
web-cache <cache-name> create bypass-list range <ipaddr-range> | list <ipaddr-list> | acl <acl-name>
```

Description

The **web-cache create bypass-list** command allows you to define the destinations to which HTTP requests are sent directly without redirection to a cache server. Specify a range of IP addresses, a list of up to four IP addresses, or an ACL that qualifies these hosts.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the caching policy.
range	<ipaddr-range>	A range of host IP addresses in the form “176.89.10.10 176.89.10.50.” This adds the hosts 176.89.10.10 through 176.89.10.50 to the bypass list.
list	<ipaddr-list>	A list of up to four destination IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12.”
acl	<acl-name>	Name of the ACL. The ACL may contain either the permit or deny keywords. The web-cache create bypass-list command only looks at the following ACL rule parameter values: • Protocol • Source IP address • Destination IP address • Source port • Destination port • TOS.

Restrictions

None.

Examples

To specify the hosts 176.89.10.10 and 176.89.10.11 for the bypass list for the caching policy *websrv1*:

```
rs(config)# web-cache websrv1 create bypass-list list  
"176.89.10.10 176.89.10.11"
```

To specify the hosts defined in the ACL *nocache* for the bypass list for the caching policy *websrv1*:

```
rs(config)# web-cache websrv1 create bypass-list acl nocache
```


web-cache create filter

Mode

Configure

Format

```
web-cache <cache-name> create filter interface <interface-name> ports <port-number>
```

Description

Use the **web-cache create filter** command to exclude packets from being redirected if they are from the specified input interface or ports.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the caching policy.
interface	<interface-name>	The name of the inbound interface on which redirection is disabled.
ports	<port-number>	The inbound port on which redirection is disabled.

Restrictions

None.

Examples

To specify no redirection of traffic on the interface *eng1* for the caching policy *websrv1*:

```
rs(config)# web-cache websrv1 create filter-list interface eng1
```

web-cache create server-list

Mode

Configure

Format

```
web-cache <cache-name> create server-list <server-list-name> range <ipaddr-range> | list  
<ipaddr-list> status [backup]
```

Description

Use the **web-cache create server-list** command to create a group of servers that use a specified caching policy. If there are multiple cache servers, caching is done based on the destination IP address. If any cache server fails, traffic is redirected to other active servers. Specify either a range of IP addresses or a list of up to four IP addresses.



Note Traffic that is sent from a server in the server list is not redirected.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the caching policy.
server-list	<server-list-name>	The name of the list of servers.
range	<ipaddr-range>	A range of host IP addresses in the form “176.89.10.10 176.89.10.50.” This adds the hosts 176.89.10.10 through 176.89.10.50 to the server list.
list	<ipaddr-list>	A list of up to four host IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12.”
status	backup	Specifies that the servers in the group are backup servers.

Restrictions

None.

Examples

To specify the server list *servers1* for the caching policy *websrv1*:

```
rs(config)# web-cache websrv1 create server-list servers1 range  
"10.10.10.10 10.10.10.50"
```

web-cache permit | deny hosts

Mode

Configure

Format

```
web-cache <cache-name> permit | deny hosts range <ipadd-range> | list <ipaddr-list> | acl <acl-name>
```

Description

Use the **web-cache permit** to specify the hosts (users) whose HTTP requests are redirected to the cache servers and the **web-cache deny** command to specify the hosts whose HTTP requests are not redirected to the cache servers. If no **permit** command is specified, all HTTP requests are redirected to the cache servers. You can specify a range of IP addresses, a list of up to four IP addresses, or an ACL.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache.
range	<ipadd-range>	A range of host IP addresses in the form “176.89.10.10 176.89.10.50.”
list	<ipaddr-list>	A list of up to four host IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12.”
acl	<acl-name>	Name of the ACL profile to be used. This ACL profile defines the packets that are permitted or denied. The web-cache permit/deny command only looks at the following ACL parameters: • Protocol • Source IP address • Destination IP address • Source port • Destination port • TOS

Restrictions

None.

Examples

To allow the HTTP requests of certain hosts to be redirected to cache servers:

```
rs(config)# web-cache webserv1 permit hosts range "10.10.20.10  
10.10.20.50"
```

To specify that the HTTP requests of certain hosts not be redirected to the cache servers:

```
rs(config)# web-cache webserv1 deny hosts list "10.10.20.61  
10.10.20.75"
```

web-cache selection-policy

Mode

Configure

Format

```
web-cache <cache-name> selection-policy {round-robin range <ipadd-range>| list <ipaddr-list>}  
{weighted-round-robin range <ipadd-range>| list <ipaddr-list>} {weighted-hash range  
<ipadd-range>| list <ipaddr-list>}
```

Description

The **web-cache selection-policy** command defines the policy for selecting cache servers when traffic is redirected.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache.
round-robin		Cache servers will be selected using round robin. If no list or range is specified, all traffic will use this policy.
weighted-round-robin		Cache servers will be selected using weighted round robin. If no list or range is specified, all traffic will use this policy. If you select this policy, you also need to specify the weight with the web-cache set server-options command.
weighted-hash		Cache servers will be selected using hashbucket weights. If no list or range is specified all traffic will use this policy. If you select this policy, you also need to specify the weight with the web-cache set server-options command.
range	<ipadd-range>	A range of host IP addresses.
list	<ipaddr-list>	A list of up to four host IP addresses.

Restrictions

None.

Example

The following example sets the selection policy of the *websrv1* cache to round robin:

```
rs(config)# web-cache websrv1 selection-policy round-robin
```

web-cache set http-port

Mode

Configure

Format

web-cache <cache-name> set http-port <port number>

Description

Some networks use proxy servers that listen for HTTP requests on a non-standard port number. The RS can be configured to redirect HTTP requests on a non-standard HTTP port. Use the **web-cache set http-port** command to specify the port number that is used by the proxy server for HTTP requests. The default is port 80.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache.
http-port	<port number>	This is the port number used by the proxy server for HTTP requests. Specify a value between 1 and 65535.

Restrictions

None.

Example

To set the port number for HTTP requests:

```
rs(config)# web-cache websvr1 set http-port 100
```

web-cache set maximum-connections

Mode

Configure

Format

```
web-cache <cache-name> set maximum-connections <server-list> <max-connections>
```

Description

Use the **web-cache set maximum-connections** command to set a limit on how many connections will be supported for a web caching server group. This number is the maximum number of connections allowed for each server in a list of web caching servers. This list must already have been created with the **web-cache create server-list** command.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the caching policy.
maximum-connections	<server-list>	The name of the list of servers.
	<max-connections>	Specify the maximum number of connections that are supported by the server group. The maximum value is 2147483647. The default value is 2000.

Restrictions

None.

Example

To limit the number of connections for servers in the server list *servers1* to 1000 connections:

```
rs(config)# web-cache set maximum-connections servers1 1000
```

web-cache set redirect-protocol

Mode

Configure

Format

```
web-cache <cache-name> set redirect-protocol tcp | udp | protocol <protocol number>
```

Description

Use the **web-cache set redirect-protocol** command to specify the protocol of the traffic that is to be redirected. The default is TCP.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache.
redirect-protocol	tcp	Specify that the redirect protocol is TCP.
	udp	Specify that the redirect protocol is UDP.
protocol	<protocol number>	The assigned Internet protocol number for the protocol, as defined in RFC 1060.

Restrictions

None.

Example

To set the redirection for UDP traffic for the cache *websvr1*:

```
rs(config)# web-cache websvr1 set redirect-protocol udp
```


web-cache set server-options

Mode

Configure

Format

```
web-cache <cache-name> set server-options <server-list> [ping-int <num>] [ping-tries <num>]
[app-int <num>] [app-tries <num>] [app-check-on] [backup <string>] [backup policy
backup-pool | one-to-one] [hashbucket-weight <num>] [wrr-weight <num>]
```

Description

Use the **web-cache set server-options** command to set various parameters for a group of web cache servers. This group must have already been created with the **web-cache create server-list** command.

Parameter	Value	Meaning
web-cache	<cache-name>	The name of the cache.
server-options	<server-list>	The name of the group of web cache servers.
ping-int	<num>	Use this parameter to set the ping interval (seconds) for servers in this group. Specify any value between 1 and 3600.
ping-tries	<num>	Use this parameter to set the number of ping retries before marking the server down. Specify any value between 1 and 255.
app-int	<num>	Use this parameter to set the interval (seconds) between application checks. Specify any value between 1 and 3600.
app-tries	<num>	Use this parameter to set the number of retries before marking the application down. Specify any value between 1 and 255.
app-check-on		Use this parameter to enable the checking of servers with TCP connection requests. The default is to check the servers with ICMP echo requests.
backup	<string>	Specifies the backup server.
backup-policy		Specifies the policy used for the backup server.
	one-to-one	Specifies that when the other server is down, it is replaced by the specified backup server.
	backup-pool	Specifies that when the backup server is down, it is replaced by any of the backups in the pool of servers. This is the default.
wrr-weight	<number>	Weight of the server list in weighted round robin distribution of IP addresses. The default is 1.
hashbucket-weight	<number>	Weight of the server list while distributing IP-addresses based on weighted hash buckets. The default is 1.

Restrictions

None.

Example

To ping the servers in the list *service2* in the cache group *websvr1* every 10 seconds:

```
rs(config)# web-cache websvr1 set server-options service2 ping-int  
10
```

web-cache show all

Mode

Enable

Format

```
web-cache show all [server-options]
```

Description

The **web-cache show all** command allows you to display all web cache information for all caching policies and all server lists.

Parameter	Value	Meaning
server-options		Displays the server options only.

Restrictions

None.

Examples

Following is an example of the **web-cache show all** command:

```
rs# web-cache show all

Legend

Server IP   : IP address of server
DPort      : Destination Port for application checking
MaxCon     : Maximum number of connections for this server
Used       : Used count for this server
WRR        : Weight used if server-selection policy is Weighted Round Robin
WH         : Weight used if server-selection policy is Weighted Hash
Oper       : Operational Status
T          : Application Checking Enabled
S          : Server status: BU = Backup; R = server Replaced by backup

-----
Cache Name       : cache1
Applied Interfaces : none
Applied Ports    : none (CONTROL)
Redirect Port    : 80
Rewrite Policy   : Off
Redirect Protocol : 6 (TCP)
I/f Filter List  : None
Input Port Filters : none
ACL              Source IP/Mask   Dest. IP/Mask   SrcPort   DstPort   TOS TOS-MASK Prot ORIG AS
-----
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Server Group | Server IP | DPort | Max Conn | Used | WRR | WH | Oper | T | S |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| list10       | 10.10.10.1 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.2 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.3 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.4 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.5 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.6 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.7 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.8 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.9 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
| list10       | 10.10.10.10 | 80 | 2000 | 0 | 1 | 1 | Down | N | - |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

Access Users
-----
Permit All Users

Server Selection Policy for Destination Sites
-----
Round Robin :
All sites (Default)
```

Table 81-1 Display field descriptions for the web-cache show all command

FIELD	DESCRIPTION
Cache Name	The name of the cache policy.
Applied Interfaces	The interfaces to which the policy is applied.
Applied Ports	The ports to which the policy is applied.
Redirect Port	The port used by the proxy server for HTTP requests.
Redirect Protocol	The protocol of the traffic that was redirected.
I/f Filter List	The inbound interface(s) on which redirection will <i>not</i> be performed.
Input Port Filters	The inbound port(s) on which redirection will <i>not</i> be performed.
ACL	The ACL that defines the destinations to which HTTP requests are sent directly.
Source IP/Mask	The source IP address and netmask specified in the ACL.
Dest. IP/Mask	The destination IP address and netmask specified in the ACL.
SrcPort	The source port specified in the ACL.
DstPort	The destination port specified in the ACL.
TOS	The TOS value specified in the ACL.
TOS-MASK	The mask value for the TOS byte specified in the ACL.
Prot	The protocol specified in the ACL.
Server Group	The server group to which the cache policy is applied.
Server IP	The IP address of each server in the group.
DPort	The destination port for application checking.
Max Conn	The maximum number of connections for each server.
Used	The number of flows that have been directed to the cache server.
WRR	If the server selection policy is weighted round robin, this is the weight of the server.
WH	If the server selection policy is weighted hash, this is the weight of the server.
Oper	The server's operational status.
T	Indicates if application checking is enabled.
S	Displays the server's status.
Access	Indicates whether the HTTP requests of the hosts in the corresponding Users field are or are not redirected to the cache servers. Permit specifies that the HTTP requests are redirected to the cache servers. Deny specifies that the HTTP requests are <i>not</i> redirected to the cache servers.

Table 81-1 Display field descriptions for the web-cache show all command

FIELD	DESCRIPTION
Users	The IP addresses or ACLs that define the hosts whose HTTP requests are or are not redirected.
Server Selection Policy for Destination Sites	The server selection policy: round robin, weighted round robin, or weighted hash.

web-cache show cache-name

Mode

Enable

Format

```
web-cache show cache-name <cache-name>|all [server-options]
```

Description

The **web-cache show** cache-name command allows you to display web caching information for specific caching policies.

Parameter	Value	Meaning
cache-name	<cache-name>	Displays web cache information for the specified caching policy.
	all	Displays all caching policies.
server-options		Displays the server options only.

Restrictions

None.

Examples

Following is an example of the **web-cache show cache-name** command:

```
rs# web-cache show cache-name testweb1

-----
Cache Name       : testweb1
Applied Interfaces : eth5.1
Redirect Port    : 80
Redirect Protocol : 6 (TCP)
Bypass list     : testacl1
Filter List     : None

ACL      Source IP/Mask Dest. IP/Mask SrcPort DstPort TOS TOS-MASK Prot
---
testacl1 1.1.1.0/30      3.3.3.0/30      80      80      any none   IP
testacl2 2.2.2.0/30      4.4.4.0/30      80      80      any none   IP

Server IP       : IP address of server
DPort          : Destination Port for application checking
MaxCon         : Maximum number of connections for this server
Used           : Used count for this server
PI             : Ping Interval
PT             : Ping Tries
AI             : Application Interval
AT             : Application Tries
Oper           : Operational Status
T              : Application Checking Enabled

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Server Group | Server IP | DPort | MaxCon | Used | PI | PT | AI | AT | Oper | T |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| weblist1    | 1.1.1.1  | 80    | 2000   | 0    | 5  | 4  | 15 | 4  | Up   | N |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

Access Users
-----
Permit testacl1
Deny   testacl2
```

Table 81-2 Display field descriptions for the web-cache show cache-name command

FIELD	DESCRIPTION
Cache Name	Identifies the web cache policy that is displayed.
Applied Interface	The interfaces to which the web cache policy is applied.
Redirect Port	The outbound interface on which the web-cache policy was applied.
Redirect Protocol	The protocol of the traffic that is to be redirected. The default is TCP.

Table 81-2 Display field descriptions for the web-cache show cache-name command (Continued)

FIELD	DESCRIPTION
Bypass List	The sites to which HTTP requests are not redirected. This can be a list or range of IP addresses, or an ACL profile that defines these sites.
Filter List	Packets from these inbound interfaces are not redirected.
ACL	Displays the ACLs. The following fields characterize the flows listed in the ACL.
Source IP/Mask	The source address and mask of the flow defined by the ACL.
Dest. IP/Mask	The destination address and mask specified in the ACL.
SrcPort	The number of the source port specified in the ACL.
DstPort	The number of the destination port specified in the ACL.
TOS	The Type of Service (TOS) value specified in the ACL.
TOS-MASK	The Mask value used for the TOS byte.
Prot	The protocol specified in the ACL.
	The following fields provide information about the server group that uses the specified caching policy.
Server Group	The name of the web caching servers group.
Server IP	The range or list of IP addresses of the servers in the group.
DPort	(Destination Port) The port on which application checks are performed.
MaxCon	(Maximum Connections) The maximum number of connections the server can handle. The default is 2000.
Used	(Used Count) The number of flows that have been directed to the web cache.
PI	(Ping Interval) The time between pings for status. The default is 15 seconds.
PT	(Ping Tries) The number of ping tries before the server's status is considered "down." The default is 5.
AI	(Application Interval) The number of seconds between application health checks. The default is 15.
AT	(Application Tries) The number application health check tries before the server's status is considered "down." The default is 5.
Oper	The operational status of the server group; will be either Up or Down.
T	Indicates whether application checking was enabled by either a Y (yes) or N (no).

Table 81-2 Display field descriptions for the web-cache show cache-name command (Continued)

FIELD	DESCRIPTION
Access	Indicates whether the HTTP requests of the hosts in the corresponding Users field are or are not redirected to the cache servers. Permit specifies that the HTTP requests are redirected to the cache servers. Deny specifies that the HTTP requests are <i>not</i> redirected to the cache servers.
Users	The IP addresses or ACLs that define the hosts whose HTTP requests are or are not redirected.

web-cache show servers

Mode

Enable

Format

```
web-cache show servers cache <cache-name>|all [server-options]
```

Description

The **web-cache show servers** command allows you to display information for the servers configured for each caching policy.

Parameter	Value	Meaning
cache	<cache-name>	Displays information for the servers configured for the specified caching policy.
	all	Displays all configured cache servers.
server-options		Displays the server options only.

Restrictions

None.

Example

Following is an example of the **web-cache show servers** command for all configured web cache policies:

rs# web-cache show servers cache all				
Cache name : wb1				
Block	IP address	Max Conn	Used Cnt	Status
-----	-----	-----	-----	-----
wb100	10.10.10.20	2000	0	Down
Cache name : wb2				
Block	IP address	Max Conn	Used Cnt	Status
-----	-----	-----	-----	-----
wb200	121.131.121.10	2000	0	Down

Table 81-3 Display field descriptions for the web-cache show servers command

FIELD	DESCRIPTION
Cache Name	The name of the cache policy.
Block	The web cache group of servers.
IP Address	The IP address of the servers in the web caching server group.
Max Conn	The maximum number of connections that can be handled by the servers.
Used Cnt	The number of connections currently being handled by the servers.
Status	The current status of the servers.

web-cache show statistics

Mode

Enable

Format

web-cache show statistics cache-block <cache-name>|server <IPAddr>

Description

The **web-cache show statistics** command allows you to display statistics for the specified cache policy.

Parameter	Value	Meaning
cache-block	<cache-name>	Displays statistics for the specified cache block.
	all	Displays statistics for all configured caches.
server	<IPAddr>	Displays statistics for the specified server.

Restrictions

None.

Example

Following is an example of the **web-cache show statistics** command for all configured web cache policies:

```
rs# web-cache show statistics cache-block cache1
Cache Name :wc-http          Server IP :192.1.1.25
  ---No Traffic---
Cache Name :wc-http          Server IP :192.1.1.26
  ---No Traffic---
Cache Name :wc-http          Server IP :192.1.1.27
  ---No Traffic---
Cache Name :wc-http          Server IP :192.1.1.28
+-----+-----+-----+-----+
|Direction      |Packets      |Bytes        |
+-----+-----+-----+-----+
|Users -> Cache |60           |5150         |
|Cache -> Users |60           |36790        |
|Origin-> Cache |0            |0            |
|Cache -> Origin|0            |0            |
+-----+-----+-----+-----+
```

Table 81-4 Display field descriptions for the web-cache show statistics command

FIELD	DESCRIPTION
Cache Name	The name of the cache policy.
Server IP	The IP address of the cache server.
Direction	The direction of the traffic.
Packets	The number of packets that were transmitted.
Bytes	The number of bytes that were transmitted.

APPENDIX A RMON 2 PROTOCOL DIRECTORY

This appendix lists the protocol encapsulations that can be managed with the RMON 2 Protocol Directory group on the RS. You can specify protocol encapsulations with the **rmon set protocol-directory** or **rmon show protocol-directory** commands. For example, **ether2.ipx** specifies IPX over Ethernet II, while ***ether2.ipx** specifies IPX over any link layer protocol. The protocol object IDs are defined in RFC 2074.

The protocols are listed in the following order:

- *"Ethernet applications"*
- *"IP (version 4) applications"*
- *"IPX applications"*
- *"TCP applications"*

Table A-1 Ethernet applications

Protocol Encapsulation	Protocol Identifier (Object ID)
ether2.idp	8.0.0.0.1.0.0.6.0.2.0.0
ether2.ip-v4	8.0.0.0.1.0.0.8.0.2.0.0
ether2.chaosnet	8.0.0.0.1.0.0.8.4.2.0.0
ether2.arp	8.0.0.0.1.0.0.8.6.2.0.0
ether2.vip	8.0.0.0.1.0.0.11.173.2.0.0
ether2.vloop	8.0.0.0.1.0.0.11.174.2.0.0
ether2.vecho	8.0.0.0.1.0.0.11.175.2.0.0
ether2.netbios-3com	8.0.0.0.1.0.0.60.0.2.0.0
ether2.dec	8.0.0.0.1.0.0.96.0.2.0.0
ether2.mop	8.0.0.0.1.0.0.96.1.2.0.0
ether2.mop2	8.0.0.0.1.0.0.96.2.2.0.0
ether2.drp	8.0.0.0.1.0.0.96.3.2.0.0
ether2.lat	8.0.0.0.1.0.0.96.4.2.0.0
ether2.dec-diag	8.0.0.0.1.0.0.96.5.2.0.0
ether2.lavc	8.0.0.0.1.0.0.96.7.2.0.0
ether2.rarp	8.0.0.0.1.0.0.128.53.2.0.0
ether2.atalk	8.0.0.0.1.0.0.128.155.2.0.0
ether2.vloop2	8.0.0.0.1.0.0.128.196.2.0.0

Table A-1 Ethernet applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
ether2.vecho2	8.0.0.0.1.0.0.128.197.2.0.0
ether2.sna-th	8.0.0.0.1.0.0.128.213.2.0.0
ether2.aarp	8.0.0.0.1.0.0.128.243.2.0.0
ether2.ipx	8.0.0.0.1.0.0.129.55.2.0.0
ether2.snmp	8.0.0.0.1.0.0.129.76.2.0.0
ether2.ip-v6	8.0.0.0.1.0.0.134.221.2.0.0
ether2.loopback	8.0.0.0.1.0.0.144.0.2.0.0
*ether2.ip-v4	8.1.0.0.1.0.0.8.0.2.0.1
*ether2.ipx	8.1.0.0.1.0.0.129.55.2.0.0

Table A-2 IP (version 4) applications

Protocol Encapsulation	Protocol Identifier (Object ID)
IP (version 4) Applications	
*ether2.ip-v4.icmp	12.1.0.0.1.0.0.8.0.0.0.1.3.0.1.0
*ether2.ip-v4.igmp	12.1.0.0.1.0.0.8.0.0.0.0.2.3.0.1.0
*ether2.ip-v4.ggp	12.1.0.0.1.0.0.8.0.0.0.0.3.3.0.1.0
*ether2.ip-v4.ipip4	12.1.0.0.1.0.0.8.0.0.0.0.4.3.0.1.0
*ether2.ip-v4.st	12.1.0.0.1.0.0.8.0.0.0.0.5.3.0.1.0
*ether2.ip-v4.tcp	12.1.0.0.1.0.0.8.0.0.0.0.6.3.0.1.0
*ether2.ip-v4.ucl	12.1.0.0.1.0.0.8.0.0.0.0.7.3.0.1.0
*ether2.ip-v4.egp	12.1.0.0.1.0.0.8.0.0.0.0.8.3.0.1.0
*ether2.ip-v4.igp	12.1.0.0.1.0.0.8.0.0.0.0.9.3.0.1.0
*ether2.ip-v4.bbn-rcc-mon	12.1.0.0.1.0.0.8.0.0.0.0.10.3.0.1.0
*ether2.ip-v4.nvp2	12.1.0.0.1.0.0.8.0.0.0.0.11.3.0.1.0
*ether2.ip-v4.pup	12.1.0.0.1.0.0.8.0.0.0.0.12.3.0.1.0
*ether2.ip-v4.argus	12.1.0.0.1.0.0.8.0.0.0.0.13.3.0.1.0
*ether2.ip-v4.emcon	12.1.0.0.1.0.0.8.0.0.0.0.14.3.0.1.0
*ether2.ip-v4.xnet	12.1.0.0.1.0.0.8.0.0.0.0.15.3.0.1.0
*ether2.ip-v4.chaos	12.1.0.0.1.0.0.8.0.0.0.0.16.3.0.1.0

Table A-2 IP (version 4) applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.udp	12.1.0.0.1.0.0.8.0.0.0.0.17.3.0.1.0
*ether2.ip-v4.mux	12.1.0.0.1.0.0.8.0.0.0.0.18.3.0.1.0
*ether2.ip-v4.dcn-meas	12.1.0.0.1.0.0.8.0.0.0.0.19.3.0.1.0
*ether2.ip-v4.hmp	12.1.0.0.1.0.0.8.0.0.0.0.20.3.0.1.0
*ether2.ip-v4.prm	12.1.0.0.1.0.0.8.0.0.0.0.21.3.0.1.0
*ether2.ip-v4.xns-idp	12.1.0.0.1.0.0.8.0.0.0.0.22.3.0.1.0
*ether2.ip-v4.trunk-1	12.1.0.0.1.0.0.8.0.0.0.0.23.3.0.1.0
*ether2.ip-v4.trunk-2	12.1.0.0.1.0.0.8.0.0.0.0.24.3.0.1.0
*ether2.ip-v4.leaf-1	12.1.0.0.1.0.0.8.0.0.0.0.25.3.0.1.0
*ether2.ip-v4.leaf-2	12.1.0.0.1.0.0.8.0.0.0.0.26.3.0.1.0
*ether2.ip-v4.rdp	12.1.0.0.1.0.0.8.0.0.0.0.27.3.0.1.0
*ether2.ip-v4.irtp	12.1.0.0.1.0.0.8.0.0.0.0.28.3.0.1.0
*ether2.ip-v4.iso-tp4	12.1.0.0.1.0.0.8.0.0.0.0.29.3.0.1.0
*ether2.ip-v4.netbit	12.1.0.0.1.0.0.8.0.0.0.0.30.3.0.1.0
*ether2.ip-v4.mfe-nsp	12.1.0.0.1.0.0.8.0.0.0.0.31.3.0.1.0
*ether2.ip-v4.merit-inp	12.1.0.0.1.0.0.8.0.0.0.0.32.3.0.1.0
*ether2.ip-v4.sep	12.1.0.0.1.0.0.8.0.0.0.0.33.3.0.1.0
*ether2.ip-v4.third-pc	12.1.0.0.1.0.0.8.0.0.0.0.34.3.0.1.0
*ether2.ip-v4.idpr	12.1.0.0.1.0.0.8.0.0.0.0.35.3.0.1.0
*ether2.ip-v4.xtp	12.1.0.0.1.0.0.8.0.0.0.0.36.3.0.1.0
*ether2.ip-v4.ddp	12.1.0.0.1.0.0.8.0.0.0.0.37.3.0.1.0
*ether2.ip-v4.idpr-cmt	12.1.0.0.1.0.0.8.0.0.0.0.38.3.0.1.0
*ether2.ip-v4.tp-plus-plus	12.1.0.0.1.0.0.8.0.0.0.0.39.3.0.1.0
*ether2.ip-v4.il	12.1.0.0.1.0.0.8.0.0.0.0.40.3.0.1.0
*ether2.ip-v4.sip	12.1.0.0.1.0.0.8.0.0.0.0.41.3.0.1.0
*ether2.ip-v4.sdrp	12.1.0.0.1.0.0.8.0.0.0.0.42.3.0.1.0
*ether2.ip-v4.sip-sr	12.1.0.0.1.0.0.8.0.0.0.0.43.3.0.1.0
*ether2.ip-v4.sip-frag	12.1.0.0.1.0.0.8.0.0.0.0.44.3.0.1.0
*ether2.ip-v4.idrp	12.1.0.0.1.0.0.8.0.0.0.0.45.3.0.1.0
*ether2.ip-v4.rsvp	12.1.0.0.1.0.0.8.0.0.0.0.46.3.0.1.0
*ether2.ip-v4.gre	12.1.0.0.1.0.0.8.0.0.0.0.47.3.0.1.0

Table A-2 IP (version 4) applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.mhrp	12.1.0.0.1.0.0.8.0.0.0.0.48.3.0.1.0
*ether2.ip-v4.bna	12.1.0.0.1.0.0.8.0.0.0.0.49.3.0.1.0
*ether2.ip-v4.sipp-esp	12.1.0.0.1.0.0.8.0.0.0.0.50.3.0.1.0
*ether2.ip-v4.sipp-ah	12.1.0.0.1.0.0.8.0.0.0.0.51.3.0.1.0
*ether2.ip-v4.i-nlsp	12.1.0.0.1.0.0.8.0.0.0.0.52.3.0.1.0
*ether2.ip-v4.swipe	12.1.0.0.1.0.0.8.0.0.0.0.53.3.0.1.0
*ether2.ip-v4.nhrp	12.1.0.0.1.0.0.8.0.0.0.0.54.3.0.1.0
*ether2.ip-v4.priv-host	12.1.0.0.1.0.0.8.0.0.0.0.61.3.0.1.0
*ether2.ip-v4.cftp	12.1.0.0.1.0.0.8.0.0.0.0.62.3.0.1.0
*ether2.ip-v4.priv-net	12.1.0.0.1.0.0.8.0.0.0.0.63.3.0.1.0
*ether2.ip-v4.sat-expak	12.1.0.0.1.0.0.8.0.0.0.0.64.3.0.1.0
*ether2.ip-v4.kryptolan	12.1.0.0.1.0.0.8.0.0.0.0.65.3.0.1.0
*ether2.ip-v4.rvd	12.1.0.0.1.0.0.8.0.0.0.0.66.3.0.1.0
*ether2.ip-v4.ippc	12.1.0.0.1.0.0.8.0.0.0.0.67.3.0.1.0
*ether2.ip-v4.priv-distfile	12.1.0.0.1.0.0.8.0.0.0.0.68.3.0.1.0
*ether2.ip-v4.sat-mon	12.1.0.0.1.0.0.8.0.0.0.0.69.3.0.1.0
*ether2.ip-v4.visa	12.1.0.0.1.0.0.8.0.0.0.0.70.3.0.1.0
*ether2.ip-v4.ipcv	12.1.0.0.1.0.0.8.0.0.0.0.71.3.0.1.0
*ether2.ip-v4.cpnx	12.1.0.0.1.0.0.8.0.0.0.0.72.3.0.1.0
*ether2.ip-v4.cphb	12.1.0.0.1.0.0.8.0.0.0.0.73.3.0.1.0
*ether2.ip-v4.wsn	12.1.0.0.1.0.0.8.0.0.0.0.74.3.0.1.0
*ether2.ip-v4.pvp	12.1.0.0.1.0.0.8.0.0.0.0.75.3.0.1.0
*ether2.ip-v4.br-sat-mon	12.1.0.0.1.0.0.8.0.0.0.0.76.3.0.1.0
*ether2.ip-v4.sun-nd	12.1.0.0.1.0.0.8.0.0.0.0.77.3.0.1.0
*ether2.ip-v4.wb-mon	12.1.0.0.1.0.0.8.0.0.0.0.78.3.0.1.0
*ether2.ip-v4.wb-expak	12.1.0.0.1.0.0.8.0.0.0.0.79.3.0.1.0
*ether2.ip-v4.iso-ip	12.1.0.0.1.0.0.8.0.0.0.0.80.3.0.1.0
*ether2.ip-v4.vmtpt	12.1.0.0.1.0.0.8.0.0.0.0.81.3.0.1.0
*ether2.ip-v4.secure-mvtp	12.1.0.0.1.0.0.8.0.0.0.0.82.3.0.1.0
*ether2.ip-v4.vines	12.1.0.0.1.0.0.8.0.0.0.0.83.3.0.1.0
*ether2.ip-v4.ttp	12.1.0.0.1.0.0.8.0.0.0.0.84.3.0.1.0

Table A-2 IP (version 4) applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.nfsnet-igmp	12.1.0.0.1.0.0.8.0.0.0.0.85.3.0.1.0
*ether2.ip-v4.dgmp	12.1.0.0.1.0.0.8.0.0.0.0.86.3.0.1.0
*ether2.ip-v4.tcf	12.1.0.0.1.0.0.8.0.0.0.0.87.3.0.1.0
*ether2.ip-v4.igrp	12.1.0.0.1.0.0.8.0.0.0.0.88.3.0.1.0
*ether2.ip-v4.ospf	12.1.0.0.1.0.0.8.0.0.0.0.89.3.0.1.0
*ether2.ip-v4.sprite-rpc	12.1.0.0.1.0.0.8.0.0.0.0.90.3.0.1.0
*ether2.ip-v4.larp	12.1.0.0.1.0.0.8.0.0.0.0.91.3.0.1.0
*ether2.ip-v4.mtp	12.1.0.0.1.0.0.8.0.0.0.0.92.3.0.1.0
*ether2.ip-v4.ax-25	12.1.0.0.1.0.0.8.0.0.0.0.93.3.0.1.0
*ether2.ip-v4.ipip	12.1.0.0.1.0.0.8.0.0.0.0.94.3.0.1.0
*ether2.ip-v4.micp	12.1.0.0.1.0.0.8.0.0.0.0.95.3.0.1.0
*ether2.ip-v4.scc-sp	12.1.0.0.1.0.0.8.0.0.0.0.96.3.0.1.0
*ether2.ip-v4.etherip	12.1.0.0.1.0.0.8.0.0.0.0.97.3.0.1.0
*ether2.ip-v4.encap	12.1.0.0.1.0.0.8.0.0.0.0.98.3.0.1.0
*ether2.ip-v4.priv-encrypt	12.1.0.0.1.0.0.8.0.0.0.0.99.3.0.1.0
*ether2.ip-v4.gmtp	12.1.0.0.1.0.0.8.0.0.0.0.100.3.0.1.0

Table A-3 IPX applications

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ipx.nov-pep	12.1.0.0.1.0.0.129.55.0.0.0.0.3.0.0.0
*ether2.ipx.nov-pep.ncp	16.1.0.0.1.0.0.129.55.0.0.0.0.0.4.81.4.0.0.0.0
*ether2.ipx.nov-pep.nov-sap	16.1.0.0.1.0.0.129.55.0.0.0.0.0.4.82.4.0.0.0.0
*ether2.ipx.nov-pep.nov-rip	16.1.0.0.1.0.0.129.55.0.0.0.0.0.4.83.4.0.0.0.0
*ether2.ipx.nov-pep.nov-netbios	16.1.0.0.1.0.0.129.55.0.0.0.0.0.4.85.4.0.0.0.0
*ether2.ipx.nov-pep.nov-diag	16.1.0.0.1.0.0.129.55.0.0.0.0.0.4.86.4.0.0.0.0
*ether2.ipx.nov-pep.nov-sec	16.1.0.0.1.0.0.129.55.0.0.0.0.0.4.87.4.0.0.0.0
*ether2.ipx.nov-pep.smb	16.1.0.0.1.0.0.129.55.0.0.0.0.0.5.80.4.0.0.0.0
*ether2.ipx.nov-pep.smb2	16.1.0.0.1.0.0.129.55.0.0.0.0.0.5.82.4.0.0.0.0
*ether2.ipx.nov-pep.burst	16.1.0.0.1.0.0.129.55.0.0.0.0.0.13.5.4.0.0.0.0

Table A-3 IPX applications (Continued)

*ether2.ipx.nov-pep.nov-watchdog	16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.64.4.4.0.0.0.0
*ether2.ipx.nov-pep.nov-bcast	16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.64.5.4.0.0.0.0
*ether2.ipx.nov-pep.nlsp	16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.144.1.4.0.0.0.0
*ether2.ipx.nov-pep.snmp	16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.144.15.4.0.0.0.0
*ether2.ipx.nov-pep.snmptrap	16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.144.16.4.0.0.0.0
*ether2.ipx.nov-rip	12.1.0.0.1.0.0.129.55.0.0.0.1.3.0.0.0
*ether2.ipx.nov-echo	12.1.0.0.1.0.0.129.55.0.0.0.2.3.0.0.0
*ether2.ipx.nov-error	12.1.0.0.1.0.0.129.55.0.0.0.3.3.0.0.0
*ether2.ipx.nov-pep2	12.1.0.0.1.0.0.129.55.0.0.0.4.3.0.0.0
*ether2.ipx.nov-spx	12.1.0.0.1.0.0.129.55.0.0.0.5.3.0.0.0
*ether2.ipx.nov-pep3	12.1.0.0.1.0.0.129.55.0.0.0.17.3.0.0.0
*ether2.ipx.nov-netbios	12.1.0.0.1.0.0.129.55.0.0.0.20.3.0.0.0

Table A-4 TCP applications

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.tcpmux	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.1.4.0.1.0.0
*ether2.ip-v4.tcp.compressnet-mgmt	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.2.4.0.1.0.0
*ether2.ip-v4.tcp.compressnet	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.3.4.0.1.0.0
*ether2.ip-v4.tcp.rje	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.5.4.0.1.0.0
*ether2.ip-v4.tcp.echo	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.7.4.0.1.0.0
*ether2.ip-v4.tcp.discard	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.9.4.0.1.0.0
*ether2.ip-v4.tcp.systat	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.11.4.0.1.0.0
*ether2.ip-v4.tcp.daytime	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.13.4.0.1.0.0
*ether2.ip-v4.tcp.qotd	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.17.4.0.1.0.0
*ether2.ip-v4.tcp.msp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.18.4.0.1.0.0
*ether2.ip-v4.tcp.chargen	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.19.4.0.1.0.0
*ether2.ip-v4.tcp.ftp-data	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.20.4.0.1.0.0
*ether2.ip-v4.tcp.ftp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.21.4.0.1.0.0
*ether2.ip-v4.tcp.telnet	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.23.4.0.1.0.0
*ether2.ip-v4.tcp.priv-mail	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.24.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.smtp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.25.4.0.1.0.0
*ether2.ip-v4.tcp.nsw-fe	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.27.4.0.1.0.0
*ether2.ip-v4.tcp.msg-icp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.29.4.0.1.0.0
*ether2.ip-v4.tcp.msg-auth	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.31.4.0.1.0.0
*ether2.ip-v4.tcp.dsp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.33.4.0.1.0.0
*ether2.ip-v4.tcp.priv-print	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.35.4.0.1.0.0
*ether2.ip-v4.tcp.time	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.37.4.0.1.0.0
*ether2.ip-v4.tcp.rap	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.38.4.0.1.0.0
*ether2.ip-v4.tcp.graphics	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.41.4.0.1.0.0
*ether2.ip-v4.tcp.nicname	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.43.4.0.1.0.0
*ether2.ip-v4.tcp.mpm-flags	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.44.4.0.1.0.0
*ether2.ip-v4.tcp.mpm	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.45.4.0.1.0.0
*ether2.ip-v4.tcp.mpm-send	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.46.4.0.1.0.0
*ether2.ip-v4.tcp.ni-ftp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.47.4.0.1.0.0
*ether2.ip-v4.tcp.auditd	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.48.4.0.1.0.0
*ether2.ip-v4.tcp.tacacs	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.49.4.0.1.0.0
*ether2.ip-v4.tcp.xns-time	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.52.4.0.1.0.0
*ether2.ip-v4.tcp.domain	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.53.4.0.1.0.0
*ether2.ip-v4.tcp.xns-ch	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.54.4.0.1.0.0
*ether2.ip-v4.tcp.isi-gl	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.55.4.0.1.0.0
*ether2.ip-v4.tcp.xns-auth	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.56.4.0.1.0.0
*ether2.ip-v4.tcp.priv-term	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.57.4.0.1.0.0
*ether2.ip-v4.tcp.xns-mail	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.58.4.0.1.0.0
*ether2.ip-v4.tcp.priv-file	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.59.4.0.1.0.0
*ether2.ip-v4.tcp.ni-mail	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.61.4.0.1.0.0
*ether2.ip-v4.tcp.acas	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.62.4.0.1.0.0
*ether2.ip-v4.tcp.covia	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.64.4.0.1.0.0
*ether2.ip-v4.tcp.tacacs-ds	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.65.4.0.1.0.0
*ether2.ip-v4.tcp.sql*net	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.66.4.0.1.0.0
*ether2.ip-v4.tcp.gopher	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.70.4.0.1.0.0
*ether2.ip-v4.tcp.netrjs-1	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.71.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.netrjs-2	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.72.4.0.1.0.0
*ether2.ip-v4.tcp.netrjs-3	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.73.4.0.1.0.0
*ether2.ip-v4.tcp.netrjs-4	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.74.4.0.1.0.0
*ether2.ip-v4.tcp.priv-dialout	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.75.4.0.1.0.0
*ether2.ip-v4.tcp.deos	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.76.4.0.1.0.0
*ether2.ip-v4.tcp.priv-rje	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.77.4.0.1.0.0
*ether2.ip-v4.tcp.vettcp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.78.4.0.1.0.0
*ether2.ip-v4.tcp.finger	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.79.4.0.1.0.0
*ether2.ip-v4.tcp.www-http	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.80.4.0.1.0.0
*ether2.ip-v4.tcp.hosts2-ns	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.81.4.0.1.0.0
*ether2.ip-v4.tcp.xfer	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.82.4.0.1.0.0
*ether2.ip-v4.tcp.mit-ml-dev	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.83.4.0.1.0.0
*ether2.ip-v4.tcp.ctf	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.84.4.0.1.0.0
*ether2.ip-v4.tcp.mit-ml-dev	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.85.4.0.1.0.0
*ether2.ip-v4.tcp.mfcobol	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.86.4.0.1.0.0
*ether2.ip-v4.tcp.priv-termlink	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.87.4.0.1.0.0
*ether2.ip-v4.tcp.kerberos	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.88.4.0.1.0.0
*ether2.ip-v4.tcp.su-mit-tg	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.89.4.0.1.0.0
*ether2.ip-v4.tcp.dnsix	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.90.4.0.1.0.0
*ether2.ip-v4.tcp.mit-dov	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.91.4.0.1.0.0
*ether2.ip-v4.tcp.npp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.92.4.0.1.0.0
*ether2.ip-v4.tcp.dcp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.93.4.0.1.0.0
*ether2.ip-v4.tcp.objcall	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.94.4.0.1.0.0
*ether2.ip-v4.tcp.supdup	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.95.4.0.1.0.0
*ether2.ip-v4.tcp.dixie	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.96.4.0.1.0.0
*ether2.ip-v4.tcp.swift-rvf	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.97.4.0.1.0.0
*ether2.ip-v4.tcp.tacnews	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.98.4.0.1.0.0
*ether2.ip-v4.tcp.metagram	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.99.4.0.1.0.0
*ether2.ip-v4.tcp.newacct	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.100.4.0.1.0.0
*ether2.ip-v4.tcp.hostname	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.101.4.0.1.0.0
*ether2.ip-v4.tcp.iso-tsap	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.102.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.gppitnp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.103.4.0.1.0.0
*ether2.ip-v4.tcp.acr-nema	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.104.4.0.1.0.0
*ether2.ip-v4.tcp.csnet-ns	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.105.4.0.1.0.0
*ether2.ip-v4.tcp.3com-tsmux	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.106.4.0.1.0.0
*ether2.ip-v4.tcp.rtelnet	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.107.4.0.1.0.0
*ether2.ip-v4.tcp.snagas	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.108.4.0.1.0.0
*ether2.ip-v4.tcp.pop2	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.109.4.0.1.0.0
*ether2.ip-v4.tcp.pop3	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.110.4.0.1.0.0
*ether2.ip-v4.tcp.sunrpc	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.111.4.0.1.0.0
*ether2.ip-v4.tcp.mcidas	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.112.4.0.1.0.0
*ether2.ip-v4.tcp.auth	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.113.4.0.1.0.0
*ether2.ip-v4.tcp.audionews	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.114.4.0.1.0.0
*ether2.ip-v4.tcp.sftp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.115.4.0.1.0.0
*ether2.ip-v4.tcp.ansanotify	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.116.4.0.1.0.0
*ether2.ip-v4.tcp.uucp-path	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.117.4.0.1.0.0
*ether2.ip-v4.tcp.sqlserv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.118.4.0.1.0.0
*ether2.ip-v4.tcp.nntp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.119.4.0.1.0.0
*ether2.ip-v4.tcp.erpc	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.121.4.0.1.0.0
*ether2.ip-v4.tcp.smakynet	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.122.4.0.1.0.0
*ether2.ip-v4.tcp.ansatrader	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.124.4.0.1.0.0
*ether2.ip-v4.tcp.locus-map	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.125.4.0.1.0.0
*ether2.ip-v4.tcp.unitary	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.126.4.0.1.0.0
*ether2.ip-v4.tcp.locus-con	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.127.4.0.1.0.0
*ether2.ip-v4.tcp.gss-xlicen	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.128.4.0.1.0.0
*ether2.ip-v4.tcp.pwdgen	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.129.4.0.1.0.0
*ether2.ip-v4.tcp.cisco-fna	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.130.4.0.1.0.0
*ether2.ip-v4.tcp.cisco-tna	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.131.4.0.1.0.0
*ether2.ip-v4.tcp.cisco-sys	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.132.4.0.1.0.0
*ether2.ip-v4.tcp.statsrv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.133.4.0.1.0.0
*ether2.ip-v4.tcp.ingres-net	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.134.4.0.1.0.0
*ether2.ip-v4.tcp.loc-srv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.135.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.profile	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.136.4.0.1.0.0
*ether2.ip-v4.tcp.netbios-ns	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.137.4.0.1.0.0
*ether2.ip-v4.tcp.netbios-dgm	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.138.4.0.1.0.0
*ether2.ip-v4.tcp.netbios-ssn	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.139.4.0.1.0.0
*ether2.ip-v4.tcp.emfis-data	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.140.4.0.1.0.0
*ether2.ip-v4.tcp.emfis-cntl	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.141.4.0.1.0.0
*ether2.ip-v4.tcp.bl-idm	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.142.4.0.1.0.0
*ether2.ip-v4.tcp.imap2	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.143.4.0.1.0.0
*ether2.ip-v4.tcp.news	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.144.4.0.1.0.0
*ether2.ip-v4.tcp.uaac	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.145.4.0.1.0.0
*ether2.ip-v4.tcp.iso-tp0	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.146.4.0.1.0.0
*ether2.ip-v4.tcp.iso-ip	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.147.4.0.1.0.0
*ether2.ip-v4.tcp.cronus	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.148.4.0.1.0.0
*ether2.ip-v4.tcp.aed-512	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.149.4.0.1.0.0
*ether2.ip-v4.tcp.sql-net	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.150.4.0.1.0.0
*ether2.ip-v4.tcp.hems	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.151.4.0.1.0.0
*ether2.ip-v4.tcp.bftp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.152.4.0.1.0.0
*ether2.ip-v4.tcp.netsc-prod	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.154.4.0.1.0.0
*ether2.ip-v4.tcp.netsc-dev	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.155.4.0.1.0.0
*ether2.ip-v4.tcp.sqlsrv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.156.4.0.1.0.0
*ether2.ip-v4.tcp.knet-cmp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.157.4.0.1.0.0
*ether2.ip-v4.tcp.pcmil-srv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.158.4.0.1.0.0
*ether2.ip-v4.tcp.nss-routing	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.159.4.0.1.0.0
*ether2.ip-v4.tcp.snmp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.161.4.0.1.0.0
*ether2.ip-v4.tcp.snmptrap	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.162.4.0.1.0.0
*ether2.ip-v4.tcp.cmip-man	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.163.4.0.1.0.0
*ether2.ip-v4.tcp.cmip-agent	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.164.4.0.1.0.0
*ether2.ip-v4.tcp.xns-courier	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.165.4.0.1.0.0
*ether2.ip-v4.tcp.s-net	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.166.4.0.1.0.0
*ether2.ip-v4.tcp.namp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.167.4.0.1.0.0
*ether2.ip-v4.tcp.rsvd	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.168.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.send	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.169.4.0.1.0.0
*ether2.ip-v4.tcp.print-srv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.170.4.0.1.0.0
*ether2.ip-v4.tcp.multiplex	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.171.4.0.1.0.0
*ether2.ip-v4.tcp.cl-1	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.172.4.0.1.0.0
*ether2.ip-v4.tcp.xyplex-mux	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.173.4.0.1.0.0
*ether2.ip-v4.tcp.mailq	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.174.4.0.1.0.0
*ether2.ip-v4.tcp.vmnnet	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.175.4.0.1.0.0
*ether2.ip-v4.tcp.genrad-mux	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.176.4.0.1.0.0
*ether2.ip-v4.tcp.nextstep	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.178.4.0.1.0.0
*ether2.ip-v4.tcp.bgp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.179.4.0.1.0.0
*ether2.ip-v4.tcp.ris	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.180.4.0.1.0.0
*ether2.ip-v4.tcp.unify	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.181.4.0.1.0.0
*ether2.ip-v4.tcp.audit	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.182.4.0.1.0.0
*ether2.ip-v4.tcp.ocbinder	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.183.4.0.1.0.0
*ether2.ip-v4.tcp.ocserver	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.184.4.0.1.0.0
*ether2.ip-v4.tcp.remote-kis	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.185.4.0.1.0.0
*ether2.ip-v4.tcp.kis	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.186.4.0.1.0.0
*ether2.ip-v4.tcp.aci	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.187.4.0.1.0.0
*ether2.ip-v4.tcp.mumps	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.188.4.0.1.0.0
*ether2.ip-v4.tcp.qft	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.189.4.0.1.0.0
*ether2.ip-v4.tcp.gacp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.190.4.0.1.0.0
*ether2.ip-v4.tcp.prospéro	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.191.4.0.1.0.0
*ether2.ip-v4.tcp.osu-nms	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.192.4.0.1.0.0
*ether2.ip-v4.tcp.srmp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.193.4.0.1.0.0
*ether2.ip-v4.tcp.irc	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.194.4.0.1.0.0
*ether2.ip-v4.tcp.dn6-nlm-aud	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.195.4.0.1.0.0
*ether2.ip-v4.tcp.dn6-smm-red	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.196.4.0.1.0.0
*ether2.ip-v4.tcp.dls	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.197.4.0.1.0.0
*ether2.ip-v4.tcp.dls-mon	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.198.4.0.1.0.0
*ether2.ip-v4.tcp.smux	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.199.4.0.1.0.0
*ether2.ip-v4.tcp.src	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.200.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.at-rtmp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.201.4.0.1.0.0
*ether2.ip-v4.tcp.at-nbp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.202.4.0.1.0.0
*ether2.ip-v4.tcp.at-3	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.203.4.0.1.0.0
*ether2.ip-v4.tcp.at-echo	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.204.4.0.1.0.0
*ether2.ip-v4.tcp.at-5	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.205.4.0.1.0.0
*ether2.ip-v4.tcp.at-zis	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.206.4.0.1.0.0
*ether2.ip-v4.tcp.at-7	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.207.4.0.1.0.0
*ether2.ip-v4.tcp.at-8	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.208.4.0.1.0.0
*ether2.ip-v4.tcp.tam	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.209.4.0.1.0.0
*ether2.ip-v4.tcp.z39-50	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.210.4.0.1.0.0
*ether2.ip-v4.tcp.914c-g	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.211.4.0.1.0.0
*ether2.ip-v4.tcp.anet	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.212.4.0.1.0.0
*ether2.ip-v4.tcp.vmpwscs	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.214.4.0.1.0.0
*ether2.ip-v4.tcp.softpc	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.215.4.0.1.0.0
*ether2.ip-v4.tcp.atls	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.216.4.0.1.0.0
*ether2.ip-v4.tcp.dbase	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.217.4.0.1.0.0
*ether2.ip-v4.tcp.mpp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.218.4.0.1.0.0
*ether2.ip-v4.tcp.uarps	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.219.4.0.1.0.0
*ether2.ip-v4.tcp.imap3	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.220.4.0.1.0.0
*ether2.ip-v4.tcp.flm-spx	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.221.4.0.1.0.0
*ether2.ip-v4.tcp.rsh-spx	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.222.4.0.1.0.0
*ether2.ip-v4.tcp.cdc	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.223.4.0.1.0.0
*ether2.ip-v4.tcp.sur-meas	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.243.4.0.1.0.0
*ether2.ip-v4.tcp.link	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.245.4.0.1.0.0
*ether2.ip-v4.tcp.dsp3270	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.246.4.0.1.0.0
*ether2.ip-v4.tcp.ldap	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.133.4.0.1.0.0
*ether2.ip-v4.tcp.https	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.187.4.0.1.0.0
*ether2.ip-v4.tcp.exec	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.0.4.0.1.0.0
*ether2.ip-v4.tcp.login	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.1.4.0.1.0.0
*ether2.ip-v4.tcp.cmd	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.2.4.0.1.0.0
*ether2.ip-v4.tcp.printer	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.3.4.0.1.0.0

Table A-4 TCP applications (Continued)

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.tcp.uucp	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.28.4.0.1.0.0
*ether2.ip-v4.tcp.banyan-vip	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.61.4.0.1.0.0
*ether2.ip-v4.tcp.doom	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.154.4.0.1.0.0
*ether2.ip-v4.tcp.notes	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.72.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-srv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.245.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-tns	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.246.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-tns-srv	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.247.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-coauthor	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.249.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-remdb	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.35.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-names	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.39.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-em1	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.212.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-em2	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.218.4.0.1.0.0
*ether2.ip-v4.tcp.ms-streaming	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.219.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-vp2	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.7.16.4.0.1.0.0
*ether2.ip-v4.tcp.orac1-vp1	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.7.17.4.0.1.0.0
*ether2.ip-v4.tcp.ccmail	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.12.192.4.0.1.0.0
*ether2.ip-v4.tcp.xwin	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.23.112.4.0.1.0.0
*ether2.ip-v4.tcp.quake	16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.101.144.4.0.1.0.0

Table A-5 UDP applications

Protocol Encapsulation	Protocol Identifier (Object ID)
*ether2.ip-v4.udp.echo	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.7.4.0.1.0.0
*ether2.ip-v4.udp.discard	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.9.4.0.1.0.0
*ether2.ip-v4.udp.systat	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.11.4.0.1.0.0
*ether2.ip-v4.udp.daytime	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.13.4.0.1.0.0
*ether2.ip-v4.udp.qotd	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.17.4.0.1.0.0
*ether2.ip-v4.udp.msp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.18.4.0.1.0.0
*ether2.ip-v4.udp.chargen	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.19.4.0.1.0.0
*ether2.ip-v4.udp.priv-mail	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.24.4.0.1.0.0

Table A-5 UDP applications (Continued)

*ether2.ip-v4.udp.nsw-fe	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.27.4.0.1.0.0
*ether2.ip-v4.udp.msg-icp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.29.4.0.1.0.0
*ether2.ip-v4.udp.msg-auth	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.31.4.0.1.0.0
*ether2.ip-v4.udp.dsp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.33.4.0.1.0.0
*ether2.ip-v4.udp.priv-print	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.35.4.0.1.0.0
*ether2.ip-v4.udp.time	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.37.4.0.1.0.0
*ether2.ip-v4.udp.rlp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.39.4.0.1.0.0
*ether2.ip-v4.udp.graphics	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.41.4.0.1.0.0
*ether2.ip-v4.udp.nameserver	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.42.4.0.1.0.0
*ether2.ip-v4.udp.auditd	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.48.4.0.1.0.0
*ether2.ip-v4.udp.re-mail-ck	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.50.4.0.1.0.0
*ether2.ip-v4.udp.la-maint	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.51.4.0.1.0.0
*ether2.ip-v4.udp.xns-time	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.52.4.0.1.0.0
*ether2.ip-v4.udp.domain	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.53.4.0.1.0.0
*ether2.ip-v4.udp.xns-ch	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.54.4.0.1.0.0
*ether2.ip-v4.udp.isi-gl	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.55.4.0.1.0.0
*ether2.ip-v4.udp.xns-auth	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.56.4.0.1.0.0
*ether2.ip-v4.udp.priv-term	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.57.4.0.1.0.0
*ether2.ip-v4.udp.xns-mail	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.58.4.0.1.0.0
*ether2.ip-v4.udp.priv-file	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.59.4.0.1.0.0
*ether2.ip-v4.udp.ni-mail	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.61.4.0.1.0.0
*ether2.ip-v4.udp.bootps	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.67.4.0.1.0.0
*ether2.ip-v4.udp.bootpc	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.68.4.0.1.0.0
*ether2.ip-v4.udp.tftp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.69.4.0.1.0.0
*ether2.ip-v4.udp.priv-dialout	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.75.4.0.1.0.0
*ether2.ip-v4.udp.deos	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.76.4.0.1.0.0
*ether2.ip-v4.udp.priv-rje	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.77.4.0.1.0.0
*ether2.ip-v4.udp.vettcp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.78.4.0.1.0.0
*ether2.ip-v4.udp.hosts2-ns	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.81.4.0.1.0.0
*ether2.ip-v4.udp.xfer	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.82.4.0.1.0.0
*ether2.ip-v4.udp.mit-ml-dev	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.83.4.0.1.0.0
*ether2.ip-v4.udp.ctf	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.84.4.0.1.0.0

Table A-5 UDP applications (Continued)

*ether2.ip-v4.udp.mit-ml-dev	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.85.4.0.1.0.0
*ether2.ip-v4.udp.kerberos	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.88.4.0.1.0.0
*ether2.ip-v4.udp.npp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.92.4.0.1.0.0
*ether2.ip-v4.udp.dcp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.93.4.0.1.0.0
*ether2.ip-v4.udp.dixie	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.96.4.0.1.0.0
*ether2.ip-v4.udp.swift-rvf	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.97.4.0.1.0.0
*ether2.ip-v4.udp.tacnews	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.98.4.0.1.0.0
*ether2.ip-v4.udp.metagram	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.99.4.0.1.0.0
*ether2.ip-v4.udp.iso-tsap	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.102.4.0.1.0.0
*ether2.ip-v4.udp.gppitnp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.103.4.0.1.0.0
*ether2.ip-v4.udp.csnet-ns	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.105.4.0.1.0.0
*ether2.ip-v4.udp.3com-tsmux	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.106.4.0.1.0.0
*ether2.ip-v4.udp.pop3	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.110.4.0.1.0.0
*ether2.ip-v4.udp.sunrpc	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.111.4.0.1.0.0
*ether2.ip-v4.udp.audionews	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.114.4.0.1.0.0
*ether2.ip-v4.udp.ansanotify	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.116.4.0.1.0.0
*ether2.ip-v4.udp.sqlserv	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.118.4.0.1.0.0
*ether2.ip-v4.udp.cfdpkt	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.120.4.0.1.0.0
*ether2.ip-v4.udp.erpc	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.121.4.0.1.0.0
*ether2.ip-v4.udp.smakynet	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.122.4.0.1.0.0
*ether2.ip-v4.udp.ntp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.123.4.0.1.0.0
*ether2.ip-v4.udp.ansatrader	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.124.4.0.1.0.0
*ether2.ip-v4.udp.unitary	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.126.4.0.1.0.0
*ether2.ip-v4.udp.gss-xlicen	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.128.4.0.1.0.0
*ether2.ip-v4.udp.pwdgen	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.129.4.0.1.0.0
*ether2.ip-v4.udp.cisco-fna	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.130.4.0.1.0.0
*ether2.ip-v4.udp.cisco-tna	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.131.4.0.1.0.0
*ether2.ip-v4.udp.cisco-sys	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.132.4.0.1.0.0
*ether2.ip-v4.udp.statsrv	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.133.4.0.1.0.0
*ether2.ip-v4.udp.loc-srv	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.135.4.0.1.0.0
*ether2.ip-v4.udp.netbios-ns	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.137.4.0.1.0.0
*ether2.ip-v4.udp.netbios-dgm	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.138.4.0.1.0.0

Table A-5 UDP applications (Continued)

*ether2.ip-v4.udp.netbios-ssn	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.139.4.0.1.0.0
*ether2.ip-v4.udp.emfis-data	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.140.4.0.1.0.0
*ether2.ip-v4.udp.emfis-cntl	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.141.4.0.1.0.0
*ether2.ip-v4.udp.bl-idm	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.142.4.0.1.0.0
*ether2.ip-v4.udp.news	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.144.4.0.1.0.0
*ether2.ip-v4.udp.uaac	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.145.4.0.1.0.0
*ether2.ip-v4.udp.iso-tp0	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.146.4.0.1.0.0
*ether2.ip-v4.udp.iso-ip	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.147.4.0.1.0.0
*ether2.ip-v4.udp.cronus	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.148.4.0.1.0.0
*ether2.ip-v4.udp.aed-512	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.149.4.0.1.0.0
*ether2.ip-v4.udp.sql-net	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.150.4.0.1.0.0
*ether2.ip-v4.udp.sgmp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.153.4.0.1.0.0
*ether2.ip-v4.udp.netsc-prod	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.154.4.0.1.0.0
*ether2.ip-v4.udp.netsc-dev	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.155.4.0.1.0.0
*ether2.ip-v4.udp.nss-routing	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.159.4.0.1.0.0
*ether2.ip-v4.udp.sgmp-traps	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.160.4.0.1.0.0
*ether2.ip-v4.udp.snmp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.161.4.0.1.0.0
*ether2.ip-v4.udp.snmpttrap	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.162.4.0.1.0.0
*ether2.ip-v4.udp.cmip-man	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.163.4.0.1.0.0
*ether2.ip-v4.udp.cmip-agent	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.164.4.0.1.0.0
*ether2.ip-v4.udp.xns-courier	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.165.4.0.1.0.0
*ether2.ip-v4.udp.s-net	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.166.4.0.1.0.0
*ether2.ip-v4.udp.namp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.167.4.0.1.0.0
*ether2.ip-v4.udp.rsvd	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.168.4.0.1.0.0
*ether2.ip-v4.udp.send	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.169.4.0.1.0.0
*ether2.ip-v4.udp.print-srv	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.170.4.0.1.0.0
*ether2.ip-v4.udp.multiplex	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.171.4.0.1.0.0
*ether2.ip-v4.udp.cl-1	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.172.4.0.1.0.0
*ether2.ip-v4.udp.xyplex-mux	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.173.4.0.1.0.0
*ether2.ip-v4.udp.mailq	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.174.4.0.1.0.0
*ether2.ip-v4.udp.vmnet	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.175.4.0.1.0.0
*ether2.ip-v4.udp.genrad-mux	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.176.4.0.1.0.0

Table A-5 UDP applications (Continued)

*ether2.ip-v4.udp.xdmcp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.177.4.0.1.0.0
*ether2.ip-v4.udp.nextstep	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.178.4.0.1.0.0
*ether2.ip-v4.udp.ris	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.180.4.0.1.0.0
*ether2.ip-v4.udp.unify	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.181.4.0.1.0.0
*ether2.ip-v4.udp.audit	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.182.4.0.1.0.0
*ether2.ip-v4.udp.ocbinder	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.183.4.0.1.0.0
*ether2.ip-v4.udp.ocserver	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.184.4.0.1.0.0
*ether2.ip-v4.udp.remote-kis	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.185.4.0.1.0.0
*ether2.ip-v4.udp.kis	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.186.4.0.1.0.0
*ether2.ip-v4.udp.aci	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.187.4.0.1.0.0
*ether2.ip-v4.udp.mumps	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.188.4.0.1.0.0
*ether2.ip-v4.udp.osu-nms	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.192.4.0.1.0.0
*ether2.ip-v4.udp.srmp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.193.4.0.1.0.0
*ether2.ip-v4.udp.irc	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.194.4.0.1.0.0
*ether2.ip-v4.udp.dls	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.197.4.0.1.0.0
*ether2.ip-v4.udp.dls-mon	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.198.4.0.1.0.0
*ether2.ip-v4.udp.src	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.200.4.0.1.0.0
*ether2.ip-v4.udp.at-rtmp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.201.4.0.1.0.0
*ether2.ip-v4.udp.at-nbp	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.202.4.0.1.0.0
*ether2.ip-v4.udp.at-3	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.203.4.0.1.0.0
*ether2.ip-v4.udp.at-echo	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.204.4.0.1.0.0
*ether2.ip-v4.udp.at-5	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.205.4.0.1.0.0
*ether2.ip-v4.udp.at-zis	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.206.4.0.1.0.0
*ether2.ip-v4.udp.at-7	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.207.4.0.1.0.0
*ether2.ip-v4.udp.at-8	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.208.4.0.1.0.0
*ether2.ip-v4.udp.tam	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.209.4.0.1.0.0
*ether2.ip-v4.udp.914c-g	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.211.4.0.1.0.0
*ether2.ip-v4.udp.anet	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.212.4.0.1.0.0
*ether2.ip-v4.udp.ipx-tunnel	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.213.4.0.1.0.0
*ether2.ip-v4.udp.vmpwscs	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.214.4.0.1.0.0
*ether2.ip-v4.udp.softpc	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.215.4.0.1.0.0
*ether2.ip-v4.udp.atls	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.216.4.0.1.0.0

Table A-5 UDP applications (Continued)

*ether2.ip-v4.udp.dbase	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.217.4.0.1.0.0
*ether2.ip-v4.udp.uarps	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.219.4.0.1.0.0
*ether2.ip-v4.udp.fln-spx	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.221.4.0.1.0.0
*ether2.ip-v4.udp.rsh-spx	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.222.4.0.1.0.0
*ether2.ip-v4.udp.cdc	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.223.4.0.1.0.0
*ether2.ip-v4.udp.sur-meas	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.243.4.0.1.0.0
*ether2.ip-v4.udp.link	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.245.4.0.1.0.0
*ether2.ip-v4.udp.dsp3270	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.246.4.0.1.0.0
*ether2.ip-v4.udp.ldap	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.1.133.4.0.1.0.0
*ether2.ip-v4.udp.biff	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.0.4.0.1.0.0
*ether2.ip-v4.udp.who	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.1.4.0.1.0.0
*ether2.ip-v4.udp.syslog	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.2.4.0.1.0.0
*ether2.ip-v4.udp.ip-xns-rip	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.8.4.0.1.0.0
*ether2.ip-v4.udp.banyan-vip	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.61.4.0.1.0.0
*ether2.ip-v4.udp.notes	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.5.72.4.0.1.0.0
*ether2.ip-v4.udp.ccmil	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.12.192.4.0.1.0.0
*ether2.ip-v4.udp.quake	16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.101.144.4.0.1.0.0