RS 2100 Switch Router Getting Started Guide

Release 7.0

36-003-03 Rev. 0B

COPYRIGHT NOTICES

REGULATORY COMPLIANCE INFORMATION

This product complies with the following:

SAFETY

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

ELECTROMAGNETIC

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

COMPATIBILITY (EMC)

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

REGULATORY COMPLIANCE STATEMENTS

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

FCC COMPLIANCE STATEMENT

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

Note   This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

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

INDUSTRY CANADA COMPLIANCE STATEMENT

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

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

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

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

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

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

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

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

VCCI COMPLIANCE STATEMENT

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

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

SAFETY INFORMATION: CLASS 1 LASER TRANSCEIVERS

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

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

- 21 CFR 1040.10 and 1040.11, U.S. Department of Health and Human Services (FDA)

- IEC Publication 825 (International Electrotechnical Commission)

- CENELEC EN 60825 (European Committee for Electrotechnical Standardization)

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

LASER RADIATION AND CONNECTORS

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6 dBm or 55×10^{-6} 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 8×10^3 W m^2 sr-1.

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

SAFETY INFORMATION: WICT1-12 T1 CARD

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

CONSUMER INFORMATION AND FCC REQUIREMENTS

1. This equipment complies with Part 68 of the FCC rules, FCC Registration Number 6TGUSA-46505-DE-N Riverstone Networks Inc. Model WICT1-12 Made in the USA. On the DS1/E1 WAN Module of this equipment is a label that contains, among other information, the FCC registration number and Ringer Equivalence Number (REN) for this equipment. If requested, provide this information to your telephone company.

2. The REN is useful to determine the quantity of devices you may connect to your telephone and still have all those devices ring when your number is called. In most, but not all areas, the sum of the REN's of all devices should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should call your local telephone company to determine the maximum REN for your calling area.

3. If your DS1/E1 WAN Module causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.

4. Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice so as to give you an opportunity to maintain uninterrupted service.

5. If you experience trouble with this equipment DS1/E1 WAN Module, please contact Riverstone Networks Inc., 5200 Great America Parkway, Santa Clara, CA 95054, 408 878-6500, for repair/warranty information. The Telephone Company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.

6. There are no repairs that can be made by the customer to the DS1/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.
SOFTWARE LICENSE AGREEMENT

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

This document is an agreement ("Agreement") between You, the end user, and Riverstone Networks, Inc. ("Riverstone") that sets forth your rights and obligations with respect to the software contained in CD-ROM or other media (including flash cards). BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIA-BILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT ALONG WITH THE HARDWARE PURCHASED AND PROOF OF PAYMENT TO RIVERSTONE OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

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

Riverstone will grant You a non-transferable, nonexclusive license to use the enclosed software (the "Licensed Software") in object code form solely on a single processing unit owned or leased by You or otherwise embedded in equipment provided by Riverstone and the accompanying documentation (the Licensed Software, the media embodying the Licensed Software, and the documentation are collectively referred to in this Agreement as the "Licensed Materials"); provided that You agree to the following terms and conditions:

1. **TERM AND TERMINATION.** This Agreement is effective from the date on which You open the package containing the Licensed Materials. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form and certifying in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been destroyed. The Agreement and your license to use the Licensed Materials will also terminate if You fail to comply with any term or condition herein. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Riverstone, Riverstone may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Riverstone and You. Upon such termination, You must destroy the Licensed Materials as set forth above. Sections 4, 5, 7, 8, 9, 10, 11, and 12 shall survive termination of this Agreement for any reason.

2. **GRANT OF SOFTWARE LICENSE.** The license granted to You by Riverstone when You open this sealed package authorizes You to use the Licensed Software for internal use only and only on any one, single processing unit owned or leased by You or otherwise embedded in equipment provided by Riverstone, or any replacement for that processing unit or equipment. A separate license, under a separate Software License Agreement, is required for any other equipment on which You or another individual or employee intend to use the Licensed Software.

3. **RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS**. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in

sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Riverstone's prior written consent, and in no event shall You operate more than one copy of the Licensed Software. You may not copy or reproduce the documentation. You agree 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.

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. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials, or any portion thereof, to any other party.

    (a)   You further 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 therefore 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. **PROTECTION AND SECURITY**. You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Riverstone or its employees, except for purposes specifically related to your use of the Licensed Software on a single unit as expressly provided in this Agreement, without the prior written consent of Riverstone. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Riverstone of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Riverstone or its Affiliates and/or its/their software suppliers.

6. **MAINTENANCE AND UPDATES**. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of a Riverstone Service and Maintenance Agreement, if Riverstone and You enter into such an agreement. Except as specifically set forth in such agreement, Riverstone shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

7. **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 Software.

8. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS**. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Riverstone and/or its suppliers. For Department of Defense units, the Product is

considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

9. **LIMITED WARRANTY AND LIMITATION OF LIABILITY**. Riverstone warrants that for a period of ninety (90) days from the date of shipment from Riverstone: (i) the media on which the Licensed Software is furnished will be free of defects in materials and workmanship under normal use; and (ii) the Licensed Software substantially conforms to its published specifications.   Except for the foregoing, the Licensed Software is provided AS IS. This limited warranty extends only to You as the original licensee. Your exclusive remedy and the entire liability of Riverstone and its suppliers and Affiliates under this limited warranty will be, at Riverstone's or its service center's option, repair or replacement; or, if neither of the foregoing is commercially reasonable, refund of the Licensed Software if reported (or, upon request, returned) to the party supplying the Licensed Software to You. In no event does Riverstone warrant that the Licensed Software is error free or that You will be able to operate the Licensed Software without problems or interruptions.

NEITHER RIVERSTONE NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, INCLUDING IMPLIED WARRANTIES OF MER-CHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED. THE LIM-ITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, LIABILITIES, REMEDIES, EXRESS OR IMPLIED, INCLUDING ANY OBLIGATION, LIABILITY, RIGHT, CLAIM, OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM NEGLIGENCE OF RIVERSTONE OR ITS AFFILI-ATES, ACTUAL OR IMPLIED.

IN NO EVENT WILL RIVERSTONE OR ITS AFFILIATES OR ANY OTHER PARTY BE LIABLE TO ANY PARTY FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, WHETHER CLAIMED BY REASON OF BREACH OF WARRANTY OR OTHERWISE AND WITHOUT REGARD TO THE FORM OF ACTION IN WHICH SUCH CLAIM IS MADE, EVEN IF RIVERSTONE, ITS AFFILIATES OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL RIVERSTONE, ITS AFFILIATES OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow exclusions of implied warranties or limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. In the event that an exclusion of any implied warranty is not permitted by law, the duration of such implied warranty is limited to the duration of the limited warranty set forth above. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

10. **GENERAL**.

(a)   This Agreement is not assignable or transferable in whole or in part by Customer without the prior written con-sent of Riverstone. Riverstone may assign this Agreement without Customer's consent, to any Affiliate, including a foreign sales corporation, or to any person or entity which acquires substantially all of the stock of Riverstone or the assets of Riverstone, or any applicable major division, unit, or subsidiary of Riverstone. Riverstone may subcontract its obligations under this Agreement pro-vided that Riverstone shall remain ultimately liable for the performance of subcontractor. The rights of Riverstone and Your obli-gations under this Agreement shall inure to the benefit of Riverstone's assignees, licensors, and licensees.

(b)   Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

(c)   The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall never-theless be binding on and enforceable by and between the parties hereto.

(d)   Riverstone's waiver of any right shall not constitute waiver of that right in future. This Agreement 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.

(e) Should You have any questions regarding this Agreement, You may contact Riverstone at the address set forth below. Any notice or other communication to be sent to Riverstone must be mailed by certified mail to the following address: RIVERSTONE NETWORKS, INC. 5200 Great America Parkway, Santa Clara, CA 95054, Attn: Legal Department.

(f) The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts.

(g) For the purposes of this Agreement, "Affiliates" shall mean an "affiliate" of or a party "affiliated" with, a specified party that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified.

RIVERSTONE STANDARD WARRANTY

A. <u>Product Warranty</u>

   i. RIVERSTONE warrants that each unit of Hardware Products will be free from defects in material and workmanship for a period of one (1) year from the date of shipment.

   ii. Breach of warranty will be enforceable against RIVERSTONE only if written notice of such breach is received by RIVERSTONE within the applicable warranty period.

   iii. If a warranty claim is invalid for any reason, PURCHASER will be charged for services performed and expenses incurred by RIVERSTONE in repairing, handling and shipping the returned item.

   iv. Expendable parts, such as fuses, lamps, filters, and other parts that are regularly replaced due to normal use are excluded from this warranty.

   v. As to replacement parts supplied for a Product or repairs performed to a Product during the original warranty period for such Product, the warranty period on the replacement part or the repaired part shall terminate thirty (30) days after shipment or upon the termination of the warranty period applicable to the original item, whichever is longer.

   vi. As to any out-of-warranty parts repaired, modified or replaced by RIVERSTONE at RIVERSTONE's regular charges, the warranty period with respect to the material and workmanship hereunder shall expire thirty (30) days after the date of shipment of said part.

B. <u>Software Warranty.</u> The only warranty RIVERSTONE makes to PURCHASER in connection with the Licensed Materials is that the media upon which the Licensed Materials are recorded will be replaced without charge, if RIVERSTONE in good faith determines that the media was defective and not subject to misuse.

C. <u>Return to Factory.</u>

   i. If Parts, Products or Licensed Materials under warranty are claimed to be defective, RIVERSTONE must be notified by PURCHASER prior to the return of said Part, Product, or Licensed Materials. Within ten (10) days of the date of said notification RIVERSTONE will provide PURCHASER with a valid Return Material Authorization number, the location to which PURCHASER must return the shipment claimed to be defective, and the method of transportation. In no event will RIVERSTONE accept any returned part or Product which does not have a valid Return Material Authorization number.

   ii. Within ten (10) days of receipt of notice from RIVERSTONE requiring return, PURCHASER shall deliver said shipment to a carrier at PURCHASER's facilities as aforesaid.

   iii. Within thirty (30) days of receipt of same, RIVERSTONE shall use reasonable efforts to fix or replace, at its option, any defective Product or Licensed Material which RIVERSTONE has determined to be under warranty.

   iv. Transportation costs relating to warranty claims will be borne by RIVERSTONE only in cases where repair or replacement is made and authorized pursuant hereto, but any applicable duties will be paid by PURCHASER. If no warranty repair or replacement was required, all transportation costs will be borne by PURCHASER. "Emergency" transportation costs shall be borne by PURCHASER or its Customer.

D. <u>Installation Warranty</u>: RIVERSTONE warrants that all Installation Services rendered pursuant hereto shall be accomplished in a good and workmanlike manner and shall be free of defects in workmanship for a period of ninety (90) days from the date that such services were rendered.

E. <u>General</u>

   i. The above warranties are for the benefit of and shall apply only to PURCHASER.

   ii. RIVERSTONE's warranties shall not apply to any Product or Licensed Material which has been subjected to accident, neglect, misuse, abuse, vandalism, negligence in transportation or handling, failure of electric power, air conditioning, humidity control, causes other than ordinary use, or causes beyond RIVERSTONE's control, or if the Product or Licensed Material was not properly maintained by PURCHASER during the warranty period.

   iii. There shall be no warranty or liability for any Product or Licensed Materials which have been modified by PURCHASER without RIVERSTONE's prior written approval.

   iv. Parts or Replacement Products or Licensed Materials outside the scope of these warranties or with respect to Product(s) or Licensed Material out-of-warranty will be furnished at the established charges of RIVERSTONE then

in effect.

   v. RIVERSTONE shall have full and free access to the Products and Licensed Materials at PURCHASER's Customer's site, if required.

   vi. RIVERSTONE shall not be responsible for failure to furnish Parts due to causes beyond its control. RIVERSTONE shall not be required to replace any Part if it would be impractical for RIVERSTONE personnel to do so because of unauthorized alterations to the Products or its unauthorized connection by mechanical or electrical means to another system or device.

F.   Limitation of Liability

   i. THESE WARRANTIES AND RIVERSTONE'S AND ITS AFFILIATES LIABILITY AND PURCHASER'S REMEDIES WITH RESPECT THERETO, AS SET FORTH HEREIN, ARE EXCLUSIVE AND EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, LIABILITIES, REMEDIES, EXPRESS OR IMPLIED, INCLUDING ANY OBLIGATION, LIABILITY, RIGHT, CLAIM, OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM NEGLIGENCE OF RIVERSTONE OR ITS AFFILIATES, ACTUAL OR IMPUTED, AND NO WARRANTIES, EXPRESS OR IMPLIED REPRESENTATIONS, PROMISES OR STATEMENTS HAVE BEEN MADE BY RIVERSTONE OR ITS AFFILIATES UNLESS CONTAINED IN THIS AGREEMENT. NO WARRANTY, EXPRESS OR IMPLIED, IS MADE HEREIN THAT THE LICENSED MATERIALS, PRODUCTS OR ANY PARTS ARE MERCHANTABLE, OR FIT OR SUITABLE FOR THE PARTICULAR PURPOSES FOR WHICH THE LICENSED MATERIALS, PRODUCTS OR PARTS MAY BE ACQUIRED BY PURCHASER. IN NO EVENT SHALL RIVERSTONE OR ITS AFFILIATES BE LIABLE TO PURCHASER FOR ANY INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES INCLUDING WITHOUT LIMITATION, LOSS OF DATA, OR PROFITS, WHETHER CLAIMED BY REASON OF BREACH OF WARRANTY OR OTHERWISE, AND WITHOUT REGARD TO THE FORM OF ACTION IN WHICH SUCH CLAIM IS MADE.

   ii. The Products and Licensed Materials are not specifically developed, or licensed for use in any nuclear, aviation, mass transit, or medical applications or in any other inherently dangerous applications. PURCHASER hereby agrees that RIVERSTONE shall not be liable for any claims or damages arising from such use if PURCHASER uses the Products and/or Licensed Materials for such applications. PURCHASER agrees to indemnify and hold RIVERSTONE harmless from any claims for losses, costs, damages, or liability arising out of or in connection with the use of the Products and/or Licensed Materials in such applications.

   iii. Notwithstanding anything contained herein to the contrary, the total maximum liability of RIVERSTONE and it's Affiliates under this warranty is limited, at the option of RIVERSTONE, to either

      (a) RIVERSTONE's use of reasonable efforts to repair any item, or part thereof; or

      (b) RIVERSTONE's use of reasonable efforts to replace any item, or part thereof, or any shipment as to which any defect is claimed by PURCHASER and duly verified by RIVERSTONE; or

      (c) The refund of the purchase price.

DECLARATION OF CONFORMITY ADDENDUM

Application of Council Directive(s)	89/336/EEC 73/23/EEC
Manufacturer's Name **Manufacturer's Address**	Riverstone Networks, Inc. 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

LIST OF FIGURES

LIST OF TABLES

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 2100.

1.1 HOW TO USE THIS GUIDE

If You Want To...	See...
Get an overview of the RS 2100 software and hardware features and specifications	Chapter 2, *"RS 2100 Introduction"*
Install the RS 2100 hardware	Chapter 3, *"Hardware Installation"*
Install the RS 2100 software, boot the software, and set up the unit	Chapter 4, *"RS 2100 Initial Configuration"*
Upgrade system software	Chapter 5, *"Managing RS 2100 Software"*
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 2100	*Riverstone RS Switch Router User Guide*
The complete syntax for all Command Line Interface (CLI) commands	*Riverstone RS Switch Router Command Line Interface Reference Manual*
Console and SYSLOG messages	*Riverstone RS Switch Router Message Reference Manual*

2 RS 2100 INTRODUCTION

The Riverstone RS 2100 provides non-blocking, wire-speed Layer-2 (switching), Layer-3 (routing), and Layer-4 (application) switching. This chapter provides a basic overview of the RS 2100 software and hardware feature set.

> **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 2100 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. Here is an example of that model. The RS 2100 operates within the layers that are not shaded. Notice that layer 2 is divided into a MAC layer, an LLC layer, and an LLC2 layer. The RS 2100 operates at the MAC and LLC layers.

Table 2-1   ISO 7-layer model and RS 2100 capabilities

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

2.2   SPECIFICATIONS

The RS 2100 provides high-speed switching and full non-blocking throughput. The hardware provides high-speed performance regardless of the performance monitoring, filtering, and Quality of Service (QoS) features enabled by the software.

The following table lists the basic hardware and software specifications for the RS 2100.

Table 2-2   Basic hardware and software specifications

Feature	Specification
Throughput	• 8.0-Gbps non-blocking switching fabric • 9.2 million packets-per-second routing throughput
Capacity	• Up to 50,000 routes • Up to 256,000 Layer-4 application flows • Up to 240,000 Layer-2 MAC addresses • 4,096 Virtual LANs (VLANs) • 2,000 Layer-2 security and access-control filters • 3MB input/output buffering per gigabit port
Routing protocols	• IP: RIP v1/v2, OSPF, BGP v2/v3/v4, IS-IS • IPX: RIP, SAP • Multicast: IGMP, DVMRP, GARP/GVRP • Network Address Translation • Server Load Balancing • Transparent Web Caching
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	• 802.3z (1000Base-SX)
Quality of Service (QoS)	• Layer-2 prioritization (802.1p) • Layer-3 source-destination flows • Layer-4 source-destination flows • Layer-4 application flows
RMON	• RMON v1/v2 for each port
Management	• SNMP v1/v2 • Emacs-like Command Line Interface (CLI)
Port mirroring	• Traffic to specific gigabit ports

2.3   SOFTWARE OVERVIEW

This section describes the features and capabilities of the RS 2100 in greater detail. For full information regarding the use of these features and capabilities, see the *Riverstone RS Switch Router User Guide*.

2.3.1   Bridging

The RS 2100 provides the following types of wire-speed bridging:

Address-based bridging – The RS 2100 performs this type of bridging by looking up a packet's destination address in an 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 RS 2100's own MAC address, the packet is routed rather than bridged.

Flow-based bridging – The RS 2100 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 2100 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 to RMON I statistics.

The RS 2100 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 2100 supports the following types of Virtual LANs (VLANs):

Port-based VLANs – A port-based VLAN is a set of ports that comprises a layer-2 broadcast domain. The RS 2100 confines MAC-layer broadcasts to the ports in the VLAN on which the broadcast originates. RS 2100 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 2100 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 RS 2100 switches. To simplify VLAN administration, the RS 2100 supports 802.1Q trunk ports, which allow you to use a single port to "trunk" traffic from multiple VLANs to another RS 2100 or to a switch that supports 802.1Q.

2.3.3   Routing

The RS 2100 provides wire-speed routing for the following protocols:

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

IPX – protocol by Novell used in NetWare products

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

By default, the RS 2100 uses one MAC address for all interfaces. The RS 2100 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 2100 receives a packet whose destination MAC address is one of the RS 2100'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 CPU) to route the packet to its IP destination(s).

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 2100 supports the following IP unicast routing protocols:

- RIP v1 and RIP v2
- OSPF v2
- BGP 2,3,4
- 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 2100 supports the following IP multicast routing protocols:

- IGMP
- DVMRP
- GARP/GVRP

The RS 2100 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 2100 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 2100 when an IPX interface is created.

2.3.4 Layer-4 Switching

In addition to layer-2 bridging and layer-3 routing, the RS 2100 performs layer-4 switching. Layer-4 switching is based on applications and flows.

Layer-4 Applications – The RS 2100 understands the application for which an IP or IPX packet contains data and therefore enables you to manage and control traffic on an application basis. For IP traffic, the RS 2100 looks at the packet's TCP or UDP port number to determine the application. For IPX packets, the RS 2100 looks at the destination socket to determine the application.

Layer-4 Flows – The RS 2100 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 2100. 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 Lists (ACLs) filters. You can implement the following types of filters and ACLs to secure traffic on the RS 2100:

- 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 TACACS, TACACS+, RADIUS. and Secure Session Shells (SSH) version 1.5.

2.3.6 Quality of Service

Although the RS 2100 supplies non-blocking, wire-speed throughput, you can configure the RS 2100 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 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

QoS mechanisms supported on the RS 2100 include the following:

- Traffic control queuing
- Weighted random early detection
- Weighted fair queuing
- Strict priority queuing
- QoS traffic control queues
- ToS octet rewrites
- Multi-Protocol Label Switching (MPLS) and the creation of LSPs for traffic engineering

> **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 2100 can provide extensive statistical data on demand. You can access the following types of statistics:

Layer-2 RMON and 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 ICMP, IP, IP-interface, IP routing, IP multicast, VLAN

Layer-4 RMON v2 Statistics – Statistics for TCP and UDP

LFAP – Light-weight File Accounting Protocol

Open APIs – Slate and FAS Lite.

2.3.8   Web Hosting Features

The RS 2100 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.

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 2100 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, *"RS 2100 Initial Configuration."*

SNMP MIBs and traps – The RS 2100 supports SNMP v1/v2 and many standard networking MIBs. The RS 2100'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 2100 is described in Chapter 4, *"RS 2100 Initial Configuration."*

2.4   HARDWARE OVERVIEW

This section describes the RS 2100's hardware specifications. For information on installing the hardware, see Chapter 3, *"Hardware Installation."*

2.4.1   Chassis

The RS 2100 chassis contains eight gigabit Ethernet (1000Base-SX) ports. The RS 2100's configuration is fixed at eight gigabit ports. No expansion modules are available. Figure 2-1 shows the front view of an RS 2100 chassis.

Figure 2-1   Front view of an RS 2100 chassis

2.4.2   External Controls

The RS 2100 has the following external controls:

- Male DB-9 Data Communications Equipment (DCE) port for serial connection from a management terminal. Use this port to establish a direct CLI connection to the RS 2100. The default baud rate is 9600.

- 10/100Base-TX Data Terminal Equipment (DTE) port for in-band management. The port is configured as Media Data Interface (MDI). Use this port to establish a management connection to the RS 2100 over an Ethernet segment.

- Reset switch (RST). Use this switch to reboot the RS 2100 in the event of a system failure. The Reset switch is recessed in the RS 2100's chassis.

- Status LEDs, described in the following table:

Table 2-3   Status LEDs

LED Label	Description
OK	When this LED is on, the RS 2100 and all gigabit ports are functioning correctly.
ERR	When this LED is on, a fatal system error has occurred. Activate the RS 2100's boot PROM to reboot the router.
HBT	This LED flashes when the RS 2100's boot PROM is active.
DIAG	When this LED is on, the RS 2100 is in diagnostic mode. (While in diagnostic mode, several other LEDs on the RS 2100 are active, as well.)

2.4.3   Motherboard Features

The internal "motherboard" performs all the RS 2100's computing and routing functions. 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 gigabit ports is handled by the motherboard. After processing traffic, the motherboard updates the L2 and L3/L4 tables on the gigabit ports that received the traffic. The gigabit ports then take over all subsequent forwarding for the learned table entry.

Boot Flash

The motherboard has a boot flash containing the RS 2100's boot software and configuration files. The system software image file resides on an internal flash chip and can be upgraded from a TFTP or BootP/TFTP server.

RAM Memory

The RS 2100's motherboard uses 128 megabytes of RAM to hold routing and other tables. To upgrade the amount of memory on the RS 2100, contact your Riverstone representative.

Power Supplies

The RS 2100 uses two power supplies, each delivering 3.3, 5, and 12 volts DC to the motherboard, internal fans, and other components. Each power supply provides a portion of the power necessary to operate the RS 2100, with the added feature that, in the unlikely event that one of the power supplies should fail, the remaining power supply will assume the entire load and provide enough current to operate the RS 2100.

	Warning	Be sure to plug the RS 2100 into a single-phase grounded power source located within 6 feet of the installation site.

	Warning	Failure to provide adequate grounding for the AC power supply can result in critical injury and serious damage to the switch router and will invalidate your warranty.

The following table lists the specifications for the power supplies.

Table 2-4   Power supply voltage and current specifications

Input voltage	Input current (maximum)
100-125 VAC	2.6 A
200-240 VAC	1.3 A

2.4.4   Fans

The RS 2100 contains three internal fans to provide cooling air flow across the motherboard and gigabit ports. The fans are located near the middle of the chassis, between the power supplies and the motherboard.

	Warning	To ensure that the fans can provide adequate cooling, Riverstone recommends that you allow a minimum of 3 inches of clearance on each side of the chassis.

2.4.5   Gigabit Ports

The RS 2100's eight gigabit (1000Base-SX) Ethernet ports are indexed into four groups of two ports each. The ports can operate in either full-duplex or half-duplex mode. Each port can be configured as a switched port or a routed port. The ports have shortwave (850 nm) lasers and connect to multimode-mode fiber (MMF) cables.
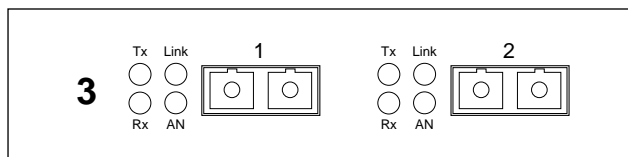
Figure 2-2 shows two of the gigabit ports.

Figure 2-2   Front panel of gigabit ports

Cabling and Connector Specifications

The following table lists the media specifications for the gigabit ports:

Table 2-5   Gigabit port specifications

Port type	Specification
1000Base-SX	• 802.3z standard (also uses 802.3x for flow control) • SC-style Media Interface Connector (MIC) • 62.5 micron or 50 micron multimode fiber-optic cable • Maximum 275 meters (902 feet) segment length for 62.5 micron fiber-optic cable, based on installed fiber bandwidth • Maximum 550 meters (1804 feet) segment length for 50 micron fiber-optic cable, based on installed fiber bandwidth

LEDs

The gigabit ports use the following LEDs.

Table 2-6   Gigabit port LEDs

LED	Description
Per-port Link	**Green** – Indicates that the port hardware detects a cable plugged into the port and a good link is established.
	Red (intermittent) – Indicates that the port 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 exists with the port.
Per-port Rx	**Green** – Indicates when the port's transceiver receives packets.
	Orange – Indicates when the port's transceiver receives flow-control packets.
Per-port Tx	**Green** – Indicates when the port's transceiver transmits packets.
	Orange – Indicates when the port's transceiver transmits flow-control packets.
Per-port AN	**Green** – Indicates that the gigabit port is autonegotiating the operating mode of the link between full-duplex and half-duplex.
	Orange (intermittent) – Indicates that autonegotiation is in process.
	Orange (solid) – Indicates a problem with autonegotiation configuration.
	Red – Indicates an autonegotiation failure. This fault may occur if the link partner does not support full duplex.
	Off – Indicates that autonegotiation has been disabled or the link is down.

3   HARDWARE INSTALLATION

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

3.1   SAFETY CONSIDERATIONS

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

3.1.1   Preventing Injury

Observe the following safety warnings to prevent accidental injury when working with the RS 2100 hardware:

- Be careful when lifting the RS 2100 out of the shipping box.
- Never attempt to rack mount the RS 2100 unaided. Ask an assistant to help you with the RS 2100.
- Before performing any mechanical upgrade or installation procedures, make sure that the RS 2100 is powered off.
- Never operate the RS 2100 if it becomes wet or the area where it has been installed is wet.

3.1.2   Preventing Equipment Damage

To prevent damage to the RS 2100 components, observe the following warnings.

	Warning	Always use proper electrostatic discharge (ESD) gear when handling line cards or other internal parts of the RS 2100.

	Warning	Make sure you allow at least three inches of room for air flow around the RS 2100 chassis.

3.2   HARDWARE SPECIFICATIONS

The following table lists the physical and environmental specifications for the RS 2100.

Table 3-1   RS 2100 physical and environmental specifications

Specification	Measurement
Dimensions	Inches: 2.8" (height) x 17" (width) x 18.5" (depth)
	Centimeters: 7.1cm x 43.2cm x 47cm
Weight	Pounds: 22
	Kilograms: 10
Power	100-125 VAC, 2.6 A maximum;
	200-240 VAC, 1.3 A maximum
Operating temperature	Fahrenheit: 41°F to 104°F
	Centigrade: 5°C to 40°C

3.2.1   Installing the Hardware

This section describes how to perform the following tasks:

- Verifying your shipment
- Installing the chassis
- Attaching console management cables

3.2.2   Verifying Your Shipment

Before you begin installing your RS 2100, check your shipment to ensure that everything you ordered arrived securely.

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

- RS 2100 switch router
- RS 2100 power cord(s)
- Console cable
- *Riverstone Networks RS 2100 Switch Router Getting Started Guide*
- *Riverstone Networks Documentation CD*
- Release Notes.
- Rack mount kit

3.2.3   Installing the Chassis

Install the RS 2100 in a standard 19" equipment rack.

	Warning	Before performing any mechanical upgrade or installation procedures, ensure that the RS 2100 is powered off.

	Warning	Never attempt to rack mount the RS 2100 unaided. Ask an assistant to help you hold the chassis.

To install the RS 2100 chassis in an equipment rack, use the following procedure. You need a #2 Phillips-head screwdriver to perform this procedure.

1. Remove the two screws that help hold the front panel of the RS 2100 on to the rest of the chassis. There is one screw located on each side of the chassis near the front of the RS 2100. These screws will be reused to hold the rack mounting brackets to the RS 2100.

2. Align one of the mounting brackets over the corresponding holes in the side of the RS 2100. The mounting bracket is correctly positioned when the mounting flange is flush with the front of the RS 2100.

3. Use the #2 Phillips-head screwdriver and the supplied Phillips-head screws to attach the mounting bracket to both the side and bottom of the chassis.

	Warning	Be sure to use the Phillips-head screws supplied by Riverstone. If you use screws that are longer than the ones included with your shipment, there is a danger of damaging the RS 2100's internal components.

4. Attach the other mounting bracket.

5. Along with an assistant, lift the RS 2100 into place in the mounting rack.

6. While your assistant holds the chassis in place, use the appropriate tool and mounting hardware to attach the mounting brackets to the equipment rack. Figure 3-1 shows an example of how to install the RS 2100 in the equipment rack.
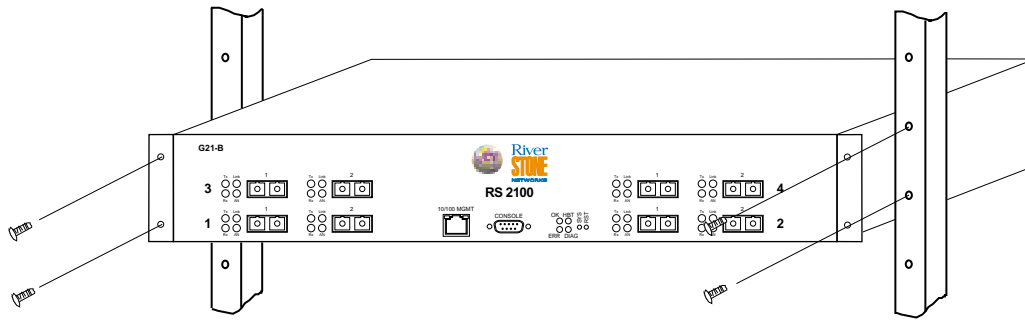
Figure 3-1   Installing the RS 2100 chassis in an equipment rack

---

![Warning icon] **Warning**   Make sure the screws are tight before your assistant releases the chassis. If you accidentally leave the screws loose, the chassis can slip and fall, possibly becoming damaged.

3.2.4   Attaching Cables to the Management Ports

The RS 2100 has two ports for attaching management devices:

Male DB-9 DCE port – This serial port is used for direct connection to a terminal or PC running terminal emulation software. Use this port to perform basic setup using the Command Line Interface (CLI).

RJ-45 10/100Base-T DTE port – This Media Data Interface (MDI) port is used for in-band management of the RS 2100 through a Telnet session to the CLI or through SNMP.

Connecting the Serial Management Cable

Use the serial cable to connect the RS 2100 to a terminal (or to a PC running terminal emulation software) to perform initial setup and configuration. The RS 2100's serial cable is a female to female DB-9 crossover cable. Figure 3-2 shows the serial port's pin-out. Table 3-2 maps the wiring of the serial cable
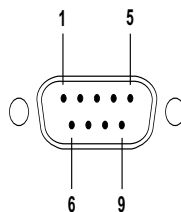
Figure 3-2   Serial port (DB-9 DCE) pin-out

Table 3-2   Wiring map for serial cable

Signal (RS 2100 serial port)	Pin	Signal (management console port)
Unused	1	Unused
TXD (transmit data)	2	RXD (receive data)[a]
RXD (receive data)	3	TXD (transmit data)
Unused	4	Unused
GND (ground)	5	GND (ground)
Unused	6	Unused
CTS (clear to send)	7	CTS (clear to send)
RTS (request to send)	8	RTS (request to send)
Unused	9	Unused

a. The left hand column pin assignments are for the male DB-9 connector on the RS 2100. Pin 2 (TXD or "transmit data") must emerge on the management console's end of the connection as RXD ("receive data").

Connecting a 10/100BASE-TX Management Cable

Use the RJ-45 10/100BASE-TX DTE port for connecting the RS 2100 to your network for in-band management through either Telnet or SNMP. Figure 3-3 shows the pin positions of the 10/100BASE-TX port, and Table 3-3 shows the wiring map for the MDI management cable:

87654321
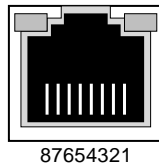
Figure 3-3   10/100BASE-TX RJ-45 port

Table 3-3   Wiring map for MDI management cable

Signal (RS 2100 port)	Pin	Signal (management console port)
TXD (transmit data)	1	RXD (receive data)[a]
TXD (transmit data)	2	RXD (receive data)
RXD (receive data)	3	TXD (transmit data)
Unused	4	Unused
Unused	5	Unused

Table 3-3   Wiring map for MDI management cable (Continued)

Signal (RS 2100 port)	Pin	Signal (management console port)
RXD (receive data)	6	TXD (transmit data)
Unused	7	Unused
Unused	8	Unused

a. The right hand column pin assignments are for the RJ-45 connector on the RS 2100. Pin 1 (TXD or "transmit data") must emerge on the management console's end of the connection as RXD ("receive data").

4   RS 2100 INITIAL CONFIGURATION

This chapter provides the following information on powering up the RS 2100 for the first time, and performing basic setup procedures. Basic setup include:

- Powering on the RS 2100 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 2100
- Configuring the SYSLOG server and server message levels

4.1   POWERING ON THE RS 2100

To power on the RS 2100 perform the following steps:

1. Make sure all exposed line card slots are free of foreign objects such as tools and are covered with blanks.

2. Make sure that the RS 2100's DB-9 console port is connected to an active terminal or a PC running terminal emulation software.

> **Note**   The RS 2100 does not have a power ON/OFF switch. The RS 2100 is turned on by plugging in its AC power cords and connecting them to the AC source

3. Plug the AC power cords into the RS 2100 chassis, then connect the RS 2100 to the AC power source.

    If this is the first time you have powered on the RS 2100, it boots automatically using the software image on the internal flash memory. While the software is booting, the amber Offline LED on the front of the RS 2100 is lit. When the software finishes booting, the Offline LED goes dark and the green Online LED lights up, indicating that the Rapid Operating System (ROS) software is online.

    In addition, as the software boots, the management terminal or PC attached to the RS 2100's DB-9 DCE port displays messages related to the phases of the boot sequence.

Here is a partial example:

```
Boot Software Version prom-2.0.0.5, Built Jan 5 2001 20:18:57

Processor: R5000 rev 2.1 [0x2321], 160 MHz, (bus: 80 MHz), 128 MB DRAM

I-Cache 32 KB, linesize 32. D-Cache 32 KB, linesize 32.

Mounting 16MB flash card . . . Done

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

using link: bootsource

link pointed at file:/pc-flash/boot/rs70/

source: file:/pc-flash/boot/rs70/

  Loaded version file

 Loading kernel (base 0x80001000, size 50592)

(base 0x8000d5a0, size 2658597)

  100% -  Image checksum validated

--------------------------------------------------------------------

RS 2100 System Software, Version 7.0.0.0

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

Built by mhaydt@diego on Mon Jan 5 17:10:42 2001

Processor: R5000, Rev 2.1, 159.99 MHz

System started on 2001-10-01 15:27:01

--------------------------------------------------------------------

2001-10-01 15:27:02 %SYS-I-FLASHCRD, Mounting 16MB Flash card

2001-10-01 15:27:06 %SYS-I-FLASHMNTD, 16MB Flash card mounted

2001-10-01 15:27:06 %SYS-I-INITSYS, initializing system RS 2100

2001-10-01 15:27:06 %SYS-I-DSCVMOD, discovered 'Control Module' module in slot CM

2001-10-01 15:27:11 %SYS-I-INITSLOTS, Initializing system slots - please wait

2001-10-01 15:27:18 %SYS-I-MODPROBE, Detecting installed media modules - please wait

2001-10-01 15:27:23 %SYS-I-INITPORT, initialized slot CM/1, port 1

2001-10-01 15:27:23 %SYS-I-INITPORT, initialized slot CM/1, port 2

2001-10-01 15:27:23 %SYS-I-INITPORT, initialized slot CM/1, port 3...
```

4. When the software is fully booted, the following messages appears on the management console:

```
Press RETURN to activate console...
```

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

Note If prompted for a password, simply press the Return key. The default passwords are blank.

Note If the message "**SYS-E-NOFLASHCARD**" appears while booting the RS 2100, the system has not detected its internal flash memory. If this occurs, reboot the system. If the system still does not recognize its memory, contact Riverstone Networks 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 2100"* 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 of which provides the ability to perform specific operations on the RS 2100 (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 system image is not found during bootup. Enter the **reboot** command to reset the RS 2100. If the RS still fails to boot, contact Riverstone Networks Technical Support.
	Certain tasks can be performed only from Boot mode. To enter the Boot mode intentionally, boot the RS 2100, and then interrupted 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 RS 2100 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. The following table lists some commonly used commands. For a complete set of commands, see the *Riverstone RS Switch Router Command Line Interface Reference Manual*.

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

The RS 2100 uses three special configuration files:

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 2100 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 2100 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 2100 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 RS 2100 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.

Note   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 2100 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 RS 2100'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 2100, but the RS 2100 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.

4.4   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 RS 2100)
- IP address for the management port on the RS 2100

> **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 RS 2100's management port.

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 RS 2100's management port.

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 2100 by setting up passwords for User mode access and Enable 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 2100 for TACACS, TACACS+, and/or RADIUS authentication by a TACACS or RADIUS server. Procedures for configuring the RS 2100 for TACACS and RADIUS can be found in the *Riverstone 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 <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)# 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 zcGzbO 5d1f73d2d478ceaa062a0b5e0168f46a
```

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 RS 2100 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 this procedure to regain access to your RS 2100.

Note   To perform this procedure, you must use a terminal or PC running terminal emulation software that is connected directly to the RS 2100 through its DB-9 console port.

---

1.   Power cycle the RS 2100.

2.   Interrupt the normal boot-cycle and enter Boot mode 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 = 62000
 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 = link:/pc-flash/boot/rs70 <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 2100:

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

Here is an example:

```
rs-boot> boot /pc-flash/boot/rs70 skipconfig=yes
```

5. When the RS 2100 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)# 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, 2001-10-02 21:53:54 %GATED-I-RECONFIGDONE, Routing
configuration changes completed (pid 0x809eab20).
configuration saved to Startup configuration.
rs(config)#
```

6. Both the User access mode and Enable access mode passwords are now reset to the default "blank" values.

7. Enter new passwords for both the User and Enable access modes.

4.6   SETTING UP SNMP

To use SNMP to manage the RS 2100, you need to set up an SNMP community and specifying the IP address of the target host for SNMP traps. Otherwise, the RS 2100's SNMP agent runs in local trap process mode, unless disabled using the `snmp stop` command.

For additional information about configuring and using SNMP, see the *Riverstone 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 2100, configure the RS with a static route to the target. If the RS 2100 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 RS 2100's en0 Ethernet port. If you want SNMP to use a different port on the RS 2100, 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 SNMP v1 or v2, it is important to protect your RS 2100 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 2100's SNMP agent, allowing access to the RS 2100 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 form any other source IP address are dropped.

Disabling Authentication Traps

To provide additional security to the RS 2100, 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 additional information about RS 2100 security and ACLs, see the *Riverstone RS Switch Router User Guide.*

4.6.3   Supported MIBs

The following lists the MIBs that are supported by the RS 2100 SNMP agent.

Table 4-4   RS 2100 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/RFUDP-MIB RFC 2012	SONET-MIB RFC 1595	BRIDGE-MIB RFC 1493	RIPv2-MIB RFC 1724		NOVELL-IPX 4/21/94
UDP-MIB RFC 2013	DS1-MIB RFC 2495	Q-BRIDGE-MIB RFC 2674	OSPF-MIB RFC 1850		CTRON-LFAP 8/28/99
IP-FORWARD-MIB IP-Group-IPCIDRTable MIB RFC 2096	DS3-MIB RFC 2496	P-BRIDGE-MIB RFC 2674			CTRON-SSR-POLICY 8/11/99
IF-MIB RFC 2233	DS0-MIB RFC 2494	PPP-LCP-MIB RFC 1471	RMON2-MIB RFC 2021		CTRON-SSR-CONFIG 8/17/99
SNMPv2-MIB RFC 1907	MAU MIB RFC 2668	PPP-SEC-MIB RFC 1472	VRRP-MIB Draft #9		CTRON-SSR-HARDWARE 8/14/99
	DOCS-IF-MIB RFC 2670	PPP-IP-NCP-MIB RFC 1473	DVMRP-MIB Draft #4		CTRON-SSR-SERVICE 8/4/98
	DOCS-BPI-MIB Draft #1	PPP-BRIDGE-NCP-MIB RFC 1474	IGMP-MIB Draft #5		CTRON-SSR-CAPACITY 5/13/99
	DOCS-CABLE-DEVICE-MIB Draft #8	RMON-MIB RFC 1757			RIVERSTONE-STP-MIB 7/11/00
		ATM-MIB RFC 1695			RIVERSTONE-RS-AGENTCAPMIB
		LAG MIB 8/17/00			RIVERSTONE-RS-CMTS-MIB 7/8/00

4.7   SETTING THE DNS DOMAIN NAME AND ADDRESS

Associating a DNS name server with your RS 2100 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 2100 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 2100 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 2100:

```
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 2100 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 2100 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 CPU 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-SAVED configuration saved to Startup configuration`

The RS 2100 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 2100 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 2100, 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.

5   MANAGING RS 2100 SOFTWARE

This chapter describes how to perform operations regarding RS 2100 operating software and bootPROM images software. The following topics are covered:

- Upgrading the system image software
- Upgrading the Boot PROM image software
- Loading RS 2100 software from a TFTP server
- Loading RS 2100 software from a BootP/TFTP server

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   : 7.0
  Copyright          : Copyright (c) 2000-2001 Riverstone Networks, Inc.
  Image Information  : rs7000, built on Mon Jan 25 14:10:21 2000
  Image Boot Location: file:/pc-flash/boot/img/rs7000
  Boot Prom Version  : prom-2.0.0.5
```

    In the example above, the location "**pc-flash**" indicates that the RS 2100 is set to use the factory-installed software on its internal flash memory.

2. Copy the upgrade system software onto a TFTP server that the RS 2100 can access. (Use the **ping** command to verify that the RS 2100 can reach the TFTP server.)

> **Note** If the TFTP server is one or more hops away from the RS 2100, 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 2100's internal flash memory:

```
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:

```
rs# system image add 134.152.178.5 tftpboot/rs7300
Downloading image 'tftpboot/rs7300' from host '134.152.178.5'
 to local image rs7300 (takes a while) . . .
 download: done
 save:
kernel: 100%
done
Image checksum validated.
%SYS-I-BOOTADDED, Image 'rs7300' added.
```

4. Enter the `system image list` command to list the images on the internal flash memory and verify
that the new image is present:

Here is an example:

```
rs# system image list
Images currently available on Master CM
slot0:
rs7300 (version 7.3.0.0)
rs7000 (version 7.0.0.0)  [selected for next boot]
```

5. Use the `system image choose` command to select the image file that the RS 2100 will use when
rebooted.

Here is an example:

```
rs# system image choose rs7300
Found image in slot0
Making image rs7300 (version 7.3.0.0) the active image
for next reboot on Master CM . . .
%SYS-I-CHS_PRIMARY_OK, image successfully chosen on Primary CM
rs#
```

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

> **Note** You do not need to activate this change.

7. Reboot the RS 2100 to load and run the new system software image.

5.2   UPGRADING BOOT PROM SOFTWARE

The RS 2100 boots using the boot PROM image software installed on the motherboard'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  : 7.0
  Copyright         : Copyright (c) 1996-2000 Riverstone Networks, Inc.
  Image Information : rs7000, built on Mon Jan 25 14:10:21 2000
  Image Boot Location: file:/pc-flash/boot/img/rs7000
  Boot Prom Version  : prom-2.0.0.5
```

2. Copy the upgrade boot PROM image software onto a TFTP server that the RS 2100 can access. (Use the **ping** command to verify that the RS 2100 can reach the TFTP server.)

> **Note** If the TFTP server is one or more hops away from the RS 2100, 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 2100'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-26
Downloading image 'tftpboot/prom-26' from host '134.152.178.5'
image is a prom upgrade to version 'prom-2.0.0.6'
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 2100.

5. Enter the **system show version** command to verify that the new boot PROM software is in the internal memory of the RS 2100's motherboard.

5.3   LOADING SOFTWARE FROM THE NETWORK

Typically, the RS 2100 loads its operating software from the flash memory contained on the motherboard. Alternately, the RS 2100 can be configured to ignore its internal flash image and obtain its software from a network server. The RS 2100 can obtain its image software from either a TFTP or BootP/TFTP server.

5.3.1   Loading Image Software from a TFTP Server

Perform the following procedure to configure the RS 2100 to load its image software from a TFTP server:

1. Copy the image software onto a TFTP server that the RS 2100 can access.

2. Reboot the RS 2100 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 bootPROM 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/ros70
  bootaddr = 0.0.0.0
   ethaddr = 00:00:1d:12:34:56
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/ros70**.

5. From the Boot prompt, use the **set** command to set the following:

*   IP address of the RS 2100 – (**netaddr**)

*   Subnet mask for the RS 2100 – (**netmask**)

*   The IP address of the RS 2100'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/ros70
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/ros70
  bootaddr = 134.152.176.5
   ethaddr = 00:00:1d:12:34:56
sysid = -1
rs-boot>
```

7. From the Boot prompt, use the **ping** command to verify that the RS 2100 can reach the TFTP server.

8. Reboot the RS 2100. As the RS 2100 initializes, it ignores the software image on the internal flash and retrieves its operating software from the TFTP server at **134.152.176.5**:

Here is an example:

```
rs-boot> boot

Rebooting. . .

. . .source: tftp://134.152.176.5/tftpboot/ros70

  Build location: host 'matrix' by 'adm'...

  Version: 7.0.0.0 . . .
```

5.3.2   Loading Image Software from a BootP/TFTP Server

The RS 2100 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 2100 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 2100 to use its BootP client to obtain its image software, perform the following procedure:

1. Load the RS 2100's image software on a BootP/TFTP server that can be reached by the RS 2100.

2. Boot the RS 2100 and enter Boot mode by interrupting the normal startup sequence by pressing the "Esc" key.

3. Use the **set** command to obtain the RS 2100's MAC address.

    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/ros70
  bootaddr = 0.0.0.0
   ethaddr = 00:00:1d:12:34:56     < MAC address >
sysid = -1
rs-boot>
```

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

    Here is an example:

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

5. Configure the BootP/TFTP server with the RS 2100's MAC address, an appropriate IP address, and the location of the RS 2100 software image file. Additionally, make sure that the ARP cache of the BootP/TFTP server is set correctly for the RS 2100.

6. Reboot the RS 2100 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\ROS70
Booting boot file C:\TFTPBOOT\ROS70.
source: tftp://134.141.179.134/C:\TFTPBOOT\ROS70
 File: version (703 bytes)
  Build location: host 'matrix' by 'adm'
  Version: 7.0.0.0
  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 . . .
```

APPENDIX A TROUBLESHOOTING

If you experience difficulty with the basic hardware or software setup procedures in this guide, check the following table to see whether the difficulty you are experiencing is described. If you find a description of the difficulty you are experiencing, try the resolution(s) recommended for the difficulty.

If the resolution does not remove the difficulty or the difficulty is not listed in this appendix, contact:

Riverstone Technical Assistance Center - RTAC

- Telephone: (408) 844-0010
- 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 2100 exhibits no activity (no LEDs are on, the fan module is not operating, and so on).	Make sure the RS 2100 is plugged into a power source and the power source is active.
The power supply is installed but is not operating.	Check the power cable and the circuit to which the RS 2100 is connected.
The fan is not active.	Check the power cable and the circuit to which the RS 2100 is connected.
No Gigabit Modules are active.	Check the power cable and the circuit to which the RS 2100 is connected.
An older software version continues to boot instead of the newer version on a TFTP server.	To configure the RS 2100 to boot using newer software, use the procedure in Section 5.1, *"Upgrading System Image Software."*
You are unable to access the configuration commands in the CLI.	From the CLI, type `enable` to access Enable mode, then type `configure` to access Configure mode.
Configuration changes do not seem to be taking effect.	To activate the changes, use the procedure in Section 4.3.1, *"Activating the Configuration Commands in the Scratchpad."*

Table A-1   Troubleshooting (Continued)

If you experience this difficulty	Try this remedy
Configuration changes are not reinstated after a reboot.	To save the configuration changes to the Startup configuration file, use the procedure in Section 4.3.2, *"Saving the Active Configuration to the Startup Configuration File."*
The RS 2100 is not resolving DNS names.	To set up DNS, use the procedure in Section 4.7, *"Setting the DNS Domain Name and Address."* 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 2100.	To set up an SNMP community string and specify a target for SNMP traps, use the procedure in Section 4.6, *"Setting Up SNMP."* If you have already performed this procedure, type `snmp show all` in the CLI to check the SNMP settings. Use the `traceroute` and `ping` commands to verify that the RS 2100 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 Networks RS Switch Router User Guide* for information.

INDEX

V

W

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com