

RS 16000 Switch Router Getting Started Guide

Release 9.3

36-023-15 Rev. 0A



River
STONE
NETWORKS™

COPYRIGHT NOTICES

© 2002 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。

BSMI (TAIWAN BUREAU OF STANDARDS, METROLOGY AND INSPECTION, MINISTRY OF ECONOMIC AFFAIR)WARNING:

Warning: This is a Class A product. In a domestic environment this product may cause radio interference..

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成電磁干擾，在這種情況下，使用者會被要求採取某些適當的對策。

SAFETY INFORMATION: CLASS 1 LASER TRANSCIVERS

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.

INFORMACIÓN SOBRE LA SEGURIDAD: TRANSMISOR/RECEPTOR LASER DE CLASE 1

Este producto puede utilizar transmisores/receptores láser de Clase 1. Lea la siguiente información de seguridad antes de instalar u operar este producto.

Los transmisores/receptores láser de Clase 1 utilizan un circuito óptico de control de retroalimentación para mantenerse dentro de los límites operativos de la Clase 1. Debido al uso del circuito de control, no es necesario llevar a cabo ajustes o revisiones de mantenimiento. La potencia ha sido configurada en la

fábrica y no puede ser ajustada por el usuario. Los transmisores/receptores láser de Clase 1 cumplen con las siguientes normas de seguridad:

- 21 CFR 1040.10 y 1040.11, Departamento de Salud y Servicios Humanos de los Estados Unidos (Administración de Alimentos y Fármacos)
- Publicación 825 de la IEC (Comisión Internacional Electrotécnica)
- CENELEC EN 60825 (Comité Europeo para la Estandarización Electrotécnica)

Al operar el equipo dentro de sus limitaciones de rendimiento, la potencia del transmisor/receptor láser cumple con los límites de emisión de las tres normas anteriores para los equipos de Clase 1. Los niveles de radiación permitidos por la Clase 1 no se consideran peligrosos.

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.

RADIACIÓN LÁSER Y CONECTORES

Una vez que el conector se encuentra en su sitio, toda la radiación láser permanece dentro de la fibra. La cantidad máxima de poder radiante que emana de la fibra (bajo condiciones normales) es de -12.6 dBm ó 55×10^{-6} vatios.

La remoción del conector óptico del transmisor/receptor permite que la radiación láser sea emitida directamente desde el puerto óptico. La radiación máxima emitida por el puerto óptico (en el peor de los casos) es de 0.8 W cm^{-2} ó $8 \times 10^3 \text{ W m}^{-2} \text{ sr}^{-1}$.

No utilice instrumentos ópticos para visualizar la potencia del láser. El uso de instrumentos ópticos para visualizar la potencia del láser aumenta el riesgo de presentar lesiones en los ojos. Al visualizar la potencia del puerto óptico, es necesario cortar la corriente del adaptador de la red.

SAFETY INFORMATION: WICT1-12 T1 CARD



Warning

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

Advertencia Para reducir el riesgo de un incendio, únicamente utilice un conductor del número 26 AWG o mayor para la línea de telecomunicaciones.

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/E1 WAN 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 Materials 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	About This Guide	1-1
1.1	How to Use This Guide	1-1
1.2	Related Documentation	1-1
2	Overview	2-1
2.1	Functional Layer Terminology	2-1
2.2	System Overview	2-2
2.3	Software Overview	2-3
2.3.1	Bridging	2-3
2.3.2	Port and Protocol VLANs	2-3
2.3.3	Routing	2-3
2.3.4	Layer-4 Switching	2-5
2.3.5	Security	2-5
2.3.6	Quality of Service	2-5
2.3.7	Statistics	2-6
2.3.8	Web Hosting Features	2-6
2.3.9	Management Platforms	2-7
2.4	Hardware Overview	2-8
2.4.1	Chassis	2-8
2.4.2	Midplane	2-9
2.4.3	Fan Assembly	2-10
2.4.4	AC Power Supply	2-10
2.4.5	DC Power Supply	2-10
2.4.6	Control Modules	2-11
2.4.7	Control Module with Telco Connector	2-12
2.4.8	Control Module with 4 Gigabit-Ethernet Ports	2-15
2.4.9	Gigabit Ethernet Line Card	2-19
2.4.10	CWDM Line Card	2-19
3	Hardware Installation	3-1
3.1	Safety Considerations En Espanol -- Appendix B	3-1
3.1.1	Preventing Injury	3-1
3.1.2	Preventing Equipment Damage	3-1
3.2	Hardware Specifications	3-2
3.3	Installing the Hardware	3-3
3.3.1	General Installation Requirements	3-3
3.3.2	Verifying Your Shipment	3-3
3.3.3	Installing the Rack Mounting Brackets	3-4
3.3.4	Installing the Chassis	3-5
3.3.5	Installing AC Power Supplies	3-7

3.3.6	Installing DC Power Supplies	3-8
3.3.7	Installing the Fan Assembly	3-12
3.3.8	Installing the Control Module	3-13
3.3.9	Installing Line Cards	3-15
3.3.10	Installing SFP Transceivers	3-15
3.3.11	Extracting SFP Transceivers	3-16
3.3.12	Attaching the Segment Cables	3-20
4	Initial Configuration	4-1
4.1	Powering on the RS 16000	4-1
4.2	Starting the Command Line Interface	4-4
4.2.1	CLI Access Modes	4-4
4.2.2	Basic Line Editing Commands	4-5
4.3	Configuration Changes and Saving the Configuration File	4-6
4.3.1	Activating the Configuration Commands in the Scratchpad	4-6
4.3.2	Saving the Active Configuration to the Startup Configuration File	4-7
4.3.3	Viewing the Current Configuration	4-8
4.3.4	Viewing Port Status	4-8
4.4	Setting the Basic System Information	4-10
4.5	Setting Up Passwords	4-13
4.5.1	If You Forget Your Passwords	4-14
4.6	Setting Up SNMP	4-16
4.6.1	Setting the Community string	4-16
4.6.2	Improving SNMP Security	4-17
4.6.3	Supported MIBs	4-18
4.7	Setting the DNS Domain Name and Address	4-20
4.8	Setting the SYSLOG Parameters	4-22
4.9	Using Redundant Control Modules	4-23
4.9.1	Failover	4-24
4.9.2	Communicating with the Backup Control Module	4-25
4.9.3	Redundant Control Module Issues	4-26
5	Software Management	5-1
5.1	Upgrading System Image Software	5-1
5.2	Upgrading Boot PROM Software	5-3
5.3	Loading Software from the Network	5-5
5.3.1	Loading Image Software from a TFTP Server	5-5
5.3.2	Loading Image Software from a BootP/TFTP Server	5-7
5.4	Hitless Software Upgrade	5-8
5.4.1	Hitless Upgrade Example	5-9
5.5	Upgrading FPGA Code	5-11
5.5.1	Upgrading FPGA Code from a TFTP Server	5-11
5.5.2	Upgrading FPGA Code from a Flash RAM Card	5-12
A	Troubleshooting	A-1

B	International Safety Information	B-1
B.1	CONSIDERACIONES DE SEGURIDAD	B-1
5.5.3	Prevencción de Lesiones	B-1
	Index.	Index-1

LIST OF FIGURES

Figure 2-1	Front View of the RS 16000 chassis	2-8
Figure 2-2	Rear view of the RS 16000 chassis	2-9
Figure 2-3	Front view of a fully loaded RS 16000 chassis	2-9
Figure 2-4	DC power supply front view	2-11
Figure 2-5	Front panel view of Control Module options	2-12
Figure 2-6	Front panel of Control Module with Telco connector	2-12
Figure 2-7	Front panel of Control Module with Gigabit Ethernet ports	2-16
Figure 2-8	Front panel of Gigabit Ethernet SFP line card	2-19
Figure 3-1	Installing the RS 16000 rack mounting brackets	3-4
Figure 3-2	Installing the RS 16000 chassis in an equipment rack	3-5
Figure 3-3	AC power supply installation	3-7
Figure 3-4	DC power supply installation	3-9
Figure 3-5	DC power supply front panel	3-10
Figure 3-6	Installing the fan assembly	3-12
Figure 3-7	Installing a Control Module	3-13
Figure 3-8	Installing SFP transceivers	3-16
Figure 3-9	Extracting an IBM SFP transceiver	3-17
Figure 3-10	Extracting a PicoLight SFP transceiver	3-18
Figure 3-11	Extracting an Agilent SFP transceiver	3-19
Figure 3-12	Extracting a Finisar SFP transceiver	3-20

LIST OF TABLES

Table 2-1	ISO 7-layer model and RS 16000 capabilities	2-1
Table 2-2	Hardware and software capabilities	2-2
Table 2-3	AC power supply specifications	2-10
Table 2-4	DC power supply specifications	2-11
Table 2-5	DB-9 pin assignments	2-14
Table 2-6	RJ-45 console connector pin assignments	2-14
Table 2-7	RJ-21 connector pin assignments	2-15
Table 2-8	SFP transceiver media specifications	2-17
Table 2-9	Port status LEDs	2-18
Table 2-10	CWDM line card specifications	2-20
Table 2-11	WDM media specifications	2-21
Table 3-1	Physical and environmental specifications	3-2
Table 3-2	AC power supply environmental specifications	3-8
Table 3-3	DC power safety requirements	3-11
Table 3-4	Requisitos de seguridad del suministro de energía DC	3-11
Table 3-5	DC power supply environmental specifications	3-12
Table 4-1	CLI access modes	4-4
Table 4-2	Common CLI line editing commands	4-5
Table 4-3	Configuration file contents	4-6
Table 4-4	Supported MIBs	4-18
Table 4-5	Types of SYSLOG messages	4-22
Table 4-6	Examples of message types	4-22
Table A-1	Troubleshooting	A-1

1 ABOUT THIS GUIDE

This guide provides a general overview of the hardware and software features, and provides procedures for initial installation and set up of the RS 16000.

1.1 HOW TO USE THIS GUIDE

If You Want To...	See...
Get an overview of the RS 16000 software and hardware features and specifications	Chapter 2, "Overview"
Install the RS 16000 hardware	Chapter 3, "Hardware Installation"
Install and boot the system software; set up the RS 16000	Chapter 4, "Initial Configuration"
Upgrade system software	Chapter 5, "Software Management"
Troubleshoot installation problems	Appendix A, "Troubleshooting."

1.2 RELATED DOCUMENTATION

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

For Information About...	See the...
How to configure and manage the RS 16000	<i>Riverstone Networks RS Switch Router User Guide</i>
The complete syntax for all Command Line Interface (CLI) commands	<i>Riverstone RS Switch Router Command Line Interface Reference Manual</i>
Console and SYSLOG messages	<i>Riverstone RS Switch Router Error Reference Manual</i>

2 OVERVIEW

The RS 16000 performs non-blocking, wire-speed layer-2 switching, layer-3 routing, and layer-4 application switching. This chapter provides a basic overview of the RS 16000 software and hardware feature set.

- If you want to skip this information and install the RS 16000, see [Chapter 3, "Hardware Installation"](#).
- If you want to boot the RS 16000 software and perform basic configuration tasks, see [Chapter 4, "Initial Configuration"](#).



Note For the latest operating software and user documentation, check the Riverstone Networks web site at www.riverstonenet.com.

2.1 FUNCTIONAL LAYER TERMINOLOGY

This guide and other RS documentation refers to layer-2 (L2), layer-3 (L3), and layer-4 (L4) switching and routing. These layers are based on the International Standards Organization (ISO) 7-layer reference model shown in [Table 2-1](#). The RS operates within the layers that are not shaded. Notice that layer 2 is divided into a Media Access Control (MAC) layer, a Link Layer Control (LLC) layer, and an LLC2 layer. The RS 16000 operates at the MAC and LLC layers.

Table 2-1 ISO 7-layer model and RS 16000 capabilities

Layer 7	Application	
Layer 6	Presentation	
Layer 5	Session	
Layer 4	Transport	TCP/UDP - application
Layer 3	Network	IP/IPX - routing
	LLC2	
Layer 2	LLC	
	MAC	Bridging
Layer 1	Physical	Physical Interfaces

2.2 SYSTEM OVERVIEW

The RS 16000 hardware provides wire-speed performance regardless of the performance monitoring, filtering, and Quality of Service (QoS) features enabled by the software. You do not need to accept performance compromises to run QoS or access control lists (ACLs).

The following table lists the basic hardware and software specifications for the RS 16000.

Table 2-2 Hardware and software capabilities

Feature	Specification
Throughput	- Up to 170-Gbps non-blocking Switch Fabric - Up to 90 million packets-per-second routing throughput
Capacity	- Up to 250,000 layer-3 routes - Up to 7,500,000 layer-4 application flows 1,600,000 layer-2 MAC addresses 4,096 virtual LANs (VLANs) 20,000 layer-2 security and access-control filters
Routing protocols	- IP: RIP v1/v2, OSPF, BGP 2, 3, 4, IS-IS - IPX: RIP, SAP - Multicast: IGMP, DVMRP, GARP/GVRP
Bridging and VLAN protocols	802.1d Spanning Tree 802.1Q (VLAN trunking) - Rapid Spanning Tree Protocol (RSTP) - Per-VLAN Spanning Tree (PVST)
Media interface protocols	802.3 (10Base-T) 802.3u (100Base-TX) 802.3x (1000Base-SX, 1000Base-LX, 1000Base-LH) 802.3z (1000Base-SX, 1000Base-LX, 1000Base-LH)
RMON	RMON v1/v2 for each port
Management	- SNMP v1/v2 (v3 is supported with RS SW version 8.1 or later) - Emacs-like Command Line Interface (CLI)
Port mirroring	- Traffic from specific ports - Traffic to specific expansion slots (line cards)
Hot swapping	- Line cards - Redundant Control Module (when redundant Control Module is installed and online) - Power Supply (when redundant supply is installed and online)
Redundancy	- Redundant power supplies - Redundant Control Modules - Virtual Router Redundancy Protocol (VRRP)

2.3 SOFTWARE OVERVIEW

This section describes the features and capabilities of the RS 16000 in greater detail.

2.3.1 Bridging

The RS provides the following types of wire-speed bridging:

Address-based bridging – The RS 16000 performs this type of bridging by looking up a packet's destination address (physical address) in a Layer 2 (L2) lookup table on the line card that received the packet from the network. The L2 lookup table indicates the exit port(s) for the bridged packet. If the packet is addressed to the router's own MAC address, the packet is routed rather than bridged.

Flow-based bridging – The RS 16000 performs this type of bridging by looking up a packet's source and destination address in an L2 lookup table on the line card that received the packet from the network.

Your choice of bridging method does not affect RS 16000 performance. However, address-based bridging requires fewer table entries. Alternately, while flow-based bridging uses more table entries, it provides tighter management and control over bridged traffic, and greater resolution for Remote Network Monitoring (RMON I) statistics.

The RS ports perform address-based bridging by default, but can be configured to perform flow-based bridging on a per-port basis. A port cannot be configured to perform both types of bridging at the same time.

2.3.2 Port and Protocol VLANs

The RS supports the following types of Virtual Local Area Networks (VLANs):

Port-based VLANs – A port-based VLAN is a set of ports that comprises a layer-2 broadcast domain. The RS confines MAC-layer broadcasts to the ports in the VLAN on which the broadcast originates. RS 16000 ports outside the VLAN do not receive the broadcast.

Protocol-based VLANs – A protocol-based VLAN is a named set of ports that comprises an IP, IPX, AppleTalk, DECNet, SNA, IPv6, or L2 broadcast domain. The RS confines protocol-specific broadcasts to the ports within the protocol-based VLAN. Protocol-based VLANs sometimes are called subnet VLANs or layer-3 VLANs.

You can include the same port in more than one VLAN, even in both port-based and protocol-based VLANs. Moreover, you can define VLANs that span across multiple routers. To simplify VLAN administration, the RS 16000 supports 802.1Q trunk ports, which allow you to use a single port to “trunk” traffic from multiple VLANs to another RS or to an L2 switch that supports 802.1Q.

2.3.3 Routing

The RS 16000 provides wire-speed routing for the following protocols:

Internet Protocol (IP) – protocol that switching and routing devices use for moving traffic across the Internet and within many corporate intranets

Internetwork Packet Exchange (IPX) – protocol by Novell used in NetWare products



Note All other protocols that require routing must be tunneled using IP.

By default, the RS 16000 uses one MAC address for all interfaces. The RS 16000 can be configured to have a separate MAC address for each IP interface and a separate MAC address for each IPX interface. When the RS 16000 receives a packet whose destination MAC address is one of the router's IP or IPX interface MAC addresses, the line card that received the packet from the network uses information in the line card's L3 lookup tables (or information supplied by the Control Module) to route the packet to its IP destination(s). See [Section 2.4.6, "Control Modules"](#) for general information about the Control Modules.

You can add secondary IP addresses to the same IP interface, however, you can create only one IP and IPX interface on a single port or VLAN. When you add an interface to a set of ports, you are adding a VLAN to those ports. Ports that contain IP and IPX interfaces can still perform layer-2 bridging.

IP Routing

The RS 16000 supports the following IP unicast routing protocols:

- Routing Information Protocol (RIP v1 and RIP v2)
- Open Shortest Path First (OSPF v2)
- Border Gateway Protocol (BGP 2,3,4)
- Intermediate System to Intermediate System (IS-IS)

IP interfaces do not use a specific routing protocol by default. When you configure an interface for routing, you also specify the routing protocol that the interface will use.

IP Multicast Routing

The RS 16000 supports the following IP multicast routing protocols:

- Internet Group Multicast Protocol (IGMP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- General Attribute Registration Protocol (Cisco Systems)/Generic VLAN Registration Protocol (GARP/GVRP)

The RS 16000 does not use a specific IP multicast routing protocol by default. When you configure an interface for IP multicast, you also specify the routing protocol you want the interface to use.

IPX Routing

The RS 16000 supports the following IPX routing protocols:

IPX RIP – a version of the Routing Information Protocol (RIP) tailored for IPX

IPX SAP – the Service Advertisement Protocol, which allows hosts attached to an IPX network to reach printers, file servers, and other services

By default, IPX routing is enabled on the RS when an IPX interface is created.

2.3.4 Layer-4 Switching

In addition to layer-2 bridging and layer-3 routing, the RS 16000 performs layer-4 switching. Layer-4 switching is based on applications and flows.

Layer-4 Applications – The RS 16000 examines an IP or IPX packet and determines the originating application. This enables you to manage and control traffic based on the application. For IP traffic, the RS 16000 looks at a packet's TCP or UDP port number to determine the application. For IPX packets, the RS 16000 looks at the destination socket to make the determination.

Layer-4 Flows – The RS 16000 can store layer-4 flows on each line card. A layer-4 flow consists of the source and destination addresses in the IP or IPX packet combined with the TCP or UDP source and destination port number (for IP) or the source and destination socket (for IPX). You can therefore manage and control individual flows between hosts on an individual application basis.

A single host can have many individual layer-4 entries in the RS 16000. For example, an IP host might have separate layer-4 application entries for email, FTP, HTTP, and so on, or separate layer-4 flow entries for specific email destinations and for specific FTP and web connections.

2.3.5 Security

The bridging, routing, and application (layer-2, layer-3, and layer-4) support described in previous sections enables you to implement security strategies that meet specific needs. For layer-2, a wide range of bridging filters are available. Additionally, all layers can be protected using Access Control List (ACL) filtering. You can implement the following types of filters and ACLs to secure traffic on the RS 16000:

- Layer-2 source filters (block bridge traffic based on source MAC address)
- Layer-2 destination filters (block bridge traffic based on destination MAC address)
- Layer-2 flow filters (block bridge traffic based on specific source-destination pairs)
- Layer-3 source ACLs (block IP or IPX traffic based on source IP or IPX address)
- Layer-3 destination ACLs (block IP or IPX traffic based on destination IP or IPX address)
- Layer-3 flow ACLs (block IP or IPX traffic based on specific source-destination address pairs)
- Layer-4 flow ACLs (block traffic based on application flows)
- Layer-4 application ACLs (block traffic based on UDP or TCP source and destination ports for IP or source and destination sockets for IPX)

In addition to filtering and ACL, the RS also provides login security in the form of Terminal Access Controller Access Control System (TACACS, TACACS+), Remote Authentication Dial-In User Service (RADIUS), and Secure Session Shells (SSH) version 1.5.

2.3.6 Quality of Service

Although the RS 16000 supplies non-blocking, wire-speed throughput, you can configure the RS 16000 to apply Quality of Service (QoS) policies during peak periods to guarantee service to specific hosts, applications, and flows (source-destination pairs). This is especially useful in networks where the traffic level can exceed the network medium's capacity.

QoS policies can be configured for the following types of traffic:

- Layer-2 prioritization (802.1p)

- Layer-3 source-destination flows
- Layer-4 source-destination flows
- Layer-4 application flows

Quality of Service (QoS) mechanisms supported on the RS 16000 include the following:

- Traffic control queuing
- Weighted random early detection
- Weighted fair queuing
- Strict priority queuing
- QoS traffic control queues
- Type of Service (ToS) octet rewrites



Note Traffic control queuing is based on assigning traffic to one of four queues: control, high, medium, and low. Control traffic (routing protocols, and so on) has the highest priority, high the second highest, and so on. The default priority for all traffic is low.

2.3.7 Statistics

The RS 16000 can provide extensive statistical data on demand. You can access the following types of statistics:

Layer-2 RMON and Management Information Base II (MIB II) Statistics – Port statistics for normal packets and for errors (packets in, packets out, CRC errors, and so on)

Layer-3 RMON v2 Statistics – Statistics for Internet Control Message Protocol (ICMP), IP, IP-interface, IP routing, IP multicast, VLAN

Layer-4 RMON v2 Statistics – Statistics for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

LFAP – Light-weight File Accounting Protocol

Open Application Program Interfaces (APIs) – Slate and FAS Lite.

2.3.8 Web Hosting Features

The RS 16000 provides features that support and improve performance for high-capacity web access:

Load balancing – allows incoming HTTP requests to a company's web site to be distributed across several physical servers. If one server should fail, other servers can pick up the workload.

Web caching – allows HTTP requests from internal users to Internet sites to be redirected to cached web objects on local servers. Not only is response time faster, since requests can be handled locally, but overall WAN bandwidth usage is reduced.

Session persistence – In certain situations where load balancing is being used, it may be critical that all traffic for the client be directed to the same physical server for the duration of the session; this is the concept of *session persistence*.

TCP persistence – a binding is determined by the matching the source IP/port address as well as the virtual destination IP/port address.

Secure Sockets Layer (SSL) persistence – a binding is determined by matching the source IP address and the virtual destination IP/port address. Note that requests from *any* source socket with the client IP address are considered part of the same session.

Sticky persistence – a binding is determined by matching the source and destination IP addresses only. This allows all requests from a client to the same virtual address to be directed to the same load balancing server.

Virtual private network (VPN) persistence – for VPN traffic using Encapsulated Security Payload (ESP) mode of IPsec, a binding is determined by matching the source and destination IP addresses in the secure key transfer request to subsequent client requests.

IP persistence – Used for L3 persistence of load balancing sessions.

2.3.9 Management Platforms

You can manage the RS using the following management platforms:

- **Command Line Interface (CLI)** – An Emacs editor-like interface that accepts typed commands and responds when applicable with messages or tables. Use the CLI to perform the basic setup procedures described in [Chapter 4, "Initial Configuration"](#).
- **Simple Network Management Protocol (SNMP) MIBs and traps** – The RS supports SNMP v1/v2 (v3 is supported with RS SW version 8.1 or later) and many standard networking MIBs. The RS 16000's SNMP agent is accessed using integration software such as HP OpenView 5.x on Windows NT or Solaris 2.x, or Aprisma SPECTRUM on Windows NT or Solaris 2.x. Setting up SNMP on the RS 16000 is described in [Chapter 4, "Initial Configuration"](#).

2.4 HARDWARE OVERVIEW

This section describes and illustrates the RS 16000 hardware components (installing the hardware is described in [Chapter 3, "Hardware Installation"](#)):

- Chassis, including the midplane
- Fan Assembly
- Power supply
- Control Modules
- Line card

2.4.1 Chassis

[Figure 2-1](#) and [Figure 2-2](#) show the various components of the RS 16000 chassis.

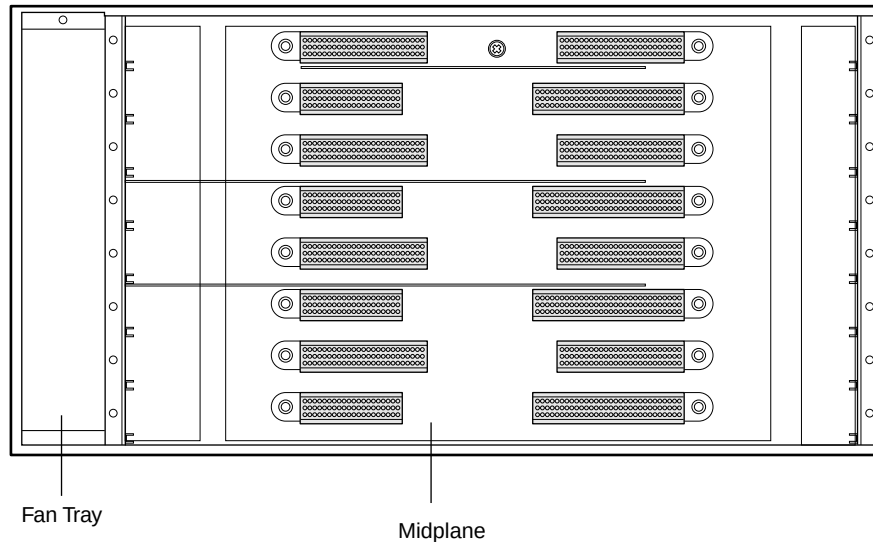


Figure 2-1 Front View of the RS 16000 chassis

The RS 16000 chassis contains 8 horizontal slots for Control Modules and line cards. These slots are numbered 1 to 8 with the number 1 slot at the bottom of the chassis. Slot 1 or slot 2 must contain a Control Module (See [Section 2.4.6, "Control Modules"](#) for more information). If slot 1 contains a Control Module, slot 2 is available for a backup Control Module or a line card. If slot 1 is empty (blank panel), slot 2 must contain a Control Module. With two Control Modules installed, the module in slot 1 is the primary Control Module. The fan assembly plugs into the front of the chassis. Power supplies are installed in the rear of the chassis. Either one AC supply or one DC power supply is required for operation. Two AC supplies or two DC supplies are required for redundant operation (the chassis supports up to three power supplies). AC and DC power supplies cannot be intermixed in the system.

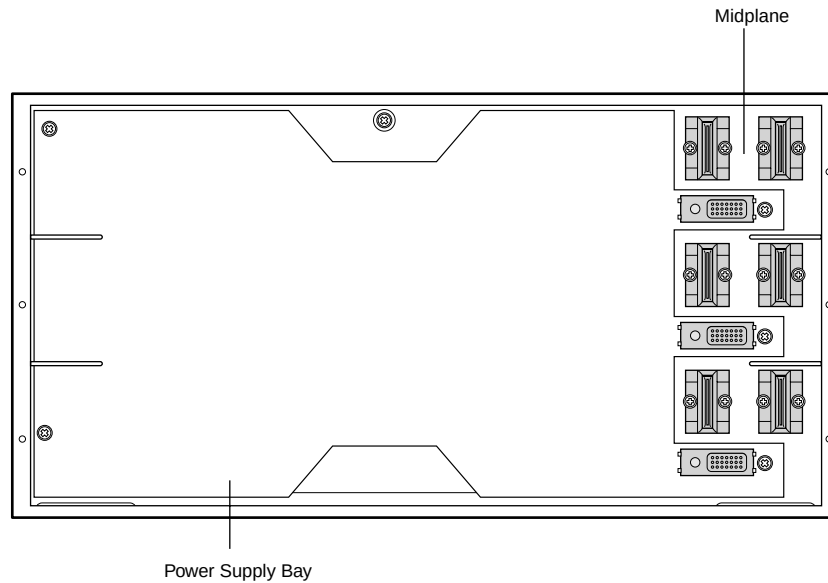


Figure 2-2 Rear view of the RS 16000 chassis

Figure 2-3 shows an RS 16000 (front view) fully loaded with 2 Control Modules and 6 Gigabit Ethernet line cards.

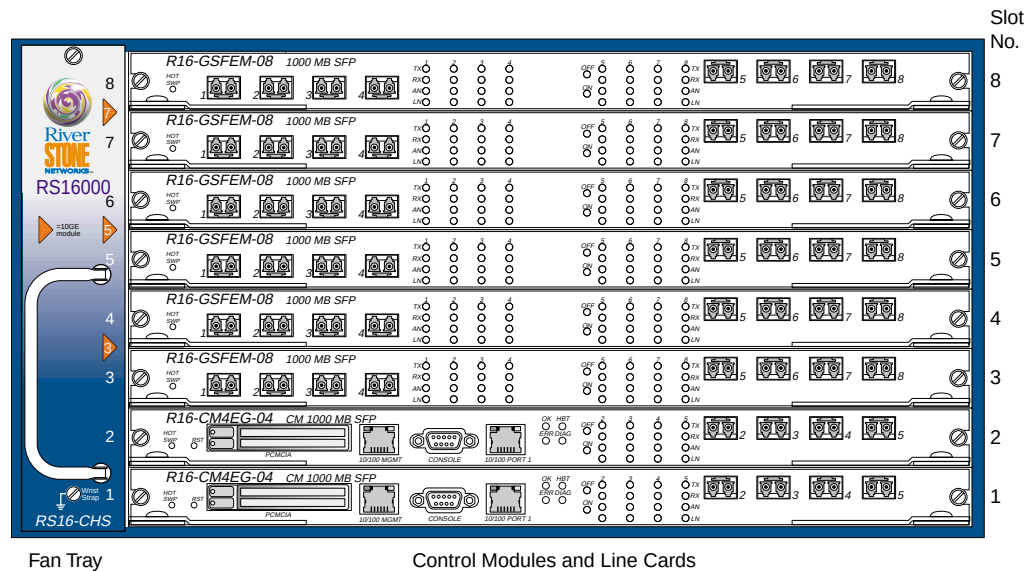


Figure 2-3 Front view of a fully loaded RS 16000 chassis

2.4.2 Midplane

The RS 16000 has an integrated midplane that provides connectivity for front- and rear-insertion components. Control Modules, line cards, and the fan assembly are inserted from the front of the chassis; the power supplies are inserted from the rear of the chassis.

2.4.3 Fan Assembly

The RS 16000 contains a fan assembly that provides a cooling air flow across the Control Modules and line cards. The fan assembly is located to the left of the horizontal slots in the front of the chassis. The fan assembly contains six fans.

2.4.4 AC Power Supply

The AC power supply autosenses over the range of 100 to 240 VAC and supplies its +3.4, +5, and +12 VDC outputs to the midplane. One supply provides enough current to operate a fully-populated chassis. An additional power supply can be added for redundancy (the chassis supports up to three supplies). The power supply has its own internal cooling fans. The vent on the side of the power supply is the inlet vent for the cooling fans.

To protect operational continuity against a power supply failure, install a redundant supply. Each supply provides 725 Watts for a total power output of 1450 Watts (2275 Watts with three supplies installed). When two or three power supplies are active in the RS 16000, they load share with each supply delivering a prorated percentage of the current needed. Moreover, if one power supply fails, the other power supplies immediately assume the entire load thus preventing an operational disruption.

[Table 2-3](#) lists the AC power supply specifications.

The AC power supply has a green status LED. When the status LED is lit, the power supply is connected to an appropriate power source and is generating the proper DC outputs. The status LED lights when the power supply is switched on, not when the power supply is plugged into a power source.

Table 2-3 AC power supply specifications

Specification	Measurement
Dimensions	17" (L) x 7.5" (W) x 2.5" (H)
Weight	12.9 lbs. (5.8 Kg)
Power Output	725 Watts
Input Voltage Range	100-240 VAC, 50-60 Hz
Output Voltage	+3.4, +5, +12 VDC

2.4.5 DC Power Supply

The DC power supply requires input voltage in the range of 48-60 VDC and supplies +3.4, +5, and +12 VDC to the midplane. One power supply provides enough current to operate a fully-populated chassis. An additional power supply can be added to provide redundant power (the chassis supports up to three supplies). The power supply has its own internal cooling fans. The vent on the side of the power supply is the inlet vent for the cooling fans.

The RS 16000 DC power supply front panel contains three power terminals: one positive (+) terminal and two negative (-) terminals (A and B). Also on the front panel are two earth ground terminals.

[Table 2-4](#) lists the DC power supply specifications.

To protect operational continuity against a power supply failure, install a redundant supply. Each power supply provides 725 Watts for a total power output of 1450 Watts (2275 Watts with three supplies installed). When two or three power supplies are active in the RS 16000, they load share with each supply delivering a prorated percentage of the current needed. Moreover, if one power supply fails, the other power supplies immediately assume the entire load thus preventing an operational disruption.

Figure 2-4 shows a front view of the DC power supply.

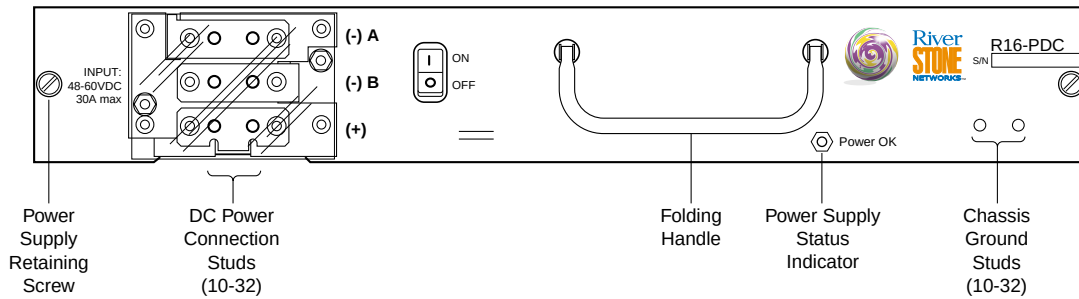


Figure 2-4 DC power supply front view

Table 2-4 DC power supply specifications

Specification	Measurement
Dimensions	17" (L) x 7.5" (W) x 2.5" (H)
Weight	12.8 lbs. (5.8 Kg)
Power Output	725 Watts
Input Voltage Range	48-60 VDC
Input Current (max)	30 A
Output Voltage	+3.4, +5, +12 VDC

2.4.6 Control Modules

The Control Module is the central processing unit of the RS 16000. It contains system-wide bridging and routing tables. Traffic that does not yet have an entry in the L2 and L3/L4 lookup tables on individual line cards is sent to the Control Module. After processing traffic, the Control Module updates the L2 and L3/L4 tables on the line cards that received the traffic. The line cards thus “learn” how to forward traffic. Figure 2-5 shows the front panels of the two available Control Module options. Later sections describe each module.

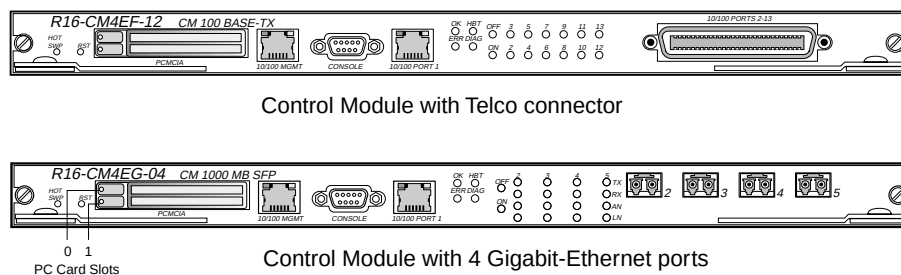


Figure 2-5 Front panel view of Control Module options

Boot Flash

Each Control Module has a boot flash containing the boot software and configuration files. The system software image file typically resides on a 32-megabyte PCMCIA card, but can also reside on a TFTP server or BootP/TFTP server. There are two PCMCIA card slots on the Control Modules; the topmost is slot 0 and beneath it is slot 1.

Memory Module

The Control Module uses memory to hold routing tables, bridging tables, and other tables. The factory configuration for the Control Modules is 512 MB (two 256 MB S0-DIMMs).

2.4.7 Control Module with Telco Connector

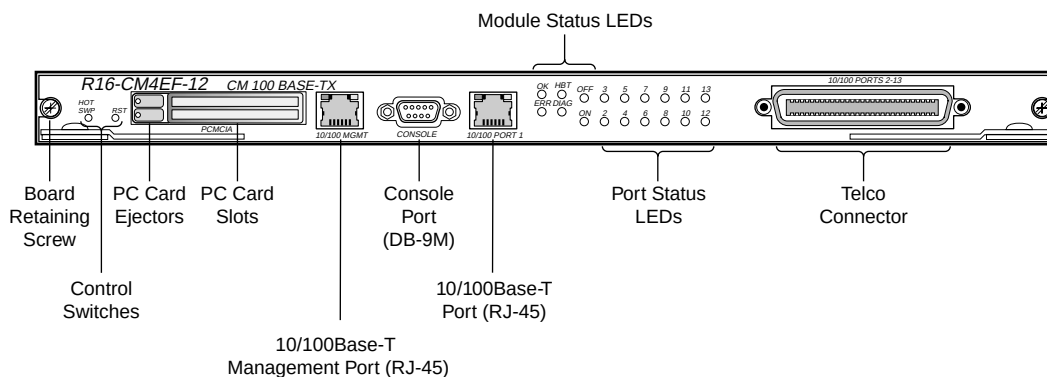


Figure 2-6 Front panel of Control Module with Telco connector

External Controls, Indicators, and Connections

The Control Module with Telco Connector has the following external controls, indicators, and connections:

- The **Control Switches** are recessed in the panel and require a pointed instrument (stylus) to operate them.

- Use the Hot Swap switch (**HOT SWP**) to deactivate the module prior to hot swapping. See the [Riverstone Networks RS Switch Router User Guide](#) for Control Module hot swap information.
 - Use the Reset switch (**RST**) to reboot the Control Module CPU.
- PC card flash memory slots (**PCMCIA**) hold the flash memory cards that contain the shipped system image software.
- 10/100 Base-T Management Port (**10/100 MGMT**) can be used for connection to a management terminal or a PC running terminal emulation software (in-band management). [Table 2-6](#) shows the pin assignments for this RJ-45 connector.
- The **CONSOLE** port is a male DB-9 Data Communications Equipment (DCE) port for serial connection to a management terminal or PC running terminal emulation software. Use this port and the supplied serial cable to establish a direct CLI connection to the RS 16000 (out-of-band management). [Table 2-5](#) shows the pin assignments for this connector.
- **10/100 PORT1** is a 10/100 Base-T port that can be used for general Ethernet port functions or for direct connection to a server that will provide services such as Light-Weight Flow Admission Protocol (LFAP), Dynamic Host Configuration Protocol (DHCP), or Light-Weight Directory Access Protocol (LDAP). [Table 2-6](#) shows the pin assignments for this RJ-45 connector.
- The **Module Status LEDs** are comprised of the following:
 - The **OK** LED lights steadily when the RS 16000 successfully completes boot.
 - The **HBT** indicator shows the heartbeat activity between the primary and backup Control Modules. This LED on one Control Module flashes when it receives a heartbeat from its counterpart Control Module. The HBT indicator is inactive with only one Control Module installed.
 - The **ERR** indicator lights steadily if a boot error occurs.
 - The **DIAG** LED flashes while the RS 16000 is booting.
 - The **ON** LED, when lit, indicates that the Control Module is online and is ready to receive, process, and send packets if configured to do so.
 - The **OFF** LED, when lit, indicates that the Control Module is offline (powered off) and is ready for hot swap. The **OFF** LED also is lit briefly during a reboot or reset of the RS 16000 and goes out as soon as the Control Module is properly initialized.
- A **Port Status LED** lights amber to show a valid link on the corresponding Telco port and lights green to show activity on that link.
- **10/100 PORTS 2-13** is an RJ-21 Telco connector that provides twelve 10/100Base-T ports. [Table 2-7](#) shows the pin assignments for this connector.

Control Module DB-9 Connector Pin Assignment

Table 2-5 DB-9 pin assignments

Control Module DB-9 connector (DCE)	Pin number	Management console DB-9 connector (DTE)
Unused	1	Unused
TXD (transmit data)	2	RXD (receive data)
RXD (receive data)	3	TXD (transmit data)
Unused	4	Unused
GND (ground)	5	GND (ground)
DTR (data terminal ready)	6	DSR (data set ready)
CTS (clear to send)	7	RTS (request to send)
RTS (request to send)	8	CTS (clear to send)
Unused	9	Unused

Control Module RJ-45 Connector Pin Assignment

Table 2-6 RJ-45 console connector pin assignments

Control Module RJ-45 connector	Pin Number	Management console RJ-45 connector
TXD (transmit data)	1	RXD (receive data)
TXD (transmit data)	2	RXD (receive data)
RXD (receive data)	3	TXD (transmit data)
Unused	4	Unused
Unused	5	Unused
RXD (receive data)	6	TXD (transmit data)
Unused	7	Unused
Unused	8	Unused

Control Module RJ-21 Connector Pin Assignment

The ports are fanned out from the 50-pin RJ-21 connector using industry-standard pin assignments.

Table 2-7 RJ-21 connector pin assignments

Port number	Connector pin number	Signal	Connector pin number	Signal
1	1	RxD (-)	26	RxD (+)
	2	TxD (-)	27	TxD (+)
2	3	RxD (-)	28	RxD (+)
	4	TxD (-)	29	TxD (+)
3	5	RxD (-)	30	RxD (+)
	6	TxD (-)	31	TxD (+)
4	7	RxD (-)	32	RxD (+)
	8	TxD (-)	33	TxD (+)
5	9	RxD (-)	34	RxD (+)
	10	TxD (-)	35	TxD (+)
6	11	RxD (-)	36	RxD (+)
	12	TxD (-)	37	TxD (+)
7	13	RxD (-)	38	RxD (+)
	14	TxD (-)	39	TxD (+)
8	15	RxD (-)	40	RxD (+)
	16	TxD (-)	41	TxD (+)
9	17	RxD (-)	42	RxD (+)
	18	TxD (-)	43	TxD (+)
10	19	RxD (-)	44	RxD (+)
	20	TxD (-)	45	TxD (+)
11	21	RxD (-)	46	RxD (+)
	22	TxD (-)	47	TxD (+)
12	23	RxD (-)	48	RxD (+)
	24	TxD (-)	49	TxD (+)
	25	Not connected	50	Not connected

2.4.8 Control Module with 4 Gigabit-Ethernet Ports

General information for this module is the same as that for the Control Module with Telco Connector and is in [Section 2.4.6, "Control Modules"](#). This section contains only information specific to the Control Module with 4 Gigabit-Ethernet ports.

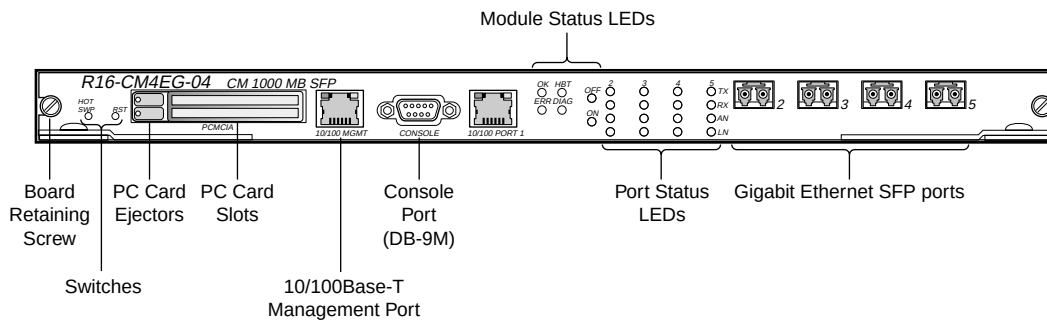


Figure 2-7 Front panel of Control Module with Gigabit Ethernet ports

External Controls, Indicators, and Connections

The Control Module with Gigabit Ethernet ports has the following external controls, indicators, and connections:

- The **Control Switches** are recessed in the panel and require a pointed instrument (stylus) to operate them.
 - Use the Hot Swap switch (**HOT SWP**) to deactivate the module prior to hot swapping. See the [Riverstone Networks RS Switch Router User Guide](#) for Control Module hot swap information.
 - Use the Reset switch (**RST**) to reboot the Control Module CPU.
- PC card flash memory slots (**PCMCIA**) hold the flash memory cards that contain the shipped system image software.
- 10/100 Base-T Management Port (**10/100 MGMT**) can be used for connection to a management terminal or a PC running terminal emulation software (in-band management). [Table 2-6](#) shows the pin assignments for this RJ-45 connector.
- The **CONSOLE** port is a male DB-9 Data Communications Equipment (DCE) port for serial connection to a management terminal or PC running terminal emulation software. Use this port and the supplied serial cable to establish a direct CLI connection to the RS 16000 (out-of-band management). [Table 2-5](#) shows the pin assignments for this connector.
- **10/100 PORT1** is a 10/100 Base-T port that can be used for general Ethernet port functions or for direct connection to a server that will provide services such as Light-Weight Flow Admission Protocol (LFAP), Dynamic Host Configuration Protocol (DHCP), or Light-Weight Directory Access Protocol (LDAP). [Table 2-6](#) shows the pin assignments for this RJ-45 connector.
- The **Module Status LEDs** are comprised of the following:
 - The **OK** LED lights steadily when the RS 16000 successfully completes boot.
 - The **HBT** indicator shows the heartbeat activity between the primary and backup Control Modules. This LED on one Control Module flashes when it receives a heartbeat from its counterpart Control Module. The HBT indicator is inactive with only one Control Module installed.
 - The **ERR** indicator lights steadily on a boot error.
 - The **DIAG** LED flashes while the RS 16000 is booting.
 - The **ON** LED, when lit, indicates that the Control Module is online and is ready to receive, process, and send packets if configured to do so.

- The **OFF** LED, when lit, indicates that the Control Module is offline (powered off) and is ready for hot swap. The **OFF** LED also is lit briefly during a reboot or reset of the RS 16000 and goes out as soon as the Control Module is properly initialized.
- Each SFP transceiver has associated with it four **Port Status LEDs**. [Table 2-9](#) describes the LED display.

Gigabit Ethernet SFP Transceiver Ports

SFP transceivers provide Gigabit Ethernet connectivity to a Control Module across multiple media types and distances. The Control Module provides the power, initialization, and control for each transceiver. Any supported combination of SFP transceivers can be used in a single Control Module. The SFP transceivers are not factory installed; you must order, insert, and connect them per your requirements. Refer to [Section 3.3.10, "Installing SFP Transceivers"](#) for instructions.

The Control Module with Gigabit Ethernet ports accepts the SFP transceivers shown in [Table 2-8](#).

Table 2-8 SFP transceiver media specifications

Port type	Specification
SFP SX (MMF)	• Multi-mode fiber interface • 50 or 62.5 125-mm multi-mode fiber cable terminated with SC connectors • 850 nm wavelength • Maximum of 300 m of cable
SFP LX (SMF-IR)	• Single-mode fiber (intermediate range) interface • 8 or 9 125-mm single-mode fiber cable terminated with SC connectors • 1310 nm wavelength • Maximum of 10 km of cable
SFP LH (SMF-LR)	• Single-mode fiber (long range) interface • 8 or 9 125-mm single-mode fiber cable terminated with SC connectors • 1550 nm wavelength • Maximum of 70 km of cable

Table 2-9 Port status LEDs

LED	Description
Per-SFP RX	Green – indicates when the SFP’s transceiver receives packets. Amber – indicates when the SFP’s transceiver receives flow-control packets.
Per-SFP TX	Green – indicates when the SFP’s transceiver transmits packets. Amber – indicates when the SFP’s transceiver transmits flow-control packets.
Per-SFP AN	Green – indicates that the port hardware has auto negotiated the operating mode of the link between full-duplex and half-duplex. Orange (intermittent) – indicates that auto negotiation is in process. Orange (solid) – indicates a problem with auto negotiation configuration. Red – indicates an auto negotiation failure. This fault may occur if the link partner does not support full duplex. Off – indicates that auto negotiation has been disabled or the link is down.
Per-SFP LINK	Green – indicates that the port hardware detects a cable plugged into the port and a good link is established. Red (intermittent) – indicates that port hardware received an error during operation. Red (solid) – indicates that the port hardware detects a cable plugged into the port, however, a bad link is established. Off – indicates that no link from the port exists.

2.4.9 Gigabit Ethernet Line Card

The 8-port Gigabit Ethernet line card contains 8 independent Ethernet ports that can be individually configured with SFP transceivers. [Figure 2-8](#) shows the front panel of the 8-port Gigabit Ethernet SFP line card.

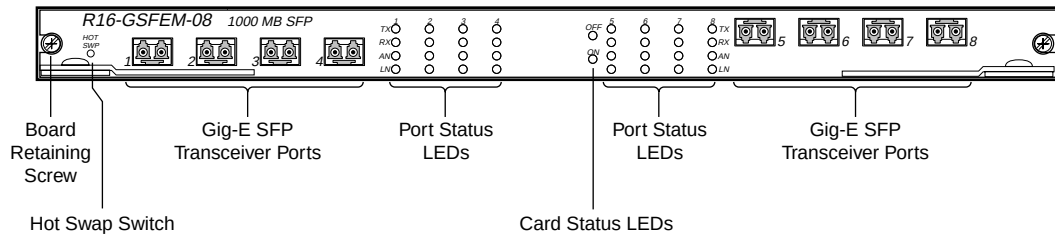


Figure 2-8 Front panel of Gigabit Ethernet SFP line card

SFP transceivers provide the media-specific portion of a Gigabit Ethernet line card, and support Gigabit Ethernet connectivity across multiple media types and distances. The host Gigabit Ethernet line card provides power, initialization, and control for each transceiver. Any combination of SFP transceivers can be used on a single Gigabit Ethernet line card. The SFP transceivers are not factory installed; you must order, insert, and connect them per your requirements. Refer to [Section 3.3.10, "Installing SFP Transceivers"](#) for instructions.

The Gigabit Ethernet line cards accept the SFP transceivers shown in [Table 2-8](#).

External Controls, Indicators, and Connections

The Gigabit Ethernet line card has the following external controls, indicators, and connections:

- Use the Hot Swap switch (**HOT SWP**) to deactivate the module prior to hot swapping. See the [Riverstone Networks RS Switch Router User Guide](#) for line card hot swap information.
- The **Gigabit Ethernet SFP transceiver ports** are described earlier in this section.
- Each SFP transceiver has associated with it four **Port Status LEDs**. [Table 2-9](#) describes the LED display.
- The **Card Status LEDs** are comprised of the following:
 - The **ON** LED, when lit, indicates that the line card is online and is ready to receive, process, and send packets if configured to do so.
 - The **OFF** LED, when lit, indicates that the line card is offline (powered off) and is ready for hot swap. The **OFF** LED also is lit briefly during a reboot or reset of the RS and goes out as soon as the line card is properly initialized.

2.4.10 CWDM Line Card

Wavelength Division Multiplexing (WDM) is a technique that allows simultaneous transmission of multiple signals over a single optical fiber. Each signal to be transmitted (channel) is modulated onto a monochromatic laser carrier with a distinct wavelength. All individual wavelengths are multiplexed onto a single optical fiber and transmitted to

the receiving end. A demultiplexer at the receiving end splits the multiplexed signal into the original, separate signals. WDM technology is capable of carrying all types of optical signals including SONET/SDH, ATM, and Gigabit Ethernet.

Currently, dense WDM (DWDM) technology can typically multiplex 32 signals onto a single fiber. DWDM equipment typically uses the 1530- to 1565-nm wavelength range. This high-density multiplexing is achieved through reducing the gap between adjacent channels to a fraction of a nanometer (about 0.8 nm). DWDM lasers are therefore extremely accurate and may require cooling to maintain their operational accuracy.

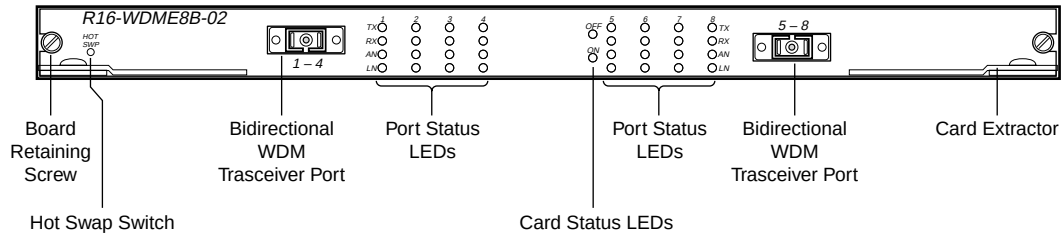
Coarse WDM (CWDM) uses the 1200- to 1600-nm wavelength range with a minimum 20-nm wavelength gap between adjacent channels. Optical components used for CWDM are less accurate and thus less expensive.

CWDM Line Card Specifications

The Riverstone CWDM line card is capable of multiplexing and simultaneously transmitting four signals. It uses the 1495- to 1567-nm wavelength range with a 20-nm gap between adjacent channels. [Table 2-10](#) lists the CWDM line card's specifications.

Table 2-10 CWDM line card specifications

Parameter	Value			
(4) Wavelengths	Wavelength	Minimum	Typical	Maximum
	λ_1	1495 nm	1501 nm	1507 nm
	λ_2	1515	1521	1527
	λ_3	1535	1541	1547
	λ_4	1555 nm	1561 nm	1567 nm
Transmission coding	8B/10B			
Communication speed	1.25 Gb/s per λ			
Average output per channel	-1.5 to 2.0 dBm			
Extinction ratio	10 dB			
Average maximum input power	-3.0 dBm			
Average optical sensitivity	-17 dBm			
Signal detect threshold assertion	-17 dBm			
Signal detect threshold deassertion	-25.5 dBm			



External Controls, Indicators, and Connections

The CWDM line card has the following external controls, indicators, and connections:

- Use the **Hot Swap switch (HOT SWP)** to deactivate the module prior to hot swapping. See the [Riverstone Networks RS Switch Router User Guide](#) for line card hot swap information.
- **Transceiver ports**
- The **Port Status LEDs** show the status of each wavelength in the same fashion as they do for the physical ports on the Gigabit Ethernet line card. [Table 2-9](#) describes the LED display.
- The **Card Status LEDs** comprise the following:
 - The **ON** LED, when lit, indicates that the line card is online and is ready to receive, process, and send packets if configured to do so.
 - The **OFF** LED, when lit, indicates that the line card is offline (powered off) and is ready for hot swap. The **OFF** LED also is lit briefly during a reboot or reset of the RS and goes out as soon as the line card is properly initialized.

Table 2-11 WDM media specifications

Port type	Specification
SX (SMF)	• Single-mode fiber (intermediate range) interface • 8 or 9 125-mm single-mode fiber cable terminated with SC/APC connectors • Maximum of 35 km cable • Receiver sensitivity -17.5 dBm • Optical power budget (Tx power) 10.5 dB



Caution You must connect to the ports of the WDM module using an SC/APC connector (Angled Polished Connector).

3 HARDWARE INSTALLATION

This chapter provides hardware installation instructions, safety considerations, environmental considerations, and regulatory standards.

3.1 SAFETY CONSIDERATIONS *EN ESPAÑOL -- APPENDIX B*



Warning

Read the following safety warnings and product cautions to avoid personal injury or product damage.

3.1.1 Preventing Injury

- To avoid injury, have someone help you lift the chassis out of its shipping crate.
- Never attempt to rack mount the RS 16000 chassis unaided. Ask an assistant to help you lift or hold the chassis.
- Never operate the RS 16000 with exposed power supply bays or line card slots. You can leave the **PCMCIA** card slots exposed but make sure you do not insert any objects other than the appropriate PC flash card(s) into the card slot(s).
- Never operate the RS 16000 if the chassis becomes wet or if the area in which the chassis is installed is wet.

3.1.2 Preventing Equipment Damage

To prevent accidental product damage, observe the following precautions:

- Always use proper electrostatic discharge (ESD) gear when handling the Control Module, backplane, line cards or other internal parts of the RS 16000.
- Make sure there are at least 3 inches (7.62 centimeters) of room on each side of the RS 16000 chassis for air flow to the cooling fans.
- Install the RS 16000 as low as possible in the rack to prevent tipping of the rack.
- If the RS 16000 is to be installed in a closed or multi-unit rack, make sure that the ambient temperature around the unit does not exceed the operating temperature range listed in [Table 3-1](#).
- Maintain reliable grounding of rack-mounted equipment, with particular attention to power supply connections other than direct connections to the branch circuit, such as power strips.

3.2 HARDWARE SPECIFICATIONS

The following table lists the physical and environmental specifications for the RS 16000.

Table 3-1 Physical and environmental specifications

Specification	Measurement
Dimensions	8.75" (H) x 17.5" (W) x 22" (L)
Component Weights	Chassis with fan assembly: 33.5 lbs. (15.2 Kg) Power Supply (AC or DC): 13 lbs. (5.9 Kg) Telco Control Module: 4.5 lbs. (2.0 Kg) Gig-E Control Module: 5.5 lbs. (2.5 Kg) Line card: 5.5 lbs. (2.5 Kg)
Total Weight (fully loaded, two power supplies)	Approximately 105 lbs. (47.6 Kg)
AC power	100-240 VAC, 50-60 Hz
DC Power	48-60 VDC
Operating Temperature	Fahrenheit: 41° F to 104° F Centigrade: 5° C to 40° C
Non-Operating Temperature	Fahrenheit: -22° F to 164° F Centigrade: -30° C to 73° C
Operating Humidity	15% to 90% (non-condensing)

3.3 INSTALLING THE HARDWARE

This section contains descriptions of the necessary operations for a successful installation of the RS 16000.

3.3.1 General Installation Requirements

The RS 16000 installation must meet the following environmental and electromechanical requirements.

- **Operating ambient temperature:** If the RS 16000 is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, install the RS 16000 in an environment that will not exceed the maximum rated ambient temperature (T_{mra}) of 40° C.
- **Air flow:** The RS 16000 installation must provide proper air flow to ensure safe equipment operation. To this end, avoid blocking fans and vents.
- **Mechanical loading:** Ensure the RS 16000 rack installation does not create a hazardous condition due to uneven mechanical loading.
- **Circuit overloading:** The RS 16000 must have a proper connection to the supply circuit and account for the effect that circuit overloading might have on overcurrent protection and supply wiring. Ensure the power connection meets the ratings stated on the equipment nameplate.
- **Reliable earthing:** The RS 16000 rack installation must maintain reliable earthing. Pay particular attention to supply connections other than direct connections to the branch circuit, such as power strip connections.

**Warning**

This equipment is to be installed only in Restricted Access Areas (Dedicated Equipment Rooms, Electrical Closets, or the like) in accordance with Articles 110-26 and 110-27 of the 1999 National Electrical Code ANSI/NFPA 70.

**Advertencia**

Este equipo deberá instalarse únicamente en Areas de Acceso Restringido (recintos dedicados al equipo, armarios eléctricos o similares) según lo estipulado en los Artículos 110-26 y 110-27 del Código Eléctrico Nacional de 1999 ANSI/NFPA 70.

3.3.2 Verifying Your Shipment

Before you begin installing the RS 16000, check your shipment to ensure that everything you ordered arrived securely.

**Warning**

To avoid possible personal injury, have someone help you lift the chassis out of its shipping crate.

**Advertencia**

To avoid possible personal injury, have someone help you lift the chassis out of its shipping crate.

Open the shipping box(es) and verify that you received the following equipment:

- RS 16000 chassis containing a midplane and a fan assembly
- Rack mounting brackets
- A Control Module
- Console cable for connecting a terminal to the Control Module's DB-9 port
- An appropriate, country-specific power cord for each AC power supply ordered
- RS 16000 Media Kit
 - *Riverstone Networks Documentation CD*
 - One PCMCIA card containing the RS 16000 operating system software
 - *Riverstone RS Switch Router Getting Started Guide*
 - Release Notes

Depending on your order, your shipment may also contain some or all of the following:

- One or more power supplies
- Redundant Control Module
- One or more line cards
- Four or more SFP transceivers

3.3.3 Installing the Rack Mounting Brackets

The RS 16000 is shipped without the rack mounting brackets installed. The brackets can be installed in the front or back of the chassis as shown in [Figure 3-1](#).

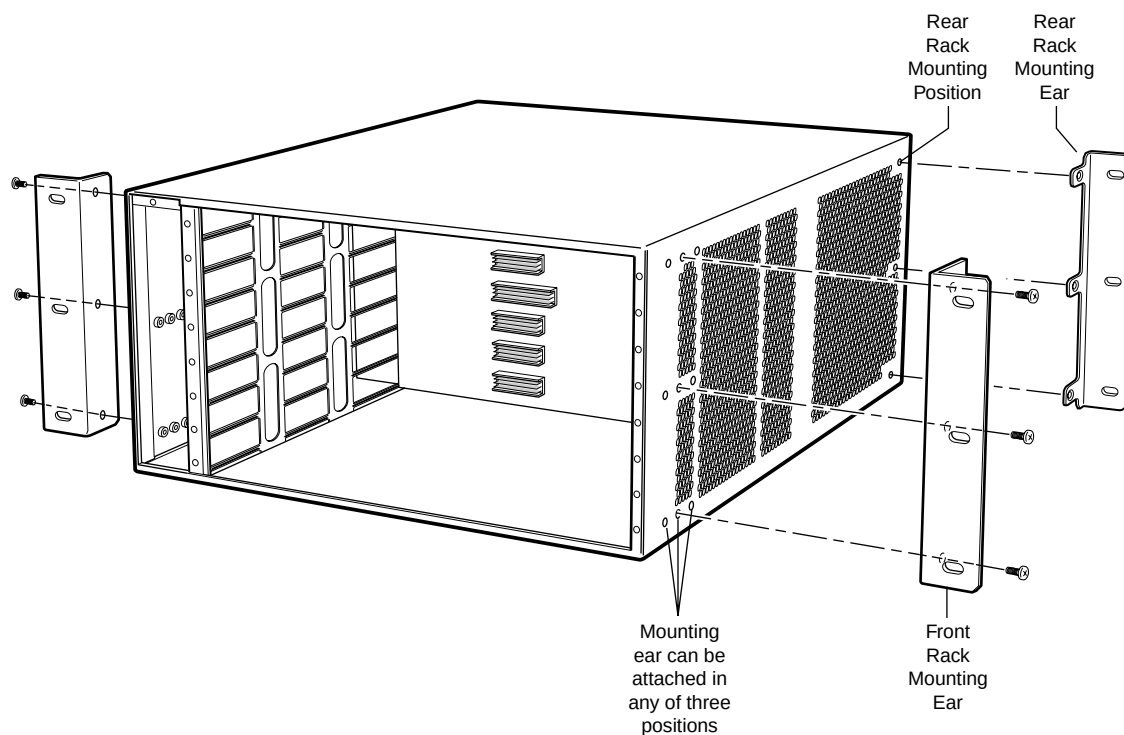


Figure 3-1 Installing the RS 16000 rack mounting brackets

3.3.4 Installing the Chassis

**Warning**

Riverstone Networks, Inc. recommends that only qualified personnel install an RS 16000 chassis.

**Advertencia**

Riverstone Networks, Inc. recomienda que el chasis RS 16000 sea instalado únicamente por personal capacitado.

Install the RS 16000 in a standard 19" equipment rack after the rack mounting brackets have been installed on the chassis, as described in [Section 3.3.3, "Installing the Rack Mounting Brackets"](#). [Figure 3-2](#) shows an example of how to install an RS 16000 chassis in an equipment rack.

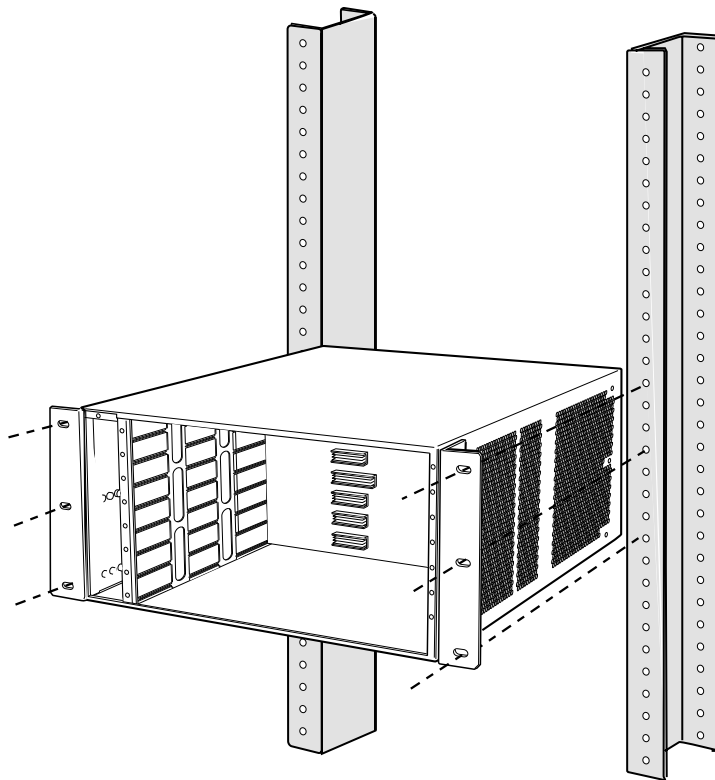


Figure 3-2 Installing the RS 16000 chassis in an equipment rack

**Warning**

Never attempt to install an RS 16000 chassis into a rack by yourself.

**Advertencia**

Nunca intente instalar el chasis del RS 16000 en un rack sin la ayuda de otra persona.

**Warning**

To make lifting and holding the chassis easier, it is recommended that you install the RS 16000 chassis while empty. Remove all line cards, Control Modules, and power supplies.

**Advertencia**

Para facilitar el proceso de levantamiento y sujeción del chasis, se recomienda instalar el chasis del RS 16000 mientras éste se encuentre vacío. Retire todas las tarjetas de línea, los módulos de control y los suministros de energía.

To install the RS 16000 chassis in an equipment rack, use the following procedure:

1. Along with an assistant, lift the chassis into place in the mounting rack.
2. While your assistant holds the chassis in place, use an appropriate screwdriver and mounting screws to attach the front-mounting brackets of the chassis to the mounting rack.

**Warning**

Make sure there are at least 3 inches (7.62 centimeters) of room on each side of the unit for air flow to the cooling fans.

**Advertencia**

Cerciórese de dejar un claro mínimo de 3 pulgadas (7.62 centímetros) en ambos lados de la unidad para permitir el flujo de aire hacia los ventiladores de enfriamiento.

**Warning**

Make sure the screws are tight before your assistant releases the chassis. If you accidentally leave the screws loose, the chassis can fall out of the rack causing damage and personal injury.

**Advertencia**

Cerciórese de que los tornillos estén debidamente ajustados antes de que su asistente suelte el chasis. Si los tornillos no están debidamente ajustados, es posible que el chasis se salga del rack y se dañe.

3.3.5 Installing AC Power Supplies

To install an AC power supply, follow the procedure in this section. For AC power supply environmental specifications, refer to [Table 3-2](#). For operating and physical specifications, refer to [Table 2-3](#).

1. Power off the AC supply, disconnect it from its power source, and disconnect the power cord.
2. From the rear of the chassis, position the power supply between the guides in an open power supply slot; refer to [Figure 3-3](#). Remove blank panels only as necessary to accommodate power supplies.

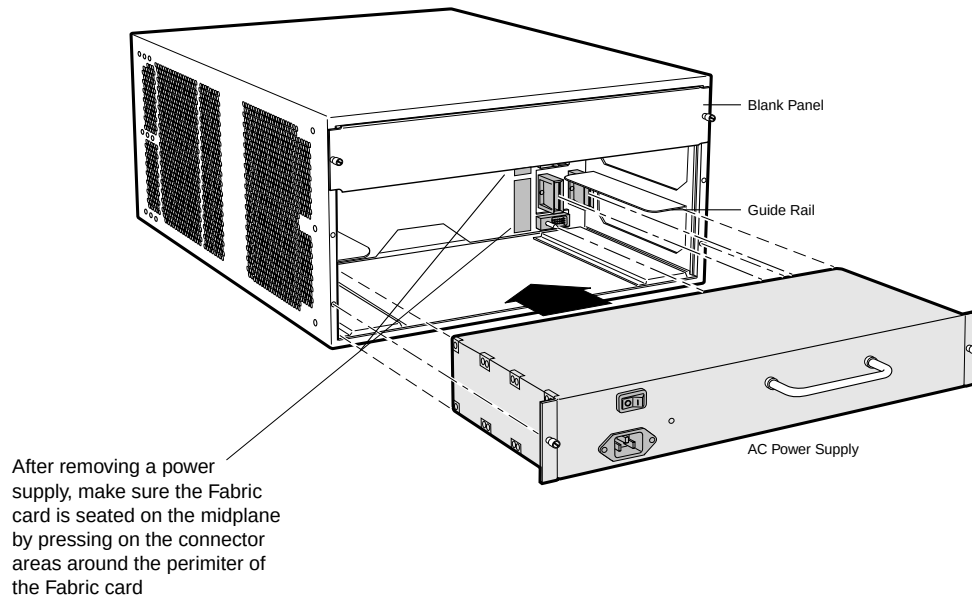


Figure 3-3 AC power supply installation

3. Slide the power supply all the way into the slot, pressing with just enough force to seat the rear connectors into the midplane.
4. Using an appropriate screwdriver, turn the captive screws on the power supply's front panel to lock the power supply into the chassis.
5. Attach the power cord to the supply.



Warning

After removing a power supply from the chassis, check the security of the Fabric card by pressing on the connector areas around its perimeter (refer to [Figure 3-3](#)). You may need to remove one or more blanking panels to access the Fabric card. Replace all panels after completing the procedure.



Warning

Use a single-phase grounded power source located within 6 feet (1.89 meters) of the installation site.



Advertencia

Utilice una fuente de poder monofásica y puesta a tierra, misma que deberá localizarse a un máximo de 6 pies (1.89 metros) de distancia del sitio de instalación.

**Warning**

High leakage current can be caused by multiple power supplies. For this reason, it is essential that each power cord be connected to a separate branch circuit with proper earth connections.

**Advertencia**

El uso de suministros de energía múltiples puede ocasionar altas corrientes de fuga. Por este motivo, resulta esencial conectar cada cable de energía a distintos ramales del circuito, mismos que deberán estar puestos a tierra..

Table 3-2 AC power supply environmental specifications

Specification	Measurement
Operating Temperature	+5° to +40°C (41° to 104°F)
Non-operating Temperature	-30° to +73°C (-22° to 164°F)
Operating Humidity	15% to 90% (non-condensing)

**Warning**

After removing a power supply from the chassis, check the security of the Fabric card by pressing on the connector areas around its perimeter (refer to [Figure 3-3](#)). You may need to remove one or more blanking panels to access the Fabric card. Replace all panels after completing the procedure.

3.3.6 Installing DC Power Supplies

**Warning**

The RS 16000 with DC power supplies should be installed only in Restricted Access Areas (Dedicated Equipment Rooms, Electrical Closets, or the like) in accordance with Articles 110-26 and 110-27 of the 1999 National Electrical Code ANSI/NFPA 70.

**Advertencia**

El RS 16000 con suministros de energía DC únicamente deberá instalarse en Areas de Acceso Restringido (recintos dedicados al equipo, armarios eléctricos o similares) según lo estipulado en los Artículos 110-26 y 110-27 del Código Eléctrico Nacional de 1999 ANSI/NFPA 70.

To install a DC power supply in the RS 16000, perform the following steps. For DC power supply environmental specifications see [Table 3-5](#). For DC power safety requirements, see [Table 3-3](#).

1. Power off the DC supply and disconnect it from any power source or ground wiring.
2. From the rear of the chassis, position the power supply between the guides in an open power supply slot; refer to [Figure 3-4](#). Remove blank panels only as necessary to accommodate power supplies.
3. Slide the power supply all the way into the slot, pressing with just enough force to seat the rear connectors into the midplane.

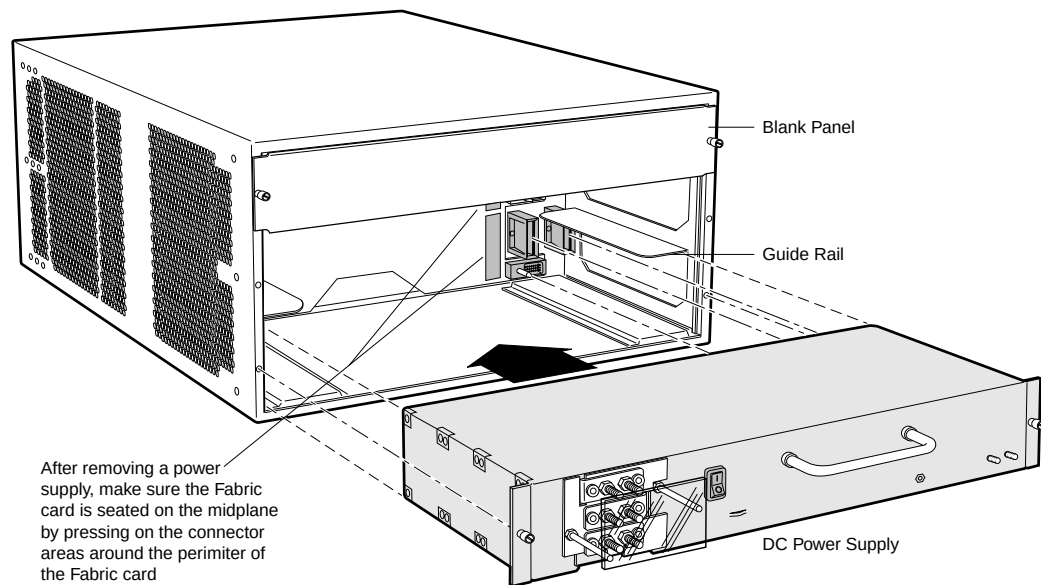


Figure 3-4 DC power supply installation

4. Using an appropriate screwdriver, turn the captive screws on the power supply's front panel clockwise to lock the power supply into the chassis.
5. **Ensure that the source power is off before proceeding with this step.** Connect the DC input wiring to the terminals on the front of the unit. To attach a wire, remove the terminal nut, place the cable's wiring lug over the terminal stud, replace and tighten the terminal nut.
6. Connect the safety ground wire(s) to the earth ground stud(s) on the front of the power supply.
7. **Ensure that the source power is off before proceeding with this step.** Connect the DC input wiring to the DC power source. For more detail, refer to the section [DC Power Supply Wiring](#).



Warning

After removing a power supply from the chassis, check the security of the Fabric card by pressing on the connector areas around its perimeter (refer to [Figure 3-4](#)). You may need to remove one or more blanking panels to access the Fabric card. Replace all panels after completing the procedure.

DC Power Supply Wiring

The DC power supply supports different wiring schemes. Review the requirements in [Table 3-3](#) prior to implementing any wiring configuration.

To connect a single power supply to a single source:

1. Install a DC supply in the RS 16000 using the procedure in [Section 3.3.6, "Installing DC Power Supplies"](#).
2. Connect the positive (+) terminal at the source to the positive (+) terminal on the supply.
3. Connect the negative (-) terminal at the source to either the (-)A or the (-)B terminal on the supply.
4. Connect the source ground to the power supply ground.

A single supply accepts input voltage from two sources. This configuration provides protection against a single power source failure.

1. Install a DC supply in the RS 16000 using the procedure in [Section 3.3.6, "Installing DC Power Supplies"](#).
2. Connect the positive (+) terminals on source 1 and source 2 to the positive (+) terminal on the DC power supply. Refer to [Figure 3-5](#).
3. Connect source 1 negative (-) terminal to the (-)A terminal on the supply. Connect source 2 negative (-) terminal to the (-)B terminal on the power supply.
4. Connect the ground terminals on source 1 and source 2 to the power supply ground.

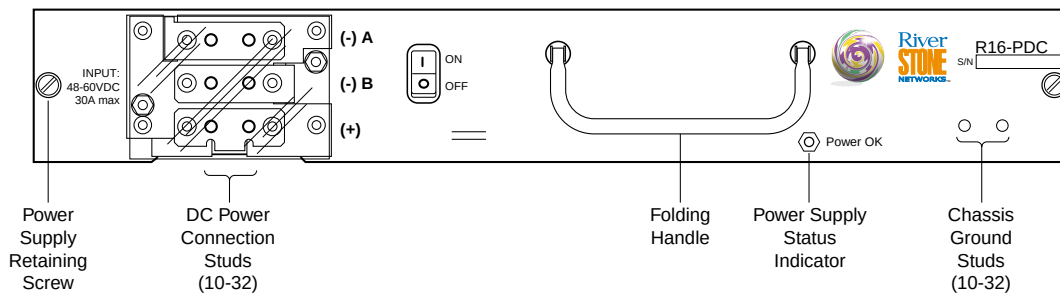


Figure 3-5 DC power supply front panel



Note The (-)A and (-)B terminals on the RS 16000 DC power supplies are isolated through MOSFET switches, therefore current should not flow from source A to source B, or vice versa, under normal operating conditions.

**Warning**

If the DC input to both (-)A and (-)B terminals goes above -40 VDC, the RS 16000 displays a warning message on the management console but will continue to operate until both sources go above -38 VDC. Riverstone cannot guarantee proper equipment operation with the DC source voltage above -38 VDC.

Table 3-3 DC power safety requirements

All power connection wiring should conform to the rules and regulations in the National Electrical Code (NEC), as well as any local codes.
Each DC-input power supply connections are rated at 60A maximum. A dedicated, commensurately-rated DC power source is required for each power entry module connection.
For DC power cables, Riverstone recommends that you use commensurately-rated, high-strand-count copper wire cable. Connection to the DC-input power supply requires one earth ground cable for the power supply and two cable leads (a DC source and a DC return) for each power supply. The length of the cables depends on your RS 16000 location. These cables are not available from Riverstone. They are available from any commercial cable vendor.
DC power cables must be terminated by cable lugs at the power supply end. The lugs should be able to fit over 1/4-20 terminal studs.
The source of power for the DC power supplies must be a reliably grounded SELV source.
Branch circuit overcurrent protection must be rated a maximum of 60A.
A readily accessible disconnect device that is suitably approved and rated should be incorporated in the field wiring.

Table 3-4 Requisitos de seguridad del suministro de energía DC

Todo el cableado de los conectores de energía deberá cumplir con los requisitos y lineamientos del Código Eléctrico Nacional (NEC) y de cualquier otro código local aplicable.
Cada conexión de entrada de corriente directa del suministro de energía está clasificado a un máximo de 60A. Se requiere el uso de un suministro de energía dedicado de corriente directa con una clasificación conmensurada para cada conexión de entrada del suministro de energía.
En el caso de los cables de energía de corriente directa, Riverstone recomienda el uso de cables de alambre de cobre con un alto conteo de hilos y con una clasificación conmensurada. La conexión al suministro de energía DC requiere el uso de un cable puesto a tierra para el suministro de energía y dos terminales de cable (una fuente DC y un retorno DC) para cada suministro de energía. La extensión de los cables depende de la ubicación del RS 16000. Riverstone no suministra dichos cables. Los cables pueden ser adquiridos de cualquier proveedor comercial de cable.
Los cables de energía DC deberán contar terminales de orejeta en el extremo del suministro de energía. Las orejetas deberán cubrir las clavijas de la terminal (1/4-20).
La fuente de poder para el suministro de energía DC deberá ser una fuente SELV debidamente puesta a tierra.
La protección de sobrecorriente del ramal del circuito deberá estar clasificada para un máximo de 60A.
Se deberá incorporar al cableado un dispositivo de desconexión de fácil acceso, mismo que deberá contar con la clasificación y la aprobación necesarias.

Table 3-5 DC power supply environmental specifications

Specification	Measurement
Operating Temperature	+5° to +40°C (41° to 104°F)
Non-operating Temperature	-30° to +73°C (-22° to 164°F)
Operating Humidity	15% to 90% (non-condensing)

3.3.7 Installing the Fan Assembly

Use this procedure to install the fan assembly.

1. Slide the fan assembly all the way into its slot, pressing with just enough force to seat the rear connectors into the midplane (refer to [Figure 3-6](#)).
2. Using a flat-blade screwdriver, tighten the retaining screw to lock the fan assembly into the chassis.

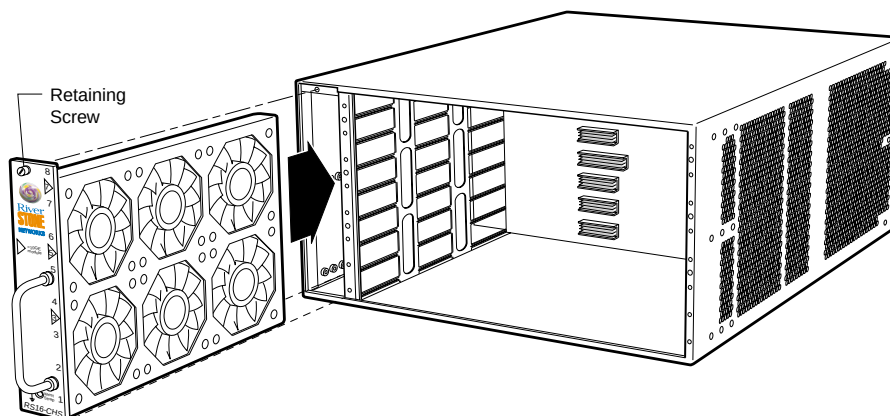


Figure 3-6 Installing the fan assembly

3.3.8 Installing the Control Module



Note If you plan to install a redundant Control Module, see [Section 4.9, "Using Redundant Control Modules"](#).

If you are installing only one Control Module, install it in either slot 1 or slot 2. If you are installing two Control Modules, the module installed in slot 1 becomes, by default, the primary and module installed in slot 2 becomes the backup. [Figure 3-7](#) illustrates Control Module installation. The steps following the figure describes the installation procedure.

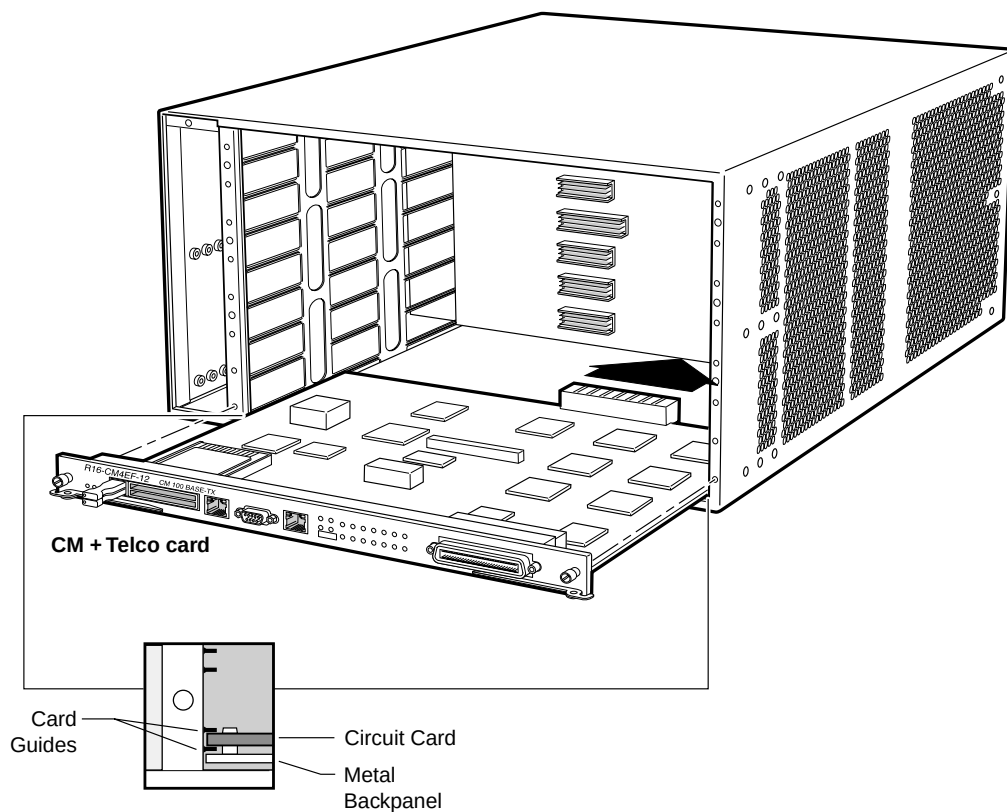


Figure 3-7 Installing a Control Module

To install the Control Module, perform the following steps.

1. If a blank panel is installed in the target Control Module slot (slot number 1 or 2), remove the panel.
2. Align the card tray of the Control Module with the card guides at the left and right of the slot opening,
3. Slide the Control Module all the way into the slot pressing with just enough force to seat the rear connector pins into the midplane. **Do not use the card ejectors to install the Control Module; use them only to disengage the module from the chassis.**

**Warning**

Slide the Control Module into the chassis in a smooth, continuous motion. Once the module's connector pins contact the mating pins on the midplane, you have three seconds to complete the insertion. Failure to complete the insertion in three seconds results in the module not being recognized by the system and may cause a system crash.

4. Using a flat-blade screwdriver, turn the captive screws on the Control Module's front panel to lock the module into the slot.
5. If the control module has Gigabit Ethernet ports, install SFP transceivers per the procedure in [Section 3.3.10, "Installing SFP Transceivers"](#).

Installing PC Flash Cards in the Control Module

**Note**

The RS 16000 supports the use of dual PC cards, one in slot0 (top slot), the other in slot1. The data on each PC card is treated as an independent file system by the RS 16000. For detailed information regarding the PC flash file system and the management of configuration files, see the [Riverstone Networks RS Switch Router User Guide](#).

**Note**

If the message "**SYS-E-NOFLASHCARD**" appears while booting the RS 16000, the system has not detected a PC card. If this occurs, ensure that the PC card is properly inserted, then reboot. If the system still does not recognize the card, contact Riverstone Networks, Inc. Technical Support.

Attaching the Control Module Management Cables

Connect a management console to the RS 16000 using the following information. The Control Module has two ports for attaching management devices to the RS 16000.

- A male DB-9 DCE port for direct serial connection from a terminal or PC running terminal emulation software. Use this port to perform basic setup, including setting up the RS 16000 for management through the Control Module's RJ-45 Ethernet port.
- An RJ-45 10/100Base-T DTE port for Telnet connection from a host on the network. The port is configured for Media Data Interface (MDI). You use this port to manage the RS 16000 using a Telnet session or SNMP-based management software.

3.3.9 Installing Line Cards

To install a line card, perform the following steps.

1. If a blank panel is installed in the target slot, remove the panel.
2. Align the card tray of the line card with the guides at the left and right of the slot opening.
3. Slide the line card all the way into the slot pressing with just enough force to seat the rear connector pins the midplane. **Do not use the card ejectors to install the line card; use them only to disengage the module from the chassis.**

**Warning**

Slide the line card into the chassis in a smooth, continuous motion. Once the card's connector pins contact the mating pins on the midplane, you have three seconds to complete the insertion. Failure to complete the insertion in three seconds results in the card not being recognized by the system and may cause a system crash.

4. Using a flat-blade screwdriver, turn the captive screws on the line card's front panel to lock the card into the slot.
5. Install SFP transceivers per the procedure in [Section 3.3.10, "Installing SFP Transceivers"](#) (this step is only for line cards with Gigabit Ethernet ports).

3.3.10 Installing SFP Transceivers

**Warning**

If the SFP transceiver does not go in easily, do not force it. If the transceiver is not oriented properly, it will stop about one quarter of the way into the slot. Remove and reorient the transceiver so that it slides easily into the slot.

SFP transceivers vary slightly among manufacturers but the insertion process is virtually the same for all. To install an SFP transceiver in either the Gigabit Ethernet line card or the Gigabit Ethernet Control Module:

1. Orient a transceiver as shown in [Figure 3-8](#). Note that for port positions 1-4, the release tab is on the bottom of the transceiver; for port positions 5-8, the tab is on top of the transceiver.

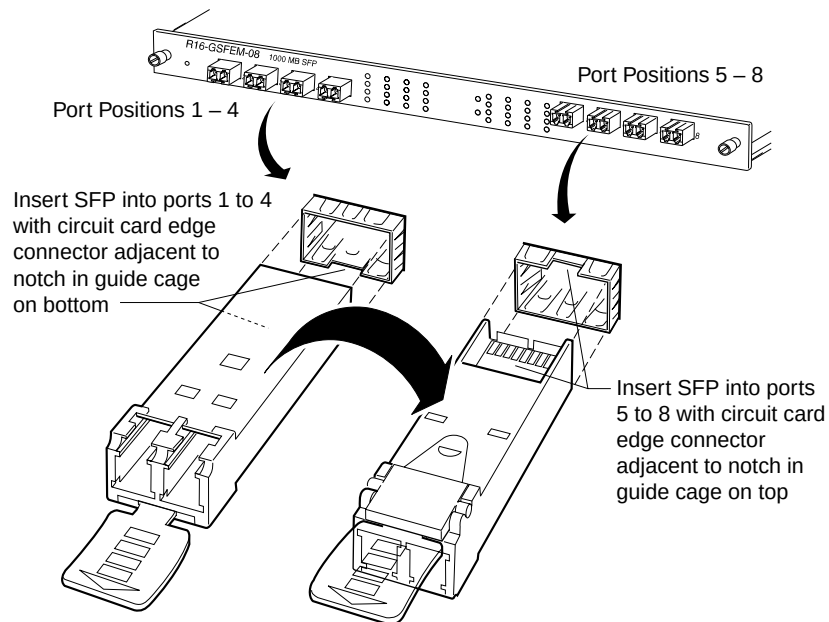


Figure 3-8 Installing SFP transceivers

2. Insert the transceiver into the target slot until it locks into position. Leave the dust plug in the transceiver until you are ready to attach a fiber cable. Clean the optic surfaces of the fiber cable prior to plugging it into the optical bores of the SFP transceiver.



Warning

Keep the dust plug in an SFP transceiver when there is no fiber cable plugged in. The optics will not work properly when obstructed with dust or contaminants.

3.3.11 Extracting SFP Transceivers

The extraction process varies among different SFP transceivers. We have illustrated and documented several examples in this section. It is likely that your transceiver is similar to one of the examples. The transceiver removal process is essentially to disengage the unit from its port via the extraction mechanism, then pull the unit straight out of the guide cage.

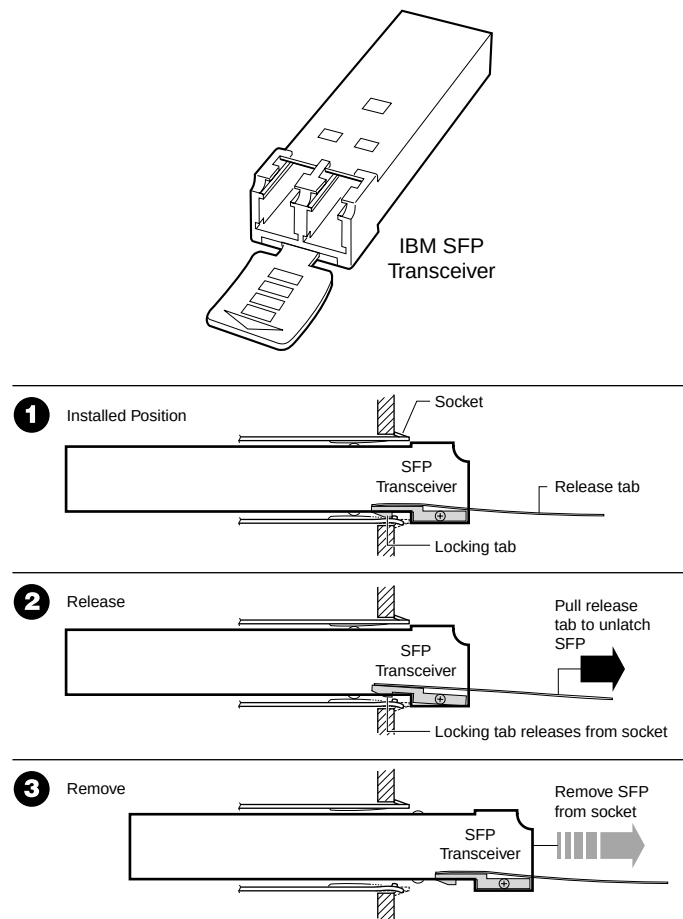


Figure 3-9 Extracting an IBM SFP transceiver

To extract an IBM SFP transceiver:

1. Remove the fiber cable from the target SFP transceiver.
2. On the target transceiver, grasp the extraction tab between the thumb and forefinger and pull the tab straight outwards until the transceiver is fully extracted from the guide cage (refer to [Figure 3-9](#)).
3. If the transceiver is not defective (disposable), protect it by inserting a dust plug.



Warning

When extracting an IBM SFP transceiver, pull straight outwards so that the unit leaves the guide cage in a parallel motion. Do not twist or pull on the tab at any angle that does not allow this straight, parallel motion.

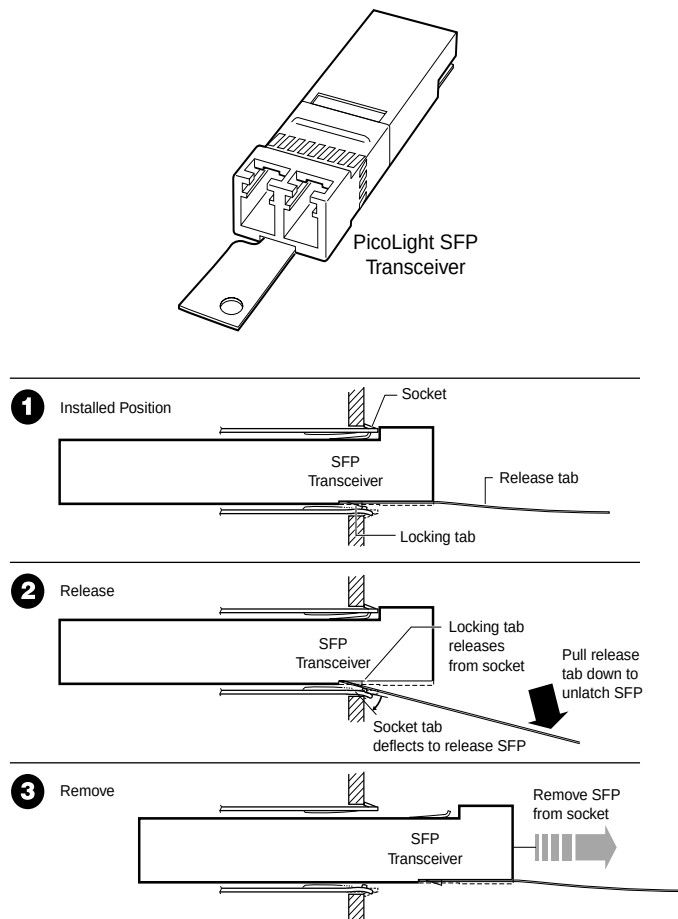


Figure 3-10 Extracting a PicoLight SFP transceiver

To extract a PicoLight SFP transceiver:

1. Remove the fiber cable from the target SFP transceiver.
2. On the target transceiver, grasp the extraction tab between the thumb and forefinger and pull the tab down until the transceiver is unlatched from its port, then pull the unit straight out of the guide cage (refer to [Figure 3-10](#)).
3. If the transceiver is not defective (disposable), protect it by inserting a dust plug.

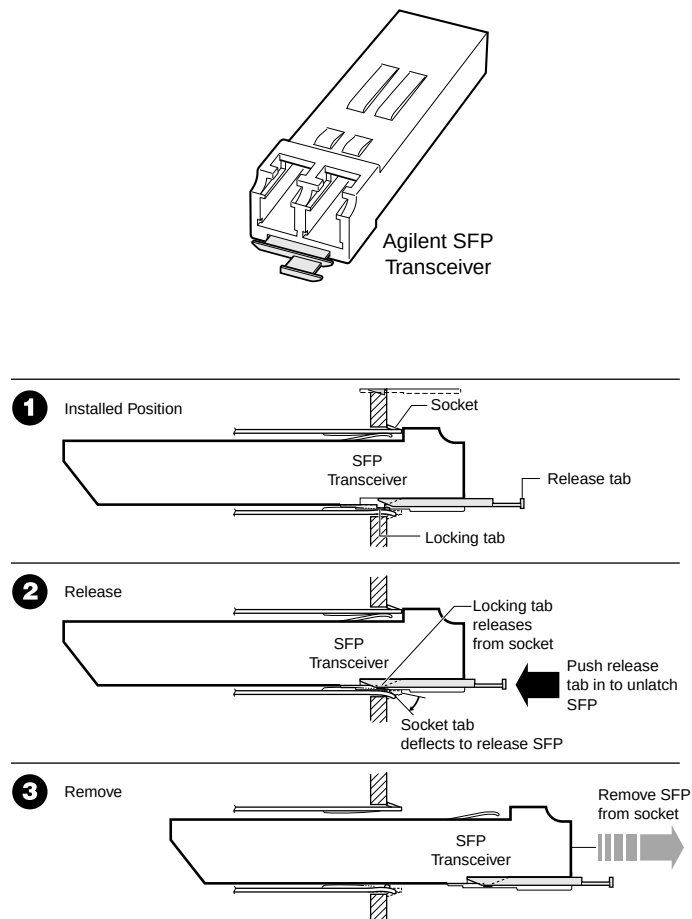


Figure 3-11 Extracting an Agilent SFP transceiver

To extract an Agilent SFP transceiver:

1. Remove the fiber cable from the target SFP transceiver.
2. On the target transceiver, push the release tab to unlatch the transceiver then pull the unit straight out of the guide cage (refer to [Figure 3-11](#)).
3. If the transceiver is not defective (disposable), protect it by inserting a dust plug.

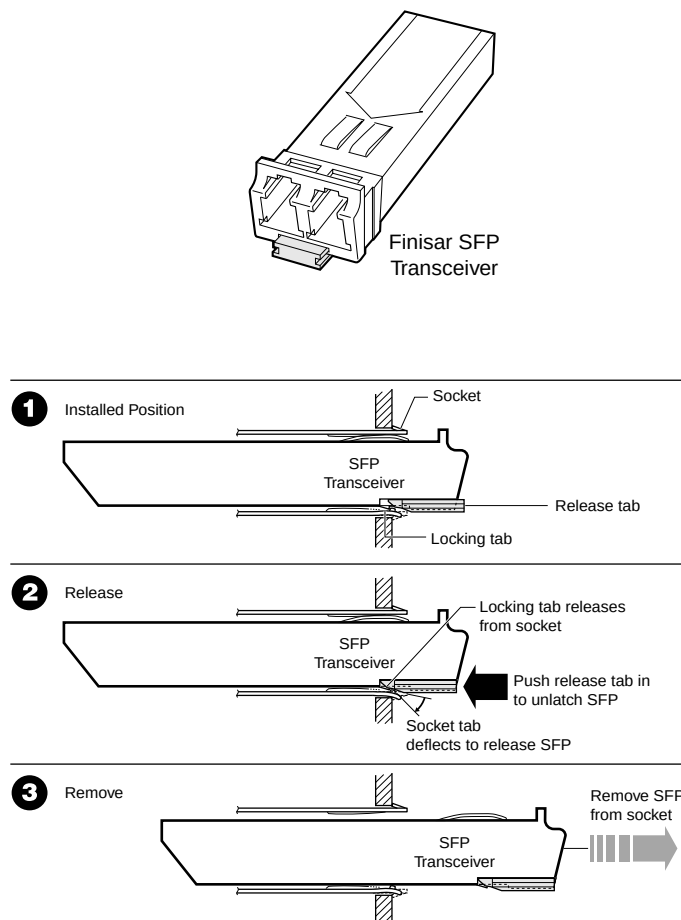


Figure 3-12 Extracting a Finisar SFP transceiver

To extract a Finisar SFP transceiver:

1. Remove the fiber cable from the target SFP transceiver.
2. On the target transceiver, push the release tab to unlatch the transceiver then pull the unit straight out of the guide cage (refer to [Figure 3-12](#)).
3. If the transceiver is not defective (disposable), protect it by inserting a dust plug.

3.3.12 Attaching the Segment Cables

With your RS 16000 installed and connected to a management console, you are now ready to attach the RS 16000's line cards to your network. The RS 16000 uses industry standard copper and fiber cables and connectors. For information regarding required connector types, cable types, and pin-out assignments, see the tables associated with the line card in [Chapter 2, "Overview"](#).

Proceed to [Chapter 4, "Initial Configuration"](#) for instructions on powering on the RS 16000 and performing initial configuration.

4 INITIAL CONFIGURATION

This chapter provides the following information on powering up the RS 16000 and performing basic setup procedures. Basic setup includes:

- Powering on the RS 16000 and booting the software
- Starting the Command Line Interface (CLI)
- Activating and saving configuration changes
- Assigning passwords
- Using the CLI to add an IP interface, subnet mask, and default gateway
- Setting up SNMP
- Assigning a DNS server(s) to the RS 16000
- Configuring the SYSLOG server and server message levels
- Using redundant Control Modules

4.1 POWERING ON THE RS 16000

To power on the RS 16000, perform the following steps:

1. Make sure all exposed line card slots and power supply bays are free of foreign objects such as tools and are covered with blanks.
2. Check the power supplies to make sure they are properly connected to their power sources.
3. Make sure that the RS 16000's DB-9 console port is connected to an active terminal or a PC running terminal emulation software.
4. Turn on each power supply.

If this is the first time you have powered on the RS 16000, it will automatically boot using the software image on the PC flash card. The DIAG LED on the Control Module flashes while the software boots. After the software successfully boots, the DIAG LED goes dark and the OK LED lights.

As the software boots, the management terminal (or PC attached to the Control Module's DB-9 DCE port) displays messages related to the phases of the boot sequence.

Here is a partial example:

```
Boot Software Version 2.0.1.1, Built Jul 1 2001 16:30:38
Processor: R7000 rev 3.2 [0x2732], 373 MHz, (bus: 93 MHz), 256 MB DRAM
I-Cache 16 KB, linesize 32. D-Cache 16 KB, linesize 32.
```

L2-Cache 256 KB, linesize 32, cache enabled.

Mounting 16MB external flash card . . . Done

Autoboot in 2 seconds - press RETURN to abort and enter prom

using link: bootsource

link pointed at file:/pc-flash/boot/ros80/

source: file:/pc-flash/boot/ros80/

Loaded version file

Loading kernel (base 0x80001000, size 50528)

(base 0x8000d560, size 4892855)

100% - Image checksum validated

RS 16000 System Software, Version 8.01.A.09

Copyright (c) 2000-2001, Riverstone Networks, Inc.

Processor: R7000, Rev 3.2, 373 MHz

System started on 2001-08-01 11:01:45

2001-08-01 11:01:45 %SYS-I-FLASHCRD, Mounting 16MB Flash card

2001-08-01 11:01:54 %SYS-I-FLASHMNTD, 16MB Flash card mounted

2001-08-01 11:01:54 %SYS-I-INITSYS, initializing system RS 16000

2001-08-01 11:01:54 %SYS-I-DSCVMOD, discovered 'Control Module / 13-10/100-TX "T"'
module in slot CM/1

2001-08-01 11:01:55 %SYS-I-INITLOTS, Initializing system slots - please wait

2001-08-01 11:02:04 %SYS-I-MODPROBE, Detecting installed media modules - please
wait

2001-08-01 11:01:54 %SYS-I-DSCVMOD, discovered 'Control Module / 13-10/100-TX "T"'
module in slot CM/1

2001-08-01 11:02:05 %SYS-I-DSCVMOD, discovered '8-Gigabit "T" (SFP)' module in
slot CM/2 ...

5. When the software is fully booted, the following message appears on the management console:

Press RETURN to activate console...

6. As prompted, press Return (or Enter) to activate the Command Line Interface (CLI) on the console.



Note If the message “**SYS-E-NOFLASHCARD**” appears while booting the RS 16000, the system has not detected a PCMCIA card. If this occurs, ensure that the PC card is properly inserted, then reboot. If the system still does not recognize the card, contact Riverstone Networks, Inc. technical support.

4.2 STARTING THE COMMAND LINE INTERFACE

To start the Command Line Interface (CLI), power on the system as described in [Section 4.1, "Powering on the RS 16000"](#). After the software is fully booted, press Return (or Enter) to activate the CLI. If prompted for a password, simply press Return; the factory default passwords for all access levels is blank.

4.2.1 CLI Access Modes

The CLI has four levels of access, each providing the ability to perform specific operations on the RS 16000 (see [Table 4-1](#)).

Table 4-1 CLI access modes

Access Mode	Description
User	Allows you to display basic information and use basic utilities such as ping but does not allow you to display SNMP, filter, and access control list information or make other configuration changes. You are in User mode when the command prompt ends with the ">" character.
Enable	Allows you to display SNMP, filter, and access control information, as well as all the information you can display in User mode. To enter Enable mode, enter the enable command, then supply the password when prompted. When you are in Enable mode, the command prompt ends with the "#" character.
Configure	Allows you to make configuration changes. To enter Configure mode, first enter Enable mode (enable command), then enter the configure command. When you are in Configure mode, the command prompt ends with "(config)".
Boot	This mode appears when the external PC card or the system image is not found during bootup. Enter the reboot command to reset the RS 16000. If the RS still fails to boot, contact Riverstone Networks, Inc. technical support. Certain tasks can be performed only from Boot mode. To enter the Boot mode intentionally, boot the RS 16000, and then interrupt the normal bootup sequence by pressing the "Esc" key. When you are in Boot mode, the command prompt is "rs-boot>".

**Note**

The command prompt will show the name of the router in front of the mode character(s). The default name is "rs." The procedure in [Section 4.4, "Setting the Basic System Information"](#), describes how to change the system name.

When you are in Configure or Enable mode, use the **exit** command or press Ctrl+z to exit to the previous access mode.

4.2.2 Basic Line Editing Commands

The CLI supports Emacs-like line editing commands. [Table 4-2](#) lists some commonly used commands. For a complete set of commands, see the [Riverstone Networks RS Switch Router User Guide](#).

Table 4-2 Common CLI line editing commands

Key sequence	Command
Ctrl+a	Move cursor to beginning of line
Ctrl+b	Move cursor back one character
Ctrl+d	Delete character
Ctrl+e	Move cursor to end of line
Ctrl+f	Move cursor forward one character
Ctrl+n	Scroll to next command in command history (use the cli show history command to display the history)
Ctrl+p	Scroll to previous command in command history
Ctrl+u	Erase entire line
Ctrl+x	Erase from cursor to end of line
Ctrl+z	Exit current access mode to previous access mode

4.3 CONFIGURATION CHANGES AND SAVING THE CONFIGURATION FILE

Table 4-3 lists and describes the three special configuration files used by the RS 16000.

Table 4-3 Configuration file contents

File	Descriptions
Scratchpad	The configuration commands you have entered during a management session. These commands do not become active until you explicitly activate them. Because some commands depend on other commands for successful execution, the RS 16000 scratchpad simplifies system configuration by allowing you to enter configuration commands in any order, even when dependencies exist. When you activate the commands in the scratchpad, the RS 16000 sorts out the dependencies and executes the commands in their proper sequence.
Active	The commands from the Startup configuration file and any configuration commands that you have made active from the scratchpad.
Startup	The configuration file that the RS 16000 uses to configure itself when the system is powered on.



Caution The active configuration remains in effect only during the current power cycle. If you power off or reboot the router without saving the active configuration changes to the Startup configuration file, the changes are lost.

4.3.1 Activating the Configuration Commands in the Scratchpad

Use the following procedure to activate the configuration commands in the scratchpad.

1. Ensure that you are in Enable mode by entering the **enable** command in the CLI.
2. Ensure that you are in Configure mode by entering the **configure** command in the CLI.
3. Enter the following command:

```
save active
```

The CLI displays the following message:

```
Do you want to make the changes Active? [y]
```

4. Enter **y** to activate the changes.



Caution If you exit the Configure mode (by entering the **exit** command or pressing Ctrl+z), the CLI will ask you whether you want to make active the changes in the scratchpad. If you do not make the changes in the scratchpad active, the changes will be lost when you log out.

4.3.2 Saving the Active Configuration to the Startup Configuration File

Use the following procedure to save Active configuration changes into the Startup configuration file so that the RS 16000 remembers and uses the changes when you reboot the software.

1. Enter the following command from Configure mode:

```
rs(config)# save startup
```

2. When the CLI displays the following message, enter **y** to save the changes:

```
Are you sure you want to overwrite the Startup configuration [no]? y
%CONFIG-I-SAVED, configuration saved to Startup configuration.
rs(config)#
```

Alternately, to save the Active configuration to the Startup configuration from Enable mode, perform the following steps.

1. Ensure that you are in Enable mode by entering the **enable** command in the CLI.
2. Enter the following command to copy the Active configuration to the Startup configuration:

```
copy active to startup
```

3. When the CLI displays the following message, enter **yes** to save the changes.

```
Are you sure you want to overwrite the Startup configuration? [n]
```

The new configuration changes are added to the Startup configuration file located in the Control Module's boot flash.

4.3.3 Viewing the Current Configuration

To view the current configuration:

1. Ensure that you are in Enable mode by entering the **enable** command.
2. Enter the following command to display the status of each command line:

```
system show active-config
```

**Note**

Remember that the Active configuration contains both the Startup configuration and any configuration changes that you've made active in the current configuration session.

The CLI displays the Active configuration file 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/line cards, it is annotated with a “**P:**” For example, if you enable STP on all ports on the RS 16000, but the RS 16000 contains only one line card, the configuration lines that enable STP will be applied to all ports on all other line cards as they are added to the system.

A command like **stp enable et.*.*** would be displayed as follows:

```
P: stp enable et.*.*
```

If you update the configuration file to state specifically which Ethernet ports STP is enabled on, the “**P:**” annotation in the above command line would disappear.

4.3.4 Viewing Port Status

To view the port status:

1. Ensure that you are in Enable mode by entering the **enable** command.
2. Enter the following command to display port status:

```
show port-status all-ports
```

Here is a partial example of the system response:

Flags: M - Mirroring enabled B - MLP Bundle S - SmartTRUNK port P -
Configured as 802.1p

Port	Port Type	Duplex	Speed	Negotiation	IFG Value	Link State	Admin State	Flags
-----	-----	-----	-----	-----	-----	-----	-----	-----
et.1.1	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.2	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.3	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.4	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.5	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.6	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.7	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.8	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.9	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.10	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.11	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.12	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.1.13	10/100-Mbit Ethernet	n/a	n/a	Auto	0	Down	Up	
et.2.1	1 Gigabit Ethernet	Full	1 Gbits	Auto	0	Down	Up	
et.2.2	1 Gigabit Ethernet	Full	1 Gbits	Auto	0	Down	Up	
et.2.3	1 Gigabit Ethernet	Full	1 Gbits	Auto	0	Down	Up	
et.2.4	1 Gigabit Ethernet	Full	1 Gbits	Auto	0	Up	Up	
et.2.8	1 Gigabit Ethernet	Full	1 Gbits	Auto	5	Up	Up	
et.2.7	1 Gigabit Ethernet	Full	1 Gbits	Auto	5	Up	Up	
et.2.6	1 Gigabit Ethernet	Full	1 Gbits	Auto	5	Up	Up	
et.2.5	1 Gigabit Ethernet	Full	1 Gbits	Auto	5	Up	Up	
et.3.1	1 Gigabit Ethernet	Full	1 Gbits	Auto	5	Up	Up	
...								



Note The 10/100 Base-T port (10/100 PORT1) is identified as “et.1.1” in the “Port” column.



Note For the Gigabit line cards, ports 5-8 are listed in reverse order in the “Port” column (et.2.8, et.2.7, and so forth). **Certain commands lead to this reversed listing while other commands display results in correct order. Be alert to this while you are examining the displayed results of similar commands.**

4.4 SETTING THE BASIC SYSTEM INFORMATION

Follow the procedures in this section to set the following system information:

- System time and date
- System name
- System location
- Contact name (the person to contact regarding this router)
- IP address for the management port on the Control Module



Note Some of the commands in this procedure accept a string value. String values can be up to a maximum of 255 characters in length including blank spaces. Surround strings that contain blanks with quotation marks (for example: **"string with internal blanks"**).

1. Enter the **enable** command to get to Enable mode in the CLI.
2. Enter the following commands to set the system time and date and to verify your settings.

```
system set date year <number> month <month-name> day <day> hour <hour> minute <minute> second <second>
system show date
```

Here is an example:

```
rs# system set date year 2003 month march day 27 hour 11 minute 54
second 0
Time changed to: Mon Mar 27 11:54:00 2003
rs# system show date
Current time: Mon Mar 27 11:54:04 2003
```

3. Enter the **configure** command to get to Configure mode in the CLI. The following commands can be entered only from Configure mode.
4. Enter the following commands to set the system name, location, and contact information:

```
system set name <string>
system set location <string>
system set contact <string>
```

Here is an example:

```
rs(config)# system set name rs  
rs(config)# system set location "Houston, TX"  
rs(config)# system set contact "John Smith"
```

5. Use the **interface add ip** command to set the IP address and netmask for the en0 Ethernet interface. The en0 Ethernet interface is used by the management port on the Control Module.

Here is an example:

```
rs(config)# interface add ip en0 address-netmask 16.50.11.22/16
```



Note The en0 interface is automatically created by the system and is reserved for the management port on the Control Module.

6. To activate the system commands entered in the previous steps, use the following command:

```
save active
```

The CLI displays the following message:

```
Do you want to make the changes Active? [y]
```

7. Enter “y” to activate the changes.
8. To display the Active configuration, exit the Configuration mode, then enter the following command:

```
system show active-config
```

Here is an example:

```
rs# system show active-config
Running system configuration:
    !
    ! Last modified from Console on Mon Jan 25 11:55:35 2001
    !
1 : system set name "rs"
2 : system set location "Houston, TX"
3 : system set contact "John Smith"
```

9. Save the Active configuration to the Startup configuration file using the following command:

```
copy active to startup
```

10. When the CLI displays the following message, enter **y** to save the changes to the Startup configuration file:

```
Are you sure you want to overwrite the Startup configuration [no]? y
%CONFIG-I-WRITTEN, file copied successfully
rs#
```

4.5 SETTING UP PASSWORDS

You can password-protect CLI access to the RS 16000 by setting up passwords for User mode access, Enable mode access, and Diag mode access. Users who have a User password but not an Enable password can use only the commands available in User mode. Users with an Enable password can use commands available in the Enable and Configure modes, as well as the commands in User mode.

In addition, you can set up the RS 16000 for TACACS, TACACS+, and/or RADIUS authentication by a TACACS or RADIUS server. Procedures for configuring the router for TACACS and RADIUS can be found in the [Riverstone Networks RS Switch Router User Guide](#).

To add password protection to the CLI, use the following procedure.

1. Ensure that you are in Enable mode by entering the **enable** command in the CLI.
2. Ensure that you are in Configure mode by entering the **configure** command in the CLI.
3. Type the following command for each password you want to set:

```
system set password login|enable|diag <string>|none
```

4. Use the **show** command to examine the commands you just entered.
5. Use the **save active** command to activate the commands.
6. Exit the Configuration mode, then use the **system show active-config** command to verify the active changes.

Here is an example of the commands in the previous steps:

```
rs(config)# system set password login demo
rs(config)# system set password enable killer
rs(config)# system set password diag trouble
rs(config)# save active
rs# exit
rs# system show active-config

Running system configuration:
!
! Last modified from Console on Mon Mar 27 12:12:19 2003
!
1 : system set name "rs"
2 : system set location "Houston, TX"
3 : system set contact "John Smith"
4 : system set hashed-password login jNIssH c976b667e681d03ccd5fc527f219351a
5 : system set hashed-password enable zcGzb0 5d1f73d2d478ceaa062a0b5e0168f46a
6 : system set hashed-password diag jdfbyp 67e681d3d2d478cf21935a0b5e016f2193
```

Notice that the passwords are shown in the Active configuration in an encrypted format. Passwords also appear this way in the Startup configuration. To keep your passwords secure, the router does not have a command for displaying passwords in an unencrypted format.



Caution Test all new passwords before saving the active configuration to the Startup configuration file.

4.5.1 If You Forget Your Passwords

If you forget your passwords, follow the procedure below to regain access to your RS 16000.



Note To perform the password recovery procedure, you must use a terminal or PC running terminal emulation software that is connected directly to the RS 16000 through its DB-9 console port.

1. Power cycle the RS 16000.
2. Enter Boot mode by interrupting the normal boot-cycle by pressing the “Esc” key.
3. From the boot prompt, enter the **set** command and note the image name displayed for **bootsource**. For example:

```
...
mfg_loop_by = time          [time count]
mfg_loop_max = 86400
bootdelay = 2
autoboot = boot
promsetaddrs = 1
    netaddr = 134.152.179.132
bootaddr = 0.0.0.0
    netmask = 255.255.255.224
    gateway = 134.152.179.129
bootsource = /pc-flash/boot/ros80      <This is the image name for this example>
    ethaddr = 00:00:1d:12:34:56
    sysid = -1
rs-boot>
```

4. Enter the following line to reboot the RS 16000:

```
boot <image name> skipconfig=yes
```

Here is an example:

```
rs-boot> boot /pc-flash/boot/ros80 skipconfig=yes
```

5. When the RS 16000 finishes booting, enter the following commands (when prompted, answer **yes**):

```
rs> enable
rs# copy startup to scratchpad
rs# config
rs(config)# system set password login none
rs(config)# system set password enable none
rs(config)# system set password diag none
rs(config)# save startup
Are you sure you want to overwrite the Startup configuration [no]? yes

There are non-committed configuration changes. Do you want to make
these changes active and then save everything to Startup [yes]? yes

%CONFIG-I-SAVED, 2001-09-02 21:53:54 %GATED-I-RECONFIGDONE, Routing
configuration changes completed (pid 0x809eab20).
configuration saved to Startup configuration.
rs(config)#
```

6. The User, Enable, and Diag access mode passwords are now reset to the default “blank” values.
7. Enter new passwords for the User, Enable, and Diag access modes.

4.6 SETTING UP SNMP

To use SNMP to manage the RS 16000, you need to set up an SNMP community and specify the IP address of the target host for SNMP traps. Otherwise, the RS 16000's SNMP agent runs in local trap process mode, unless disabled using the **snmp stop** command.

For additional information about configuring SNMP, see the [Riverstone Networks RS Switch Router User Guide](#).

4.6.1 Setting the Community string

Use the following procedure to add the SNMP community string, specify the target host for traps, and the trap interface.

1. Ensure that you are in Enable mode by entering the **enable** command in the CLI.
2. Ensure that you are in Configure mode by entering the **configure** command in the CLI.
3. Use the following commands to add an SNMP community string and set a target host IP address for the traps:

```
rs(config)#snmp set community <community-name> privilege read|read-write
rs(config)#snmp set target <IP-addr> community <community-name> status enable|disable
```



Note

If the IP address of the trap target is more than one hop away from the RS 16000, configure the RS with a static route to the target. If the RS 16000 is rebooted, the static route allows a cold-start trap to be sent to the trap target. Without a static route, the cold-start trap is lost while the routing protocols are converging.

4. Use the **save startup** command to activate the commands entered in the previous steps.

Here is an example of the commands and output for configuring SNMP and saving the changes.

```
rs# config
rs(config)# snmp set community public privilege read-write
rs(config)# snmp set target 16.50.11.12 community public status enable
rs(config)# save startup
Are you sure you want to overwrite the Startup configuration [no]? yes

There are non-committed configuration changes. Do you want to make
these changes active and then save everything to Startup [yes]? yes

%CONFIG-I-SAVED, 2001-09-02 21:53:54 %GATED-I-RECONFIGDONE, Routing
configuration changes completed (pid 0x809eab20).
configuration saved to Startup configuration.
rs(config)#
```

By default, SNMP information is sent and received on the Control Module's en0 Ethernet port. If you want SNMP to use a different port on the RS 16000, use the following command:

```
snmp set trap-source <interface>|<IPaddr>
```

Here is an example:

```
rs(config)# snmp set trap-source 134.152.78.192
```

SNMP will now use the port with IP address 134.152.78.192. Remember, to make this change permanent, enter the **save startup** command.

4.6.2 Improving SNMP Security

SNMPv1 is not a secure protocol. Messages containing community strings are sent in plain text from manager application to agent. Anyone with a protocol decoder and access to the wire can capture, modify, and replay messages.

Applying ACLs to SNMP

When using SNMPv1, it is important to protect your RS 16000 by applying an Access Control List (ACL) to the SNMP agent to prevent unauthorized access and route your SNMP traffic through trusted networks only.

Here are the basic configuration commands to apply an ACL to the RS 16000's SNMP agent, allowing access to the RS 16000 by only one management station.

```
rs(config)# acl mgmt_only permit udp <IPaddr> any any any
rs(config)# acl mgmt_only apply service snmp
```

The above ACL applied to the SNMP service allows messages from source IP address <IPaddr> to be processed by the SNMP agent. Packets from any other source IP address are dropped.

Disabling Authentication Traps

To provide additional security to the RS 16000, disable the sending of authentication traps. Authentication traps are sent when SNMP v1 packets are received with invalid community strings. A common security attack on an SNMP v1 agent is to send a message containing an invalid message, and then capture the authentication trap to learn the community string.

Here is an example of how to turn off the sending of authentication traps:

```
rs(config)#snmp disable trap authentication
```

For more information about RS 16000 security and ACLs, refer to the [Riverstone Networks RS Switch Router User Guide](#).

4.6.3 Supported MIBs

The following lists the MIBs that are supported by the RS 16000 SNMP agent.

Table 4-4 Supported MIBs

MIB II	Layer 1	Layer 2	Layer 3	System Related	Enterprise
IP-MIB RFC 2011	ETHERLIKE-MIB RFC 2665	FRAME-RELAY-DTE-MIB RFC 2115	BGP4-MIB RFC 1657	RADIUS-AUTH-CLIENT-MIB RFC 2618	NOVELL-IPX-RIPSAP 2/94
TCP-MIB RFC 2012	SONET-MIB RFC 2558	BRIDGE-MIB RFC 1493	RIPv2-MIB RFC 1724	RADIUS-ACC-CLIENT MIB RFC 2620	NOVELL-IPX 4/21/94
UDP-MIB RFC 2013	DS0 MIB	Q-BRIDGE-MIB RFC 2674	OSPF-MIB RFC 1850	DISMAN-SCHEDULE-MIB RFC 2591	RIVERSTONE-STP-MIB 7/11/00
IP-FORWARD-MIB RFC 2096	DS1-MIB RFC 2495	P-BRIDGE-MIB RFC 2674	OSPF-TRAP-MIB RFC 1850	ENTITY-MIB RFC 2737	RIVERSTONE-RS-AGENT-CAP-MIB
IF-MIB RFC 2233	DS3-MIB RFC 2496	PPP-LCP-MIB RFC 1471	RMON2-MIB RFC 2021	SNMPv3-MIB Modules RFC 2570-2576	RIVERSTONE-ATM-MIB 1/31/01
	DS0BUNDLE-MIB RFC 2494	PPP-SEC-MIB RFC 1472	VRRP-MIB RFC 2787	SNMPv2-MIB RFC 1907	RIVERSTONE-IMAGE-MIB 7/8/00
	MAU MIB RFC 2668	PPP-IP-NCP-MIB RFC 1473	DVMRP-MIB Draft #4	DIFF-SERV-MIB Draft #5	CISCO-BGP-POL-ACCOUNTING-MIB 05/01
		PPP-BRIDGE-NCP-MIB RFC 1474	IGMP-MIB Draft #5	PING-MIB RFC 2925	CISCO-SRP-MIB
		RMON-MIB RFC 1757	ISIS-MIB	TRACEROUTE-MIB RFC 2925	RIVERSTONE-LFAP-MIB 3/1/01
		ATM-MIB RFC 2515	MPLS-LSR-MIB dRAFT #7	NOTIFICATION-LOG-MIB	RIVERSTONE-RL-MIB 11/30/00
		ATM2-MIB			RIVERSTONE-SNMP-MIB
		LAG MIB 802.3ad			RIVERSTONE-NOTIFICATIONS-MIB
					CTRON-LFAP (deprecated) 8/28/99
					CTRON-SSR-POLICY (deprecated) 8/11/99
					CTRON-SSR-CONFIG 8/17/99
					CTRON-SSR-HARDWARE (deprecated) 8/14/99
					CTRON-SSR-SERVICE-STATUS (deprecated) 8/4/98
					CTRON-SSR-CAPACITY-MIB

Table 4-4 Supported MIBs (Continued)

	RIVERSTONE-INVENTORY-MIB 6/19/01
	RIVERSTONE-CONFIG-MIB
	RIVERSTONE-DHCP-MIB
	RIVERSTONE-MPLS-MIB
	RIVERSTONE-QUEUE-MIB

4.7 SETTING THE DNS DOMAIN NAME AND ADDRESS

Associating a DNS name server with your RS 16000 allows you to use device names (rather than IP addresses) when entering certain commands. For example, you can use a device's name (which the DNS server knows) when using the **ping** command.

If you want the RS 16000 to access a DNS server, use the following procedure to specify the domain name and IP address for the DNS server.

1. Ensure that you are in Enable mode by entering the **enable** command in the CLI.
2. Use the **ping** command to verify that the RS 16000 can reach the DNS server.

Here is an example:

```
rs# ping 16.50.11.12 <IP address of the DNS server>
PING 16.50.11.12 (16.50.11.12): 56 data bytes
64 bytes from 16.50.11.12: icmp_seq=0 ttl=255 time=0 ms

--- 16.50.11.12 ping statistics ---

1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

3. Enter Configure mode by entering the **configure** command in the CLI.
4. Enter the following command to specify the domain name for which the DNS server(s) have authority:

```
system set dns domain <domain-name>
```

For example: *<domain-name>* = **riverstone.com**

5. Enter the following command to add the DNS server to the RS 16000:

```
system set dns server <IP-addr>[,<IP-addr>[,<IP-addr>]]
```

where *<IP-addr>* is the IP address of the DNS server(s). You can specify up to three DNS servers. Separate the server IP addresses with commas.

6. Enter the **save active** command to activate the commands and enter **yes** to activate the changes.

Here is an example:

```
rs# config  
rs(config)# system set dns domain "mktg.mrb.com"  
rs(config)# system set dns server 16.50.11.12  
rs(config)# save active
```

7. Exit Configure mode, then enter the **system show dns** command to verify the new DNS settings.

Here is an example:

```
rs# system show dns  
DNS domain: mrb.com, DNS server(s): 16.50.11.12
```

8. Use the **ping** command to verify that the RS can resolve the DNS server name into its IP address.

Here is an example:

```
rs# ping rs  
PING rs.mktg.mrb.com (16.50.11.22): 56 data bytes  
64 bytes from 16.50.11.22: icmp_seq=0 ttl=255 time=0 ms  
  
--- rs.mktg.mrb.com ping statistics ---  
1 packets transmitted, 1 packets received, 0% packet loss  
round-trip min/avg/max = 0/0/0 ms
```

4.8 SETTING THE SYSLOG PARAMETERS

The RS 16000 can use SYSLOG messages to communicate the following types of messages to a SYSLOG server:

Table 4-5 Types of SYSLOG messages

Message Type	Description
Fatal	Information about events that caused the RS 16000 to crash and reset.
Error	Information about errors.
Warning	Warnings against invalid configuration information and other conditions that are not necessarily errors.
Informational	Informational messages such as status messages. The SYSLOG messages that the Control Module displays while booting the software and reading the startup configuration file are examples of Informational messages.

Table 4-6 shows examples of the types of SYSLOG messages. Notice that after the facility type (in this case, “CONFIG”) the message contains a letter that refers to the message type: “F” for fatal, “E” for error, and so on.

Table 4-6 Examples of message types

Message Type	Example
Fatal	%CONFIG-F-CREATE_SEMA4 Unable to create %s semaphore: %d
Error	%CONFIG-E-NEED_COMMAND Need at least one command word to match
Warning	%CONFIG-W-BACKUP_CFG Cannot find Startup config - using backup on PCMCIA flash
Informational	%CONFIG-I-MAVED configuration saved to Startup configuration

The RS 16000 writes the SYSLOG messages to a SYSLOG daemon on UDP port 514. You can set the CLI to send all or only some of the message types. By default, the CLI sends warning, error, and fatal messages but not informational messages to the specified SYSLOG server.

Use the following procedure to specify the SYSLOG server and the types of messages you want the CLI to send to the server.

1. Ensure that you are in Enable mode by entering the **enable** command in the CLI.
2. Use the **ping** command to verify that the RS 16000 can reach the SYSLOG server.
3. Ensure that you are in Configure mode by entering the **configure** command in the CLI.
4. Enter the following commands to add the SYSLOG server to the RS 16000, set the message level, and set the SYSLOG facility:

```
system set syslog server <hostname-or-IP-addr>
system set syslog level fatal|error|warning|info
system set syslog facility <facility-type>
```



Note The *<facility-type>* is a string of the form: *user*, *kern*, or *local0* through *local7*. These strings are reserved by the SYSLOG server daemon. for information on how *<facility-type>* is used by the SYSLOG server, see the documentation for your server's *syslog.conf* file.

Here is an example:

```
rs# config
rs(config)# system set syslog server 16.50.11.12
rs(config)# system set syslog level info
rs(config)# system set syslog facility local0
```

5. To activate the SYSLOG commands, use the **save active** command. Enter **yes** to activate the changes.



Note Up to four SYSLOG servers can be configured for each RS.

4.9 USING REDUNDANT CONTROL MODULES

The RS 16000 supports the use of redundant Control Modules (CMs). One Control Module acts as the primary CM, while the other Control Module acts as the backup CM. By default, the CM installed in slot 1 is the primary CM, while the CM installed in slot 2 is the backup CM. The purpose of the backup CM is to take over as the primary CM in the event that the primary CM fails.

In normal operation, whenever changes are made to the primary CM's Configuration file, the changes are copied to the backup CM's configuration file. In this way, if the primary CM fails, the backup CM has all the configuration information necessary to take over as the primary CM. For instance, a static route is added to the RS 16000. Notice the messages displayed in the example when the change is saved to both the Active and Startup Configuration:

```
rs1(config)# ip add route 134.141.169.0/24 gateway 134.141.179.129
rs1(config)# save active

%SYS-I-ACTIVECFGTOBACKUP, active configuration updated on Backup CM

rs1(config)# save startup

Are you sure you want to overwrite the Startup configuration [no]? yes

%CONFIG-I-MAVED, configuration saved to Startup configuration.

%SYS-I-STARTUPCFGTOBACKUP, startup configuration file updated on Backup CM
rs1(config)#
```

Each message confirms that the Active and Startup Configurations were saved to the backup CM.

4.9.1 Failover

There are two ways that the primary CM can fail – either by a software failure (which causes a *soft failover*) or by a hardware failure (which causes a *hard failover*). Each of these failures cause the backup CM to assume the role of primary CM in a different way.

Soft Fail Over

If the primary CM experiences a crash because of a software failure, it sends a command to the backup CM to take over the role of primary CM. Because the backup CM's configuration has been kept in sync with the primary CM's configuration, the switch over to becoming the primary CM occurs immediately. The new primary CM (formerly the backup CM) maintains existing layer-2 and layer-3 flows and begins learning new flows within 5 to 20 seconds. After the routing protocols have had a chance to converge (60 seconds), layer-3 flows are aged out gracefully and replaced with new flows. When the original primary CM reboots or is reset, it assumes the role of the backup CM.

Notice that the default positions for the CMs within the RS 16000 chassis have now changed – the primary CM now resides in slot CM/1 and the backup CM resides in slot CM. As configuration changes are saved on the new primary CM (in slot CM/1) they are copied over to the new backup CM (in slot CM). Again, the two Control Modules always keep their configurations in sync.

Hard Fail Over

During normal operation, the status of the primary CM is communicated to the backup CM through a heartbeat signal. As long as the backup CM receives heartbeats from the primary CM, the backup CM retains its standby status. If, however, the primary CM experiences a hardware failure, the heartbeat signals cease. The backup CM waits 20 seconds for the heartbeats to resume, if they do not, the backup CM assumes the role of primary CM. As with the soft fail over, the new primary CM maintains existing layer-2 and layer-3 flows and begins learning new flows within 5 to 20 seconds. Once the routing protocols have converged (60 seconds), layer-3 flows are aged out gracefully and replaced with new flows.



Note The amount of time that the backup CM waits before taking over as the primary CM because of a hard failover is configured using the **system set backup-cm-timeout** command from within Configure mode. The timeout can be set between 20 and 1000 seconds.

If the failed primary CM (in slot 1) is replaced by a new Control Module, the new CM assumes the role of backup CM.

4.9.2 Communicating with the Backup Control Module

There are two ways to establish communication with the backup CM: through the backup CM's console port or through a telnet session from the primary CM to the backup CM using the keyword **backup-cm**. For instance, the following example shows a telnet session from the primary CM to the backup CM.

telnet RS1

```
-----  
RS 16000 System Software, Version 8.0  
Copyright (c) 2000-2001 Riverstone Networks  
System started on 2001-04-24 09:37:35  
-----
```

Press RETURN to activate console . . .

```
rs1> enable  
rs1#  
rs1# telnet backup-cm  
Trying 127.0.0.1, port 10130 ...  
Connected to 127.0.0.1.  
Escape character is '^['.
```

```
-----  
RS 16000 System Software, Version 8.0  
Copyright (c) 2000-2001 Riverstone Networks, Inc.  
System started on 2001-04-19 14:40:57  
-----
```

Press RETURN to activate console . . .

```
rs1>$
```

Notice in the example above that the prompt displays a dollar sign (\$). This indicates that the display belongs to the backup CM. The dollar sign also appears if you connect to the backup CM through its console port.

When connected to the backup CM (either through telnet or the console), you are provided with only a sub-set of the commands available on the primary CM.

For example, enter Enable mode on the backup CM, and then enter the help command (?). This produces the following output:

```
rs1>$enable

rs1# $?
cli          - Modify the command line interface behavior
enable       - Enable privileged user mode
exit         - Exit current mode
file         - File manipulation commands
logout       - Log off the system
reboot       - Reboot the system
system       - Show system global parameters
rs1# $
```

Notice that most of the Enable mode functionality is missing and there is no access to Configure mode. However, the backup CM does provide access to both the **file** and **system** facilities. These facilities allow you to do the following on the backup CM:

- Copy files
- Delete files
- Rename files
- Reformat the file system
- List system images
- Choose system images

**Note**

Also, you can enter the **reboot** command from the backup CM, however, the command reboots only the backup CM – the primary CM is not affected.

4.9.3 Redundant Control Module Issues

This section points out several issues that must be taken into account when using redundant Control Modules.

Booting the RS 16000 From the Network

If you have set the RS 16000 to obtain its image software from a TFTP server (see [Section 5.3, "Loading Software from the Network"](#)), the IP addresses that appear for **netaddr** from within BootPROM mode should be different for both the primary and backup CM. Furthermore, the IP address of the Ethernet management interface (en0) should differ from both **netaddr** addresses. These IP addresses are listed below:

- One unique primary CM boot IP address
- One unique backup CM boot IP address
- One unique en0 interface IP address

If any of these IP addresses are the same, non-unique IP address errors will occur during failover. Furthermore, none of the IP addresses mentioned above can be used to create an IP interface.

Software/Hardware Versions

Make sure that the software images are the same on the primary CM and backup CM – it is possible to have two different software images on each Control Module. If the images are not the same and fail over occurs, the image on the backup CM may or may not be able to process the configuration of the failed primary CM.



Caution Both the primary and backup Control Modules should be of the same hardware version, and should contain the same amount of memory.

Changing Mastership

Whenever the power is cycled on the RS, the default relationship between the primary and backup CM is reestablished. In other words, the Control Module in slot CM (whatever its role) becomes the primary CM and the Control Module in slot CM/1 becomes the backup CM. If a hardware fail over occurs, do not power down the RS. Instead, hot-swap the new Control Module into slot CM. As it boots, it will assume the role of the backup CM, and will obtain its configuration from the current primary CM. Enter the **save startup** command on the primary CM. Once this file transfer is complete, you can restore the default roles of the Control Modules by entering the **system redundancy change-mastership** command.

Hot-Swapping

Never hot-swap a line card either in or out of the RS 16000 while the backup CM is still booting. Always wait until both CMs are fully operational before hot-swapping line cards.

5 SOFTWARE MANAGEMENT

This chapter describes how to perform operations with RS 16000 operating software and bootPROM image software. The following topics are covered:

- Upgrading the system image software
- Upgrading the Boot PROM image software
- Loading RS 16000 software from a TFTP server
- Loading RS 16000 software from a BootP/TFTP server
- Upgrading the operating software without rebooting the RS
- Upgrading FPGA code on line cards

5.1 UPGRADING SYSTEM IMAGE SOFTWARE

To upgrade the system software and boot using the upgraded image, perform the following procedure.

1. Display the current boot settings by using the **system show version** command. Note the current **Image Boot Location**.

Here is an example:

```
rs# system show version
Software Information
  Software Version   : 8.01.A.09
  Copyright          : Copyright (c) 2000-2001 Riverstone Networks, Inc.
  Image Information  : Version 8.01.A.09, built on Mon Jul 30 11:07:13 2001
  Image Boot Location: file:/pc-flash/boot/img/ros801
  Boot Prom Version  : prom-2.0.1.1
```

In the example above, the location “**pc-flash**” indicates that the RS 16000 is set to use the factory-installed software on the PC card.

2. Copy the upgrade system software onto a TFTP server that the RS 16000 can access. (Use the **ping** command to verify that the RS 16000 can reach the TFTP server.)



Note If the TFTP server is one or more hops away from the RS 16000, add a route to the TFTP server's network using the **ip add route** command.

3. Enter the following command to copy the software upgrade onto the RS 16000's PC card:

```
system image add <IPaddr-of-TFTP-host> <image-file-name>
```



Note The *<image-file-name>* is the full directory path and filename to the image software file on the TFTP server.

Here is an example:

Figure 1.

```
rs# system image add 134.152.178.5 tftpboot/ros8100
Downloading image 'tftpboot/ros8100' from host '134.152.178.5'
to local image ros8100 (takes a while) . . .
download: done
save:
kernel: 100%
done
Image checksum validated.
%SYS-I-BOOTADDED, Image 'ros8100' added.
```

4. Enter the **system image list** command to list the images on the PC card and verify that the new image is present:

Here is an example:

```
rs# system image list
Images currently available on Master CM
slot0:
ros8100 (version 8.1.0.0)
ros7000 (version 8.0.0.0) [selected for next boot]
```

5. Use the **system image choose** command to select the image file that the RS 16000 will use when rebooted.

Here is an example:

```
rs# system image choose ros8100
Found image in slot0
Making image rs7300 (version 8.1.0.0) the active image
for next reboot on Master CM . . .
%SYS-I-CHS_PRIMARY_OK, image successfully chosen on Primary CM
rs#
```



Note If the RS has a redundant Control Module, the upgrade performed on the primary CM will occur automatically on the backup CM.

6. Use the **system image list** command to verify the change.



Note You do not need to activate this change.

7. Reboot the RS 16000 to load and run the new system software image.

5.2 UPGRADING BOOT PROM SOFTWARE

The RS 16000 boots using the boot PROM image software installed on the Control Module's internal memory. To upgrade the boot PROM image, use the following procedure.

1. Display the current boot settings by entering the **system show version** command. Note the current **Boot Prom Image** version.

Here is an example:

```
rs# system show version
Software Information
  Software Version   : 8.01.A.09
  Copyright          : Copyright (c) 2000-2001 Riverstone Networks, Inc.
  Image Information  : Version 8.01.A.09, built on Mon Jul 30 11:07:13 2001
  Image Boot Location: file:/pc-flash/boot/img/ros801
  Boot Prom Version  : prom-2.0.1.1
```

2. Copy the upgrade boot PROM image software onto a TFTP server that the RS 16000 can access. (Use the **ping** command to verify that the RS 16000 can reach the TFTP server.)



Note If the TFTP server is one or more hops away from the RS 16000, add a route to the TFTP server's network using the **ip add route** command.

3. Enter the following command to copy the bootPROM upgrade onto the RS 16000's internal memory:

```
system promimage upgrade <IPaddr-of-TFTP-host> <image-file-name>
```



Note The *<image-file-name>* is the full directory path and filename to the bootPROM image file on the TFTP server.

Here is an example:

```
rs# system promimage upgrade 134.152.178.5 tftpboot/prom-211
Downloading image 'tftpboot/prom-211' from host '134.152.178.5'
image is a prom upgrade to version 'prom-2.0.1.1'
tftp complete
checksum valid. Ready to program.
Active-CM: flash found
Active-CM: erasing...
Active-CM: programming...
Active-CM: verifying...
Active-CM: programming successful.
Active-CM: Programming complete.
rs#
```

4. Reboot the RS 16000.
5. Enter the **system show version** command to verify that the new boot PROM software is in the internal memory of the RS 16000's Control Module.

5.3 LOADING SOFTWARE FROM THE NETWORK

Typically, the RS 16000 loads its operating software from the PC flash card inserted in the Control Module. Alternately, the RS 16000 can be configured to ignore its PC flash image and obtain its software from a network server. The RS 16000 can obtain its image software from either a TFTP or BootP/TFTP server.



Note If you are loading software from the network and are using redundant Control Modules, see [Section 4.9.3, "Redundant Control Module Issues"](#) for information regarding interface addresses.

5.3.1 Loading Image Software from a TFTP Server

Perform the following procedure to configure the RS 16000 to load its image software from a TFTP server:

1. Copy the image software onto a TFTP server that the RS 16000 can access.
2. Reboot the RS 16000 and enter Boot mode by pressing the "Esc" key to interrupt the normal boot process.
3. At the Boot prompt, enter the **set** command to view the current bootROM variable values.

Here is an example:

```
re-boot> set
...tty1 = 9600
bootdiagmode = off           [off on quick mfg-test]
  diag_log =
mfg_loop_by = time           [time count]
mfg_loop_max = 86400
  bootdelay = 2
promsetaddrs = 1
flow_control = on            [off on]
bootptimeout = 5
  netaddr = 0.0.0.0
  autoboot = boot
  netmask = 0,0,0,0
  gateway = 0.0.0.0
bootsource = /pc-flash/boot/ros80
  bootaddr = 0.0.0.0
  ethaddr = 00:00:1d:12:34:56
(ethaddr is base MAC addr, add one for actual CPU MAC address)
  sysid = -1
rs-boot>
```

4. Notice in the example above that netaddr, netmask, and gateway have the value **0.0.0.0**, and that **bootsource = /pc-flash/boot/ros80**.
5. From the Boot prompt, use the **set** command to set the following:
 - IP address of the RS 16000 – (**netaddr**)

- Subnet mask for the RS 16000 – (**netmask**)
- The IP address of the RS 16000's default gateway – (**gateway**)
- Full path and filename to the software image on the TFTP server – (**bootsource**)
- IP address of the TFTP server – (**bootaddr**)

```
rs-boot> set netaddr <IPaddr>
rs-boot> set netmask <subnet-mask>
rs-boot> set gateway <IPaddr>
rs-boot> set bootsource <dir-filename>
rs-root> set bootaddr <IPaddr>
```

Here is an example:

```
rs-boot> set netaddr 134.152.179.132
rs-boot> set netmask 255.255.255.224
rs-boot> set gateway 134.152.179.129
rs-boot> set bootsource /tftpboot/ros80
rs-boot> set bootaddr 134.152.176.5
```

6. Enter the **set** command to view the changes.

Here is an example:

```
rs-boot> set
...
  netaddr = 134.152.179.132
  autoboot = boot
  netmask = 255.255.255.224
  gateway = 134.152.179.129
  bootsource = /tftpboot/ros80
  bootaddr = 134.152.176.5
  ethaddr = 00:00:1d:12:34:56
(ethaddr is base MAC addr, add one for actual CPU MAC address)
  sysid = -1
rs-boot>
```

7. From the Boot prompt, use the **ping** command to verify that the RS 16000 can reach the TFTP server.
8. Reboot the RS 16000. As the RS 16000 initializes, it ignores the software image on the PC card and retrieves its operating software from the TFTP server at **134.152.176.5**.

Here is an example

```
re-boot> boot
Rebooting. . .
. . .source: tftp://134.152.176.5/tftpboot/roa80
Build location: host 'matrix' by 'adm'...
Version: 8.0.0.0 . . .
```

5.3.2 Loading Image Software from a BootP/TFTP Server

The RS 16000 contains a BootP client and can be configured to obtain its image software from a BootP/TFTP server. Using the BootP client allows the RS 16000 to obtain its software network address from the server using only its MAC address. This eliminates the need to initially configure the RS's IP address, subnet mask, and boot source.

To configure the RS 16000 to use its BootP client to obtain its image software, perform the following procedure:

1. Load the RS 16000's image software on a BootP/TFTP server that can be reached by the RS 16000.
2. Boot the RS 16000 and enter Boot mode by interrupting the normal startup sequence by pressing the "Esc" key.
3. Use the **set** command to obtain the RS 16000's base MAC address (**ethaddr**).
4. Add one to the base address to obtain the MAC address of the RS 16000's CPU.

Here is an example:

```
re-boot> set
...tty1 = 9600
bootdiagmode = off           [off on quick mfg-test]
  diag_log =
mfg_loop_by = time           [time count]
mfg_loop_max = 86400
  bootdelay = 2
promsetaddrs = 1
flow_control = on            [off on]
bootptimeout = 5
  netaddr = 0.0.0.0
  autoboot = boot
  netmask = 0,0,0,0
  gateway = 0.0.0.0
bootsource = /pc-flash/boot/ros80
  bootaddr = 0.0.0.0
  ethaddr = 00:00:1d:12:34:56          <base MAC address>
(ethaddr is base MAC addr, add one for actual CPU MAC address)
  sysid = -1
rs-boot>
```

From the example above, adding one to the base MAC address equals **00:00:1d:12:34:57**, which is the address of the RS 16000's CPU.

5. Use the **set** command to change the value of **autoboot** to **bootp**.

Here is an example:

```
rs-boot> set autoboot bootp
```

6. Configure the BootP/TFTP server with the RS 16000's CPU MAC address, an appropriate IP address, and the location of the RS 16000 software image file. Additionally, make sure that the ARP cache of the BootP/TFTP server is set correctly for the RS 16000.
7. Reboot the RS 16000 by entering the **reboot** command at the Boot prompt.

Here is an example:

```
rs-boot> reboot

Ethernet Base address = 00:00:1d:12:34:56
Ethernet CPU address  = 00:00:1d:12:34:57

Performing Bootp with timeout in 5 seconds.
** plen = 300 plen - sizeof(struct bootp) = 0
BOOTPD='134.141.179.134'
netaddr='134.141.179.132'
* bootp source is C:\TFTPBOOT\ROS80
Booting boot file C:\TFTPBOOT\ROS80.
source: tftp://134.141.179.134/C:\TFTPBOOT\ROS80
File: version (703 bytes)
Build location: host 'matrix' by 'adm'
Version: 8.0.0.0
Build date: Mon Dec 25 23:56:47 2000
File: kernel (3568593 bytes)
Loading kernel (base 0x80001000, size 50528)
(base 0x8000d560, size 3507312)
100% - kernel loaded...
...
...
Press RETURN to activate console . . .
```

5.4 HITLESS SOFTWARE UPGRADE

The operating software for RS 16000 switch routers equipped with redundant Control Modules (CMs) can be upgraded without having to reboot the system. This ability to update the software without rebooting the RS is known as a “hitless” upgrade, referencing the fact that all flows and routes are maintained throughout the upgrade process.



Note OC-12 and all Smartcards in general are reset when performing a hitless upgrade if there is a change to the code for these specific line cards (checksum has changed).

The basic process of performing a hitless upgrade is outlined below:

- New software is placed on a reachable TFTP server
- Software is downloaded to the backup CM

- The backup CM is rebooted
- The backup CM is changed to the primary CM

5.4.1 Hitless Upgrade Example

The following is a step-by-step example of performing a hitless upgrade. Note that for this example, the TFTP server IP address is 134.141.178.5 and the upgrade image path and filename is “/tftpboot/ros12.” Furthermore, in this example, the primary CM resides in slot CM and the backup CM resides in slot CM/1.

1. Load the new RS operating software image onto a TFTP server that is reachable by the RS.
2. Enter the **system image add backup-cm** command to load the new software image onto the backup CM.

```
rs# system image add 134.141.178.5 /tftpboot/ros12 backup-cm

**Warning: Be sure to also add this image to the
Primary Control Module so that the same images
exist on the Control Modules. Failure to do so
may prevent hot failover from working correctly.

Downloading image '/tftpboot/ros12' from host '134.141.178.5'
download: done

Adding Image (Backup CM)
to local image ros12 (takes a while) . . .
save:
kernel: 100%
images/ssr_atm: 100%
images/ssr_cmhe: 100%
images/ssr_wan: 100%
images/ssr_atm155_sar: 100%
images/ssr_atm155_fpga_400: 100%
images/ssr_atm155_fpga_800: 100%
images/ssr_mpls_dp_tmac: 100%
images/ssr_mpls_mc_tmac: 100%
images/ssr_atm622_amac: 100%
images/ssr_atm622_sar_rcv: 100%
images/ssr_atm622_sar_xmt: 100%
images/ssr_atm622_sar_diag: 100%
images/hdrproc2: 100%
done
Image checksum validated.
%SYS-I-BOOTADDED, Image 'ros12' added.
rs#
```

3. Enter the **system image choose backup-cm** command and choose the new software image as the image to use for the next reboot.

```
rs# system image choose ros12 backup-cm

**Warning: Be sure to also choose this image on the
Primary Control Module so that the same images
are chosen for next reboot on the Control Modules.
Failure to do so may prevent hot failover
from working correctly.

Choosing image on Backup CM
Making image ros12 (version 12.0.0.0) the active image
for next reboot . . .
%SYS-I-CHS_OK, image successfully chosen
rs#
```

4. Enter the **system redundancy reboot-backup-cm** command to reboot the backup CM, which contains the new software image.

```
rs# system redundancy reboot-backup-cm
%SYS-I-HOTSWAP_OUTRXD, received hotswapped-out request for slot 1
%SYS-I-HOTSWAP_INQUEUED, hotswap busy, request for hotswap-in slot 1
queued
2001-12-05 18:12:21 %SYS-I-HOTSWAPOUT, module in slot CM/1 is hotswapped
out
rs# 2001-12-05 18:12:21 %SYS-I-HOTSWAP_INRXD, received hotswapped-in
request for slot 1, detecting, please wait
2001-12-05 18:12:24 %SYS-I-MULTICPU, additional CPU Module(s) detected
in slot CM/1
2001-12-05 18:12:24 %SYS-I-HOTSWAPIN, module in slot CM/1 is hotswapped
in
2001-12-05 18:13:42 %SYS-I-ACTIVECFGTOBACKUP, active configuration
updated on Backup CM
rs#
```

5. Once the backup CM is fully active, enter the **system redundancy change-mastership** command

```
rs# system redundancy change-mastership
Upgrading in progress
2001-12-05 18:18:22 %HBT-I-DISABLE, disabled failover
rs# 2001-12-05 18:18:24 %HBT-I-ENABLE, enabled failover
```

The backup CM (in slot CM/1) becomes the primary CM, while the old primary CM (in slot CM) becomes the backup CM.

6. Log into the new primary CM and check for hardware/software incompatibility and configuration file issues (if any). Remember, if needed, the current backup CM (in slot CM) still contains the old software and configuration files.

- When satisfied with the software upgrade, you can repeat the previous steps to load the upgraded software onto the Control Module in slot CM (currently the backup CM) and return its state to primary CM.

5.5 UPGRADING FPGA CODE

On occasion, Riverstone Networks may make upgraded Field Programmable Gate Array (FPGA) code available for certain line cards. To download an FPGA upgrade, use the **system linecard** command from Enable mode.

The **system linecard** command can download FPGA code from either a flash RAM card residing in one of the active Control Module's flash RAM slots (**slot0** or **slot1**) or from a TFTP server on the network. In either case, a filename is specified that contains the FPGA code, and the line card that receives the upgrade is hot swapped out and then back in for the upgraded code to take effect.



Note No traffic is passed on the line card while the FPGA upgrade process is being performed.

5.5.1 Upgrading FPGA Code from a TFTP Server

Follow these steps to upgrade a line card's FPGA code using a TFTP server.

In this example, the TFTP server address is **10.50.89.88**, the path and filename of the FPGA code is **posrel/oc12_mpls_38k/oc12mr38.000**, and the line card to be upgraded is a 2-port, OC-12c, POS board in slot **6**.

- Load the FPGA code onto the TFTP server. Make sure that the RS can reach the server across the network.
- Enter the **system linecard upgrade** command, specifying the IP address of the TFTP server, the full path and filename of the FPGA code, and the slot number within which the line card resides.

```
rs# system linecard upgrade 10.50.89.88 posrel/oc12_mpls_38k/oc12mr38.000 module 6
Downloading package 'posrel/oc12_mpls_38k/oc12mr38.000' from host '10.50.89.88'
download: done
pos02_oc12_mpls.bin: 100%
pos13_oc12_mpls.bin: 100%
pos_tmac_dp.bin: 100%

About to program the module in slot 6.
This will stop any traffic on that module until the
programming is complete and the module is restarted.

Are you sure you want to do this [no]? yes
upgrading POSITRON_FLASH_0_2 in slot 6 with pos02_oc12_mpls.bin
flash found
erasing...
erasing...
programming...
```

```

verifying...
programming successful.
Programming complete.
upgrading POSITRON_FLSH_1_3 in slot 6 with pos13_oc12_mpls.bin
flash found
erasing...
erasing...
programming...
verifying...
programming successful.
Programming complete.
upgrading TMAC_FLSH_0 in slot 6 with pos_tmac_dp.bin
flash found
erasing...

erasing...
programming...
programming...
verifying...
programming successful.
Programming complete.
Do you want to restart module 6 at this time [no]? yes
%SYS-I-HOTSWAP_OUTRXD, received hotswapped-out request for slot 6
%SYS-I-HOTSWAP_INQUEUED, hotswap busy, request for hotswap-in slot 6
queued
2002-05-30 14:08:37 %SYS-I-HOTSWAPOUT, module in slot 6 is hotswapped out
2002-05-30 14:08:37 %SYS-I-HOTSWAP_INRXD, received hotswapped-in
request for slot 6, detecting, please wait
2002-05-30 14:08:44 %SYS-I-DSCVMOD, discovered '2-POS OC12 "M"' module in slot 6
2002-05-30 14:08:47 %SYS-I-INITPORT, initialized slot 6, port 1
2002-05-30 14:08:47 %SYS-I-INITPORT, initialized slot 6, port 2
2002-05-30 14:08:52 %SYS-I-HOTSWAPIN, module in slot 6 is hotswapped in
rs#

```

3. After the FPGA upgrade process completes, the line card starts passing traffic.

Notice in the example above that the hot swapping out and in occurs as part of the upgrade process – and does not have to be performed after the upgrade.

5.5.2 Upgrading FPGA Code from a Flash RAM Card

FPGA code can be downloaded directly from a flash RAM card residing within one of the Control Module's RAM card slots. Upgrading a line card's FPGA code from a flash RAM card may be desirable if, for instance, your upgrade involves a large number of RS switch routers. In such a case, the flash RAM card can be moved from RS to RS.

In this example, the FPGA code is downloaded from a network TFTP server and copied directly to the flash RAM card in **slot0** of the active Control Module. Once copied to the flash RAM card, the upgrade is performed using the image on the flash RAM card in **slot0**.

1. Load the FPGA code files onto the TFTP server. Make sure that the RS can reach the server across the network.

Enter the **system linecard upgrade** command, specifying the IP address of the TFTP server, the full path and filename of the FPGA code, and the slot number within which the flash RAM card resides.

```
rs# system linecard upgrade 10.50.89.88 posrel/oc12_mpls_38k/oc12mr38.000 slot0
Downloading package 'posrel/oc12_mpls_8k/oc12mr8x.000' from host '10.50.89.88'
download: done
Writing package 'oc12mr8x.000' to '/pc-flash0/linecard'
save: done
rs#
```

2. Use the **system linecard list-images** command to see the FPGA code that has been copied to the flash RAM card.

```
rs# system linecard list-images
slot0: oc12mr8x.000
rs#
```

3. Use the **system linecard upgrade** command to upgrade the line card with the FPGA code on the flash RAM card in **slot0**. Notice that only the filename is specified – the RS knows the correct path to the FPGA files on the flash RAM card.

```
rs# system linecard upgrade slot0 oc12mr8x.000 module 6
Downloading package '/pc-flash0/linecard/oc12mr38.000' from slot0
download: done
pos02_oc12_mpls.bin: 100%
pos13_oc12_mpls.bin: 100%
pos_tmac_dp.bin: 100%

About to program the module in slot 6.
This will stop any traffic on that module until the
programming is complete and the module is hotswapped.

Are you sure you want to do this [no]? yes
upgrading POSITRON_FLSH_0_2 in slot 6 with pos02_oc12_mpls.bin
flash found
erasing...
```

As with the previous example, the line card is hot swapped out and then back in as part of the upgrade process.

APPENDIX A TROUBLESHOOTING

If you experience difficulty with the basic hardware or software setup procedures in this guide, check the following table. If you find a description of the difficulty you are experiencing, try the recommended resolution. If the resolution does not remove the difficulty or it is not listed in this appendix, contact:

Riverstone Technical Assistance Center - RTAC

- Telephone: (408) 844-0010 or (877) 776-8229 toll free
- International toll-free numbers are listed on the Internet support site (www.riverstonenet.com/support)
- FAX: (408) 878-6920
- Internet address: www.riverstonenet.com/support
- Email: support@riverstonenet.com

Table A-1 Troubleshooting

If you experience this difficulty...	Try this remedy...
The RS 16000 exhibits no activity (no LEDs are on, the fan assembly is not operating, and so forth).	If you have an AC power supply, make sure the power supply is installed properly and plugged into an active power source. Also make sure the power switch is on. Refer to Section 3.3.5, "Installing AC Power Supplies". If you have a DC power supply, make sure it is wired properly to a functional, active DC source. Also ensure the power supply is installed properly and the power switch is on. Refer to Section 3.3.6, "Installing DC Power Supplies"
The power supply is properly installed but is not operating.	Check the power cord (wiring) and the circuit (source) to which the supply is connected.

Table A-1 Troubleshooting (Continued)

If you experience this difficulty...	Try this remedy...
The fan assembly is not active.	Make sure the fan assembly is properly installed. Refer to Section 3.3.7, "Installing the Fan Assembly". Check the power cord (wiring) and the circuit (source) to which the supply is connected. If the green status LED on the power supply indicates that it is active, immediately power down the chassis, unplug (disconnect) the power supply, and contact Riverstone Technical Support. The fan assembly may be improperly connected or damaged.
Control Module is not active.	Check the power cord (or wiring) and the circuit to which the power supply is connected. If the power supply is working, make sure the Control Module is inserted all the way into its slot in the chassis and the captive screws are screwed in. The Control Module must be in a Control Module slot (slot 1 or slot 2), and not in a line card slot. Refer to Section 3.3.8, "Installing the Control Module".
No line cards are active.	Check the power cord (wiring) and the circuit (source) to which the supply is connected.
A specific line card is inactive.	Make sure the line card is inserted all the way into the chassis and the captive screws are screwed in. Refer to Section 3.3.9, "Installing Line Cards".
The chassis LEDs indicate activity but the RS 16000 is not performing as expected.	Make sure you have properly connected the primary Control Module to a management console and the console is powered on. Refer to Section 3.3.8, "Installing the Control Module" .
An older software version continues to boot instead of the newer version on a PC card or TFTP server.	Use the procedure in Section 5.1, "Upgrading System Image Software" to configure the RS 16000 to boot using newer software.
You cannot access the configuration commands in the CLI.	Enter the enable command to access the Enable mode, then enter the configure command to access the Configuration mode.
Configuration changes do not take effect.	Use the procedure in Section 4.3.1, "Activating the Configuration Commands in the Scratchpad" to activate the changes.
Configuration changes are not reinstated after a reboot.	Use the procedure in Section 4.3.2, "Saving the Active Configuration to the Startup Configuration File" to save the configuration changes to the Startup configuration file.

Table A-1 Troubleshooting (Continued)

If you experience this difficulty...	Try this remedy...
The RS 16000 is not resolving DNS names.	Use the procedure in Section 4.7, "Setting the DNS Domain Name and Address" to set up DNS. If you have already performed this procedure, make sure you can use NS lookup on the DNS server to get the default domain.
An SNMP manager cannot access the RS 16000.	Use the procedure in Section 4.6, "Setting Up SNMP" to set up an SNMP community string and specify a target for SNMP traps. If you have already performed this procedure, enter the snmp show all command to check the SNMP settings. Use the traceroute and ping commands to verify that the RS 16000 can reach the SNMP management station.
You are unable to ping a certain host.	Create and add an IP or IPX interface for the host. See the Riverstone RS Switch Router User Guide for information.

APPENDIX B INTERNATIONAL SAFETY INFORMATION

B.1 CONSIDERACIONES DE SEGURIDAD

Lea las siguientes advertencias relacionadas con la seguridad y el uso del equipo para evitar posibles lesiones personales o daños al producto.



Advertencia Lea las siguientes advertencias relacionadas con la seguridad y el uso del equipo para evitar posibles lesiones personales o daños al producto.

5.5.3 Prevención de Lesiones

- Para evitar una posible lesión, solicite la ayuda de otra persona al sacar el chasis fuera de la caja de embalaje.
- Nunca intente montar el chasis del RS 16000 en un rack sin la ayuda de otra persona. Solicite ayuda al levantar o sostener el chasis.
- Nunca opere el RS 16000 si las ranuras de las tarjetas de línea o los compartimientos del suministro de energía están expuestos. Es posible dejar expuestas las ranuras para las tarjetas **PCMCIA**, pero cerciúrese de no insertar objetos ajenos a las tarjetas PC flash correspondientes.
- Nunca opere el RS 16000 si el chasis se moja o se instala en un lugar mojado.

INDEX

A

access modes	4-4
activating config commands in scratchpad.....	4-6
address-based bridging	2-3
annotations in configuration files.....	4-8
application switching	2-5
assigning DNS servers	4-20
autoboot.....	5-7

B

backup CM	4-23
available commands	4-26
communicating with	4-25
prompt.....	4-25
rebooting.....	4-26
telnet	4-25
base MAC address.....	5-7
BGP	
2, 3, 4	2-4
Boot mode	4-4
boot PROM	5-3
boot sequence	4-1
boot source	5-5
booting from the network.....	4-26
BootP	
ethaddr	5-7
bootp.....	5-7
BootP client.....	5-7
autoboot	5-7
reboot	5-8
set autoboot bootp.....	5-8
set command	5-7
BootP/TFTP server.....	5-7
configuring.....	5-8
bootsource	4-14
bridging	2-3
address-based.....	2-3
flow-based	2-3
L2 lookup table.....	2-3
bridging and VLAN protocols	2-2

C

CLI	
activating.....	4-3
command history	4-5
Ctrl+a	4-5
Ctrl+b.....	4-5
Ctrl+d.....	4-5
Ctrl+e	4-5
Ctrl+f.....	4-5
Ctrl+n.....	4-5
Ctrl+p.....	4-5
Ctrl+u.....	4-5
Ctrl+x.....	4-5
Ctrl+z.....	4-5
line editing commands.....	4-5
starting	4-4
CLI access modes.....	4-4
Boot.....	4-4
Configure	4-4
Enable	4-4
User.....	4-4
Coarse Wavelength Division Multiplexing.....	2-20
community string.....	4-16
configuration	
active.....	4-6
DNS domain name and address	4-20
en0 Ethernet interface	4-11
saving.....	4-6
scratchpad	4-6
startup	4-6
trap target.....	4-16
viewing	4-8
configuration file annotations.....	4-8
Configure mode.....	4-4
configuring BootP/TFTP server	5-8
console port	4-1
Control Module	5-8
changing mastership	4-27
fail over	4-24
fail over time.....	4-25
IP addresses	4-26
messages	4-24
copy active to startup.....	4-7, 4-12

copy startup to scratchpad	4-15
CPU MAC address	5-7
Ctrl+z.....	4-4
CWDM	2-20
CWDM line card	2-19

D

date and time	4-10
default name	4-4
Dense Wavelength Division Multiplexing.....	2-20
DNS	4-20
DNS domain name	4-20
DNS names.....	A-3
DVMRP.....	2-4
DWDM.....	2-20

E

en0 Ethernet interface.....	4-11
Enable mode.....	4-4
exit command	4-4

F

fail over time	4-25
failover	4-24
Flash card	
adding new software image	5-1
flash RAM card	5-12
flow ACLs	
layer-3	2-5
layer-4	2-5
flow switching.....	2-5
flow-based bridging.....	2-3
FPGA.....	5-11, 5-12
FPGA code	5-11
functional layer terminology	2-1

G

GARP/GVRP	2-4
-----------------	-----

H

hard fail over	4-24
hardware and software capabilities	2-2
hardware overview	2-8
hitless upgrade.....	5-8

I

if you forget your password.....	4-14
IGMP	2-4
improving SNMP security	4-17
initial configuration	4-1
Internet address.....	A-1
ip add route	5-2
IPX routing	2-4
default	2-4
RIP	2-4
SAP	2-4
IS-IS.....	2-4
ISO 7-layer model	2-1

L

L2 lookup table.....	2-3
L3 lookup tables	2-4
Layer-4	
application switching	2-5
flow switching.....	2-5
layer-4 switching	2-5
LFAP	2-6
line editing commands.....	4-5
load balancing.....	2-6
loading image from BootP/TFTP	5-7
loading software from a TFTP server.....	5-5
loading software from the network	5-5

M

MAC address	5-7
management.....	2-2
CLI	2-7
SNMP.....	2-7
traps.....	2-7
management platforms	2-7
managing software	5-1
media interface	
802.3 (10Base-T)	2-2
802.3u (100Base-TX)	2-2
802.3x (1000Base-SX, 1000Base-LX).....	2-2
802.3z (1000Base-SX, 1000Base-LX).....	2-2
media interface protocol.....	2-2
MIB II.....	2-6
MIB II statistics	2-6
MIBs	4-18
multicast routing.....	2-4

DVMRP	2-4	redundant CMs	5-8
GARP/GVRP	2-4	redundant Control Modules	
IGMP	2-4	backup CM.....	4-23
O		primary CM	4-23
OSPF		RIP.....	2-4
v2	2-4	v1	2-4
P		v2	2-4
password		Riverstone Technical Assistance Center .	A-1
bypassing	4-14	RMON	2-6
Enable	4-13	RMON support.....	2-2
User.....	4-13	RMON v2.....	2-6
passwords	4-13	routing	2-3
persistence	2-7	IP.....	2-3
Port status		IPX.....	2-3
viewing	4-8	L3 lookup tables	2-4
port-based VLANs	2-3	routing protocols	2-2, 2-4
powering on.....	4-1	RS 16000	
primary CM.....	4-23	bridging and VLAN protocols.....	2-2
protocol-based VLANs	2-3	capacity	2-2
protocols		default name.....	4-4
bridging and VLAN.....	2-2	hot swapping.....	2-2
media interface	2-2	initial configuration	4-1
routing.....	2-2	management.....	2-2
Q		media interface protocols.....	2-2
QoS.....	2-5	redundancy.....	2-2
application flows.....	2-6	RMON support	2-2
layer-3	2-6	routing protocols.....	2-2
layer-4.....	2-6	security.....	2-5
prioritization	2-5	throughput.....	2-2
source-destination flows.....	2-6	RS 16000 not performing.....	A-2
strict priority queuing	2-6	RTAC	A-1
ToS octet rewrites.....	2-6	International toll-free numbers	A-1
traffic control queues	2-6	support@riverstonenet.com	A-1
traffic control queuing	2-6	Telephone numbers.....	A-1
weighted fair queuing	2-6	www.riverstonenet.com/support.....	A-1
weighted random early detection.....	2-6	S	
Quality of Service	2-6	SAP.....	2-4
R		save active	4-6, 4-11
RADIUS.....	2-5	save startup.....	4-7
redundancy	5-8	saving active configuration to startup	4-6
redundant.....	5-8	saving configuration changes	4-6
		scratchpad.....	4-6
		secondary IP addresses.....	2-4
		Secure Session Shells	2-5
		security	2-5
		application ACLs	2-5

applying ACLs to SNMP.....	4-17	LFAP.....	2-6
destination ACLs	2-5	MIB II	2-6
destination filters	2-5	Open APIs.....	2-6
flow ACLs	2-5	RMON	2-6
flow filters.....	2-5	RMON v2	2-6
RADIUS	2-5	sticky persistence.....	2-7
source ACLs	2-5	strict priority queuing	2-6
source filters.....	2-5	support@riverstonenet.com.....	A-1
SSH.....	2-5	supported MIBs	4-18
TACACS.....	2-5	SYSLOG	
TACACS+	2-5	error.....	4-22
session persistence.....	2-6	facility-type	4-23
set autoboot bootp	5-8	fatal	4-22
set command.....	4-14, 5-5, 5-7	informational.....	4-22
setting basic system information	4-10	setting levels	4-23
setting boot source.....	5-5	syslog.conf file	4-23
setting date and time.....	4-10	warning	4-22
setting passwords.....	4-13	SYSLOG levels	4-22
setting system contact.....	4-10	SYSLOG message types	4-22
setting system location	4-10	SYSLOG parameters.....	4-22
setting system name	4-10	syslog.conf file	4-23
setting trap target.....	4-16	system image add	5-2
setting up SNMP	4-16	system image choose.....	5-3
show port-status.....	4-8	system image list	5-2
skipconfig	4-15	system information	4-10
SNMP	4-16	system messages.....	4-22
applying ACLs.....	4-17	system promimage upgrade.....	5-4
community string	4-16	system set contact.....	4-10
disabling authentication traps	4-17	system set date.....	4-10
improving security	4-17	system set location.....	4-10
initial configuration	4-16	system set name.....	4-10
MIBs	4-18	system set syslog level	4-23
privilege	4-16	system show active-config	4-11
security.....	4-17	system show dns	4-21
supported MIBs	4-18	system show version.....	5-1, 5-3
trap-source	4-17		
SNMP manager cannot access the RS.....	A-3	T	
soft fail over	4-24	TACACS	2-5
software	5-8	TACACS+	2-5
software upgrade	5-1	TCP persistence	2-7
SSL persistence	2-7	Telnet to back-CM.....	4-25
starting the command line interface	4-4	TFTP server	5-1, 5-6, 5-11
startup configuration	4-6	loading software.....	5-5
static route to trap target.....	4-16	ToS octet rewrites.....	2-6
statistics	2-6	traffic control queues.....	2-6
layer-2	2-6	traffic control queuing	2-6
layer-3	2-6	trap target.....	4-16
layer-4	2-6		

static route.....	4-16
trap-source.....	4-17
Troubleshooting	A-1
config changes do not take effect	A-2
config changes not reinstated	A-2
config. command access	A-2
Control Module not active.....	A-2
fan module not active	A-2
line cards inactive	A-2
not operating	A-1
SNMP cannot access RS 16000.....	A-3
specific line card is inactive.....	A-2
unable to ping a host.....	A-3
wrong software version boots.....	A-2

U

unicast routing protocols	
BGP	2-4
IS-IS.....	2-4
OSPF.....	2-4
RIP	2-4
upgrade	5-8
upgrading.....	5-8
upgrading boot image	
image-file-name.....	5-4
ip add route	5-4
system promimage upgrade	5-4
system show version.....	5-3
upgrading boot PROM software	5-3
Upgrading FPGA	5-12
Upgrading FPGA Code	5-11
upgrading software	
image-file-name.....	5-2
ip add route	5-2
system image add.....	5-2
system image list	5-2
TFTP server	5-1
upgrading system image software.....	5-1
upgrading system software.....	5-8
User access mode	4-4

V

viewing active configuration.....	4-11
viewing current configuration	4-8
VLANs	
port-based	2-3

protocol-based.....	2-3
secondary IP addresses	2-4
VPN persistence	2-7

W

Wavelength Division Multiplexing (WDM)2-19	
web caching.....	2-6
web hosting	2-6
load balancing.....	2-6
persistence.....	2-6
session persistence	2-6
SSL persistence.....	2-7
sticky persistence	2-7
TCP persistence	2-7
VPN persistence.....	2-7
web caching	2-6
weighted fair queuing.....	2-6
weighted random early detection	2-6
www.riverstonenet.com/support	A-1