Juniper Networks®
Steel-Belted Radius® Carrier

Installation Guide

Release 7.0

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
http://www.juniper.net

Part Number: 530-025135-01, Revision 02

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Ulticom, Signalware, Programmable Network, Ultimate Call Control, and Nexworx are registered trademarks of Ulticom, Inc. Kineto and the Kineto Logo are registered trademarks of Kineto Wireless, Inc. Software Advancing Communications and SignalCare are trademarks and service marks of Ulticom, Inc. CORBA (Common Object Request Broker Architecture) is a registered trademark of the Object Management Group (OMG). Raima, Raima Database Manager and Raima Object Manager are trademarks of Birdstep Technology. Sun, Sun Microsystems, the Sun logo, Java, Solaris, and all trademarks and logos that contain Sun, Solaris, or Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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

Products made or sold by Juniper Networks (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS, JUNOSe, and SDX-300 software) or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Portions of this software copyright 1999-2004 Apasphere Ltd. This product includes omniOrb CORBA software from Apasphere Ltd, under the LGPL license: The libraries in omniORB are released under the LGPL license.

Portions of this software copyright 2003, 2004, 2005, 2006 Lev Walkin <vlm@lionet.info> All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

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

Portions of this software copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California All Rights Reserved Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this software copyright © 2001-2002, Networks Associates Technology, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

Portions of this software are copyright © 2001-2002, Cambridge Broadband Ltd. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

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

Portions of this software copyright © 1995-2002 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

This notice may not be removed or altered from any source distribution.

HTTPClient package Copyright © 1996-2001 Ronald Tschalär (ronald@innovation.ch).

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. For a copy of the GNU Lesser General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Copyright (c) 2000 - 2008 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright © 2008, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Steel-Belted Radius Carrier Installation Guide, Release 7.0
Writing: Art Campbell
Editing: Ben Mann
Illustration: Nathaniel Woodward

Revision History
17 September 2008—Revision 02

The information in this document is current as of the date listed in the revision history.

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT (“AGREEMENT”) BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. **The Software.** In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

   a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

   b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

   c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

   d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

   e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

   The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes;

completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information**. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

About This Guide xi

Objective xi
Audience xi
Documentation Conventions xii
Related Documentation xiii
Requests for Comments (RFCs) xiv
3GPP Technical Specifications xv
WiMAX Technical Specifications xv
Third-Party Products xv
Obtaining Documentation xv
Documentation Feedback xvi
Requesting Technical Support xvi
Self-Help Online Tools and Resources xvi
Opening a Case with JTAC xvii

Part 1 Steel-Belted Radius Carrier Installation

Chapter 1 Steel-Belted Radius Carrier Installation Overview

Migrating from Earlier SBR Releases 3
Supporting SIM, WiMAX, or SS7 with Steel-Belted Radius Carrier 4
Installation Workflow 4
Installation Checklists 5
New Release 7.0 Installation 5
Before You Begin 5
Installing SBR Software 7
Basic Configuration 7
SIM Server 5.4 Migration Checklist 8
Before You Begin 8
Installing Steel-Belted Radius Carrier Software 11
Basic Configuration 12
Release 6.x Migration Checklist 13
Before You Begin 13
Installing SBR Software 16
Basic Configuration 16

Chapter 2 Before You Begin

Reviewing the Release Notes 19
Determining the Server Role 20
Selecting an Appropriate Server 20

Meeting System Requirements 21
Hardware 21
Recommended Configuration 21
Minimum Configuration 21
Software 21
Perl 23
Backing Up SIM Server 5.4 or 6.x Release Files 23
Setting Up External Database Connectivity 24
Installing Signalware and SS7 Interfaces 24
Setting Up RSA Authorization Client 24
Verifying Network Requirements 25
Verifying Network Connectivity 25
Verifying Host Name Resolution 25
Verifying Root Access 25
Obtaining a License Key 26

Chapter 3 Installing SBR Software

Unpacking the Steel-Belted Radius Carrier Software 29
Package Management Commands 29
Shutting Down SNMP 31
Running the Steel-Belted Radius Carrier **configure** Script 32
Historic Files 37

Chapter 4 Basic Configuration

Steel-Belted Radius Carrier Server Commands 39
Starting the RADIUS Server 39
Stopping the RADIUS Server 39
Displaying RADIUS Status Information 40
Running SBR Administrator 40
Configuring the Server 42
Configuring SNMP 43
Migrating Files from Earlier Releases 44
Manual Migration of XML Configurations 44
Manual Migration of JRE Extensions 44
Manual Migration of JavaScript files 45
Manual Migration of ROOT Certificates 45
Manual Migration of Dictionaries 45
Manual Migration of Third-Party Plug-ins and Other Binaries 45

Chapter 5 Removing Steel-Belted Radius Carrier Software

Uninstalling the Steel-Belted Radius Carrier Server 47
Uninstalling the SBR Administrator Files 49

Part 2 Signalware 9 Support for Steel-Belted Radius Carrier

Chapter 6 Installing Signalware 9

Beginning the Installation 53
Developing and Deploying SS7 Services 55
Configuring the Platform 60
Commission Instance 62
Configuring Nodes 62
Installing Signalware Service Pack 5T 65
Installing the Patch Package 65

Chapter 7 Configuring SS7/IP Network Communication Files

Configuring Communication Files Overview 71
Communication Pathways and Corresponding Files 72
Configuration Activities 73
Signalware MML Commands 73
Defining Links, Link Sets, and Route Sets 74
Example MML Commands 74
SS7 Example: Creating Links, Link Sets, and Route Sets 76
SIGTRAN Example: Creating Links, Link Sets, and Route Sets 76
Configuring the authGateway Application for HLR Communication 76
Configuring the authGateway Routing Location Information 76
Example 1 — Global Title Routing Using Global Title Identification .. 77
Example 2 — PCSSN Routing Using Point Code Identification 77
Configuring the authGateway.conf File 77
Remote Routing Options 78
Authorization Options 79
Example 1 — authGateway.conf file 80
Example 2 — authGateway.conf file 80
Configuring the authGateway Startup Information 80
Example—Creating and Starting the authGateway Process 82
Configuring the ulcmmg.conf File 82
Example 82
Loading the MML Configuration Settings 83
Example 83
SS7 Sample Configuration Files 83
Basic Provisioning MML File with One Point Code/ Two SS7 Links 83
Routing Based on PC/SSN 84
Redundant SS7 Links Backing Up Each Other (Two Point Codes) 85
Sample authGateway Commands and Files 85
AS4StartMapGw.mml — One Point Code/ Two SS7 Links 85
AS4StartMapGw.mml — Routing Based on PC/SSN 85
authGateway.conf (Gateway routing configuration file) 86
ulcmmg.conf 87

About This Guide

This preface provides guidelines for using the *Steel-Belted Radius Carrier Installation Guide*:

- Objective on page xi
- Audience on page xi
- Documentation Conventions on page xii
- Related Documentation on page xiii
- Obtaining Documentation on page xv
- Documentation Feedback on page xvi
- Requesting Technical Support on page xvi

Objective

The *Steel-Belted Radius Carrier Installation Guide* describes how to install the Steel-Belted Radius Carrier software on a server running the Solaris operating system and how to install the SBR Administrator application.

It includes instructions for migrating configurations from servers running a limited number of earlier SBR releases.

It stops at a point where the server is installed and is fully functional, but it intentionally does not address all unique site configuration possibilities. For site-specific customizing, see the *Steel-Belted Radius Carrier Administration and Configuration Guide*.

Audience

This guide is intended for wireline and wireless carrier customers who are deploying converged services or implementing emerging wireless technologies such as WiMAX. Network administrators responsible for implementing and maintaining authentication, authorization, and accounting (AAA) services can use this guide to set up their Steel-Belted Radius Carrier servers.

This guide assumes that you are familiar with general RADIUS and networking concepts, as well as the specific environment in which you are installing Steel-Belted Radius Carrier.

If you use Steel-Belted Radius Carrier with third-party products such as Oracle or RSA SecurID, this guide assumes you are familiar with the installation, configuration, and use of those products.

Documentation Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

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

Table 2 describes the text conventions used throughout this manual.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Text Conventions		
Bold text like this	Represents commands and keywords in text.	■ Issue the **clock source** command. ■ Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	host1(config)#**traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	`host1#show ip ospf 2`
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	■ Emphasizes words. ■ Identifies variables. ■ Identifies chapter, appendix, and book names.	■ There are two levels of access, *user* and *privileged*. ■ *clusterId*, *ipAddress*. ■ *Appendix A*, *System Specifications*.
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
radiusdir	Represents the directory into which Steel-Belted Radius Carrier has been installed. The default location is `/opt/JNPRsbr/radius` on Solaris systems, but any location may be specified during installation.	Change directories to `/radiusdir`
Syntax Conventions		
Plain text like this	Represents keywords.	terminal length

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Italic text like this	Represents variables.	*mask*, *accessListName*
< > (angle brackets)	Enclose a list of possible selections.	<add | replace>
| (pipe symbol)	Represents a choice to select one keyword or variable in a list of choices that is separated by the pipe symbol.	diagnostic | line In this example, you must specify *add* or *replace* but cannot specify both: <add | replace> = Attribute [,Attribute]
[ ] (brackets)	Represent optional keywords or variables.	[internal | external], or < add | replace > = Attribute [,Attribute], where the second attribute is identified as optional by the brackets. When they are used in a configuration files brackets identify a section of the file. In scripts or in operating system commands, brackets indicate the default response or entry.
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Related Documentation

Table 3 lists and describes the Steel-Belted Radius Carrier documentation set:

Table 3: Steel-Belted Radius Carrier Documentation

Document	Description
Steel-Belted Radius Carrier Installation Guide	Describes how to install the Steel-Belted Radius Carrier software on the server and the SBR Administrator application on a client workstation. Posted at http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-install.pdf
Steel-Belted Radius Carrier Administration and Configuration Guide	Describes how to configure and operate the Steel-Belted Radius Carrier and its separately licensed modules. Posted at http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-admin.pdf
Steel-Belted Radius Carrier Reference Guide	Describes the settings and valid values of the Steel-Belted Radius Carrier configuration files. Posted at http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-reference.pdf
Steel-Belted Radius Carrier Release Notes	Contains the latest information about features, changes, known problems, and resolved problems. Posted at http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-rn700.pdf

NOTE: If the information in the Release Notes differs from the information in any guide, follow the Release Notes.

Requests for Comments (RFCs)

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFC)s online at http://www.ietf.org/rfc.html. Table 4 lists the RFCs that apply to Steel-Belted Radius Carrier.

Table 4: RFCs Related to Steel-Belted Radius Carrier

RFC Number	Title
RFC 1035	*Domain Names - Implementation and Specification*. P. Mockapetris. November 1987.
RFC 1155	*Structure and Identification of Management Information for TCP/IP-based Internets*. M. Rose, K. McCloghrie, May 1990.
RFC 1213	*Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. K. McCloghrie, M. Rose, March 1991.
RFC 2006	*The Definitions of Managed Objects for IP Mobility Support using SMIv2*. D. Cong and others. October 1996.
RFC 2246	*The TLS Protocol*. T. Dierks, C. Allen. January 1999.
RFC 2271	*An Architecture for Describing SNMP Management Frameworks*. D. Harrington, R. Presuhn, B. Wijnen, January 1998.
RFC 2284	*PPP Extensible Authentication Protocol (EAP)*. L. Blunk, J. Volbrecht, March 1998.
RFC 2433	*Microsoft PPP CHAP Extensions*. G. Zorn, S. Cobb, October 1998.
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*. G. Zorn. March 1999.
RFC 2607	*Proxy Chaining and Policy Implementation in Roaming*. B. Aboba, J. Vollbrecht, June 1999.
RFC 2618	*RADIUS Authentication Client MIB*. B. Aboba, G. Zorn. June 1999.
RFC 2619	*RADIUS Authentication Server MIB*. G. Zorn, B. Aboba. June 1999.
RFC 2620	*RADIUS Accounting Client MIB*. B. Aboba, G. Zorn. June 1999.
RFC 2621	*RADIUS Accounting Server MIB*. G. Zorn, B. Aboba. June 1999.
RFC 2622	*PPP EAP TLS Authentication Protocol*. B. Aboba, D. Simon, October 1999.
RFC 2809	*Implementation of L2TP Compulsory Tunneling via RADIUS*. B. Aboba, G. Zorn. April 2000.
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*. C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
RFC 2866	*RADIUS Accounting*. C. Rigney. June 2000.
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*. G. Zorn, B. Aboba, D. Mitton. June 2000.
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*. G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret. June 2000.
RFC 2869	*RADIUS Extensions*. C. Rigney, W. Willats, P. Calhoun. June 2000.
RFC 2882	*Network Access Servers Requirements: Extended RADIUS Practices*. D. Mitton. July 2000.
RFC 3046	*DHCP Relay Agent Information Option*. M. Patrick. January 2001.
RFC 3118	*Authentication for DHCP Messages*. R.Droms and others. June 2001.
RFC 3162	*RADIUS and IPv6*. B. Aboba, G. Zorn, D. Mitton. August 2001.
RFC 3344	*IP Mobility Support for IPv4*. C. Perkins. August 2002.
RFC 3539	*Authentication, Authorization, and Accounting (AAA) Transport Profile*. B. Aboba, J. Wood. June 2003.

Table 4: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
RFC 3575	*IANA Considerations for RADIUS (Remote Authentication Dial-In User Service)*. B. Aboba, July 2003.
RFC 3579	*RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*. B. Aboba, P. Calhoun, September 2003.
RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*. P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.
RFC 3748	*Extensible Authentication Protocol*. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz. June 2004.
RFC 3957	*Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4*. C. Perkins and P. Calhoun. March 2005.
RFC 4017	*Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*. D. Stanley and others. March 2005.
RFC 4186	*Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*. H. Haverinen, J. Salowey. January 2006.
RFC 4187	*Extensible Authentication Protocol Method for Global System for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. J. Arkko, H. Haverinen. January 2006.
RFC 4282	*The Network Access Identifier*. B. Aboba and others. December 2005.
RFC 4284	*Identity Selection Hints for the Extensible Authentication Protocol (EAP)*. F. Adrangi, V. Lortz, F. Bari, P. Eronen. January 2006.
RFC 4372	*Chargeable User Identity*. F. Adrangi and others. January 2006.
RFC 4510	*Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map*. K. Zeilenga, June 2006.

3GPP Technical Specifications

The 3rd Generation Partnership Project (3GPP) and (3GPP2) maintains an online repository of Technical Specifications and Technical Reports online at http://www.3gpp.org and http://www.3gpp2.org, respectively.

WiMAX Technical Specifications

The WiMAX Forum Networking Group (NWG) maintains a repository of technical documents and specifications online at http://www.wimaxforum.org. You can also view the WiMAX IEEE standards, 802.16e-2005 for mobile WiMAX and 802.16-2004 for fixed WiMAX, online at http://www.ieee.org.

Third-Party Products

For more information about configuring your access servers and firewalls, consult the manufacturer's documentation provided with each device.

Obtaining Documentation

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

Documentation Feedback

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

- Document name
- Document part number
- Page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- **JTAC Policies**—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/customers/support/downloads/710059.pdf
- **Product Warranties**—For product warranty information, visit http://www.juniper.net/support/warranty/
- **JTAC Hours of Operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings:
  http://www.juniper.net/customers/support/
- Search for known bugs:
  http://www2.juniper.net/kb/
- Find product documentation:
  http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base:
  http://kb.juniper.net/
- Download the latest versions of software and review release notes:
  http://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Manager: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at http://www.juniper.net/cm/
- Call 1-888-314-JTAC (1-888-314-5822 – toll free in the USA, Canada, and Mexico)

For international or direct-dial options in countries without toll-free numbers, visit http://www.juniper.net/support/requesting-support.html

When you are running SBR Administrator, you can choose **Web >** Steel-Belted Radius Carrier **User Page** to access a special home page for Steel-Belted Radius Carrier users.

When you contact technical support, be ready to provide:

- Your Steel-Belted Radius Carrier release number (for example, Steel-Belted Radius Carrier Release 7.x).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- A detailed description of the problem.
- Any documentation that may help in resolving the problem, such as error messages, memory dumps, compiler listings, and error logs.

Part 1
Steel-Belted Radius Carrier Installation

This part contains chapters that describe the installation and migration process for Steel-Belted Radius Carrier.

These chapters are included in this part:

- *Chapter 1, Steel-Belted Radius Carrier Installation Overview*
- *Chapter 2, Before You Begin*
- *Chapter 3, Installing SBR Software*
- *Chapter 4, Basic Configuration*
- *Chapter 5, Removing Steel-Belted Radius Carrier Software*

Chapter 1

Steel-Belted Radius Carrier Installation Overview

This chapter is an overview of the installation process for Steel-Belted Radius Carrier. The chapter also includes checklists that you can use to keep track of the tasks while you go through the installation process.

This chapter includes these topics:

- Migrating from Earlier SBR Releases on page 3
- Supporting SIM, WiMAX, or SS7 with Steel-Belted Radius Carrier on page 4
- Installation Workflow on page 4
- Installation Checklists on page 5

Migrating from Earlier SBR Releases

If you are an existing SIM Server 5.4 or SBR 6.0 or 6.1 Solaris platform customer, you can migrate the SBR database and some settings (stored in configuration and XML files) into a new Release 7.0 server as you install the Steel-Belted Radius Carrier software. The type of server — standalone, primary, or replica — must also be the same on both the old and new platforms.

Some files from previous releases can be moved from the old platform into the new Release 7.0 environment by the configuration script when Steel-Belted Radius Carrier is installed. Other files require manual editing to move existing settings into the corresponding Release 7.0 files without disabling new features. Automatically copying all old configuration files directly into the new environment — upgrading — would disable new features and improved modules in Release 7.0. So the method of moving from earlier versions to the current release is called migration.

NOTE: Migration is only supported between like operating systems — one Sun or Solaris server to a second and from the same type of server (stand-alone, primary, or replica) to the same type of server. Cross-OS and cross-type migration is not possible.

5.4 If you are migrating from an earlier release, as you use this guide, look for small margin headlines and related text, such as the “5.4” label to the left of this paragraph, or the “SIM” label on the next line.

SIM The text that accompanies these notes contains release-specific (SIM Server 5.4, 6.0, or 6.1) migration information or topic-specific (SIM, WiMAX, SS7, SQL) information. If text is labeled with a margin headline, it is required for that environment.

Supporting SIM, WiMAX, or SS7 with Steel-Belted Radius Carrier

Steel-Belted Radius Carrier support for SIM and WiMAX depends on Signalware 9 with Service Pack 5T software being properly installed on the Solaris server. If the SBR Carrier server communicates with an SS7 device, both Signalware 9 with Service Pack 5T and a supported Ulticom SS7 communications interface board must be present on the Solaris server.

Also, if EAP-SIM or EAP-AKA authentications are used, Signalware 9 with Service Pack 5T is required.

NOTE: We strongly recommend that Signalware software and the SS7 interface board, if one is used, be installed and configured before Steel-Belted Radius Carrier is installed.

The Ulticom installation documentation is delivered with the Signalware 9 and hardware packages. For your reference, there are two chapters in Part 2, Signalware 9 Support for Steel-Belted Radius Carrier on page 51, that show an example Signalware installation with the correct settings for simple integration with Steel-Belted Radius Carrier and the details of Signalware 9 configuration files.

Installation Workflow

The installation workflow follows a list of tasks that must be performed to make the Steel-Belted Radius Carrier server fully functional. This guide is organized the same way, presenting groups of related tasks in the order in which they should be performed.

The high-level view of the installation has three groups of tasks:

1. Before You Begin — The tasks to complete and the information to gather before the Steel-Belted Radius Carrier software can be installed. These topics are discussed in detail in *Chapter 2, Before You Begin*.

2. Software installation — Unpacking the software package, selecting installation options, and providing settings that are used to set up the server. These topics are discussed in detail in *Chapter 3, Installing SBR Software*.

3. Basic configuration — Starting and stopping the server daemon, setting up SNMP, and editing configuration files to include information from earlier releases. These topics are discussed in detail in *Chapter 4, Basic Configuration*.

Installation Checklists

This section includes installation checklists for different types of installations:

- New Release 7.0 Installation on page 5. This checklist records the steps for a new installation. It includes all possible options. If your install uses fewer options, some steps may be omitted.
- SIM Server 5.4 Migration Checklist on page 8. This checklist calls out steps for existing SIM Server migration to the Release 7.0 platform.
- Release 6.x Migration Checklist on page 13. This checklist calls out steps for existing Release 6.0 and 6.1 migration to the Release 7.0 platform.

New Release 7.0 Installation

This set of procedures installs a new, unconfigured Steel-Belted Radius Carrier Release 7.0 build on a Solaris 10 platform. It includes all possible options that can be included in the Steel-Belted Radius Carrier installation.

Before You Begin

Before you begin to install the Steel-Belted Radius Carrier software, perform these preliminary tasks or verify that they have been accomplished:

1. Review the Steel-Belted Radius Carrier *Release Notes* for up-to-date information that became available after the Steel-Belted Radius Carrier guides were published.

   Download the most recent Release Notes file from:
   http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-rn700.pdf

   If the information in the *Release Notes* differs from the information in any Steel-Belted Radius Carrier guide, follow the *Release Notes.*

2. Ensure that the server chassis is physically secure.

   To review recommendations on the server's characteristics, see Selecting an Appropriate Server on page 20.

3. Confirm that the server chassis provides at least the minimum hardware and software requirements.

   See Meeting System Requirements on page 21.

4. Verify root access.

5. Verify that the server meets basic network requirements:

   - See Verifying Network Connectivity on page 25
   - See Verifying Host Name Resolution on page 25

6. Verify the server role in the authentication environment. The installation script can configure a Steel-Belted Radius Carrier server as:

   - A stand-alone server.
   - The primary server in a group made up of replication servers.
   - A replication server.
     In an environment that uses replication servers, the primary server must be configured first to provide a base for replication.

LDAP

7. (Optional) If the server will interact with a Lightweight Directory Access Protocol (LDAP) directory service agent, verify or record the path to the LDAP library files (The default path is /usr/lib.)

SQL

8. (Optional) If the Steel-Belted Radius Carrier server will use an external database, you need to:

   - Verify database compatibility and interoperability.

     See Setting Up External Database Connectivity on page 24.

ORACLE

   - If the external database is Oracle, the Steel-Belted Radius Carrier server must be configured as a client of the Oracle server.

     As you set up the client, collect this information, or if the client is already installed, record this information to use while installing SBR software:

     - Record the path to the local Oracle Home directory (for example: **/opt/10g/app/oracle/product/10.2.0.3**).
     - Record the path to the local Oracle shared library (for example: **/opt/10g/app/oracle/product/10.2.0.3/lib32**)
     - Record the path to the local TNS_ADMIN (for example: **/opt/10g/app/oracle/product/10.2.0.3/network/admin**)

SS7

9. (Optional) Install a compatible SS7 interface board.

   See Installing Signalware and SS7 Interfaces on page 24 for a list of supported boards, and the documentation that comes with the board for installation instructions.

SIM / WiMAX / SS7

10. (Optional) Install and configure Signalware 9 with Service Pack 5T software, following the product documentation.

    - See *Chapter 6, Installing Signalware 9,* to see an example of a Signalware 9 installation.
    - See *Chapter 7, Configuring SS7/IP Network Communication Files*, for information on editing Signalware configuration files.

RSA

11. (Optional) If the Steel-Belted Radius Carrier server will interact with an RSA authorization server, the Steel-Belted Radius Carrier server must be set up as an RSA client. Follow the RSA product documentation for the procedure.

The Steel-Belted Radius Carrier server should receive a copy of several files from the RSA server. See Setting Up RSA Authorization Client on page 24 for Steel-Belted Radius Carrier requirements and the list of required files.

12. Verify that Steel-Belted Radius Carrier license keys have been assigned by logging in to your Juniper Networks support account.

    If you do not have a key, you can go ahead with the installation, but a 30-day trial license with a low maximum session limit is automatically installed.

Installing SBR Software

If all items on the "Before You Begin" list have been checked off, you are ready to install the SBR software. These are the key steps:

1. Unpack the Steel-Belted Radius Carrier Software.

   See Unpacking the Steel-Belted Radius Carrier Software on page 29.

   If you are not familiar with UNIX package management commands, you can review a list of Package Management Commands on page 29.

2. Check for running SNMP processes on the server and shut down any that are active.

   See Shutting Down SNMP on page 31.

3. Run the Steel-Belted Radius Carrier configure script. As the script runs, enter the information you recorded on the previous pages.

   See Running the Steel-Belted Radius Carrier configure Script on page 32.

Basic Configuration

After the Steel-Belted Radius Carrier software is on the Solaris server, you can ensure that the base software runs properly and then perform basic configuration steps:

1. Start the Steel-Belted Radius Carrier daemon.

   If you usually do not start and stop the daemon from the command line, the basic commands follow, and you can review Steel-Belted Radius Carrier Server Commands on page 39:

   - Start the RADIUS Server:
     */radiusdir/***sbrd start**
     or restart: */radiusdir/***sbrd restart**

   - Stop the RADIUS Server:
     */radiusdir/***sbrd stop**

   - Display RADIUS Status Information:
     */radiusdir/***sbrd status**

2. Start SBR Administrator.

Use an HTML browser to address the Steel-Belted Radius Carrier server HTML server. The default page should let you download the Administrator client application and log in as root. You should also confirm that the links to the documentation work.

Verify that you can download and run the application both from the local host and from a workstation on the network.

3. Configuring the environment. This step includes basic, low-level configuration tasks, such as:

   - Configuring communications between any additional devices and the Steel-Belted Radius Carrier server.

   - Adding additional users to the server.

   For additional information, see Configuring the Server on page 42.

4. SNMP configuration. If you elected to configure the Steel-Belted Radius Carrier SNMP agent during software installation and other agents also run on the server (such as the Solaris operating system agent), you will need to adjust the ports the agents use so multiple agents do not contend for the same resource.

   See Configuring SNMP on page 43.

SIM Server 5.4 Migration Checklist

This checklist lists the recommended steps to migrate an existing SIM Server 5.4 installation to the Release 7.0 platform.

We recommend that the SIM Server 5.4 environment be duplicated so far as possible. For instance, if SIM Server 5.4 uses a specific LDAP server or Oracle database, those should be set up so that the new Release 7.0 installation can access them using the older server's configuration information.

Before You Begin

Before you begin to install the Steel-Belted Radius Carrier software, perform these preliminary tasks or verify that they have been accomplished:

1. Review the Steel-Belted Radius Carrier *Release Notes* for up-to-date information that became available after the Steel-Belted Radius Carrier guides were published.

   Download the most recent Release Notes from:
   http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-rn700.pdf

   If the information in the *Release Notes* differs from the information in any Steel-Belted Radius Carrier guide, follow the *Release Notes.*

2. Create a copy of the SIM Server 5.4 SBR installation on the system that will host Release 7.0.

The recommended method is:

a. As root on the SIM Server 5.4, shut down the SBR daemon.
Execute: */radiusdir/***sbrd stop**.

b. Create a gzip archive of the SIM Server 5.4 *radiusdir* directory, preserving the file structure.

Change directories to */opt/JNPRsbr/* and execute:
tar cfE - radius |gzip > 5_4radius.tgz

c. As root on the Release 7.0 host, create a working directory for the archive:

Execute:
mkdir -p /opt/JNPRsbr/5_4backup

and:

cd /opt/JNPRsbr/5_4backup

d. Use ftp to copy the archive file to the Release 7.0 host.

e. Ungzip the archive in the working directory. This will not create a working installation, just serve as a source of files that can be reused by the Release 7.0 server.

Execute:
gunzip -dc 5_4radius.tgz |tar xf -

f. Check the file permissions on the unzipped archive to ensure that the files are writable.

See "Backing Up SIM Server 5.4 or 6.x Release Files" on page 23 for more information.

3. Ensure that the Release 7.0 server chassis is physically secure.

   To review recommendations on the server's characteristics, see Selecting an Appropriate Server on page 20.

4. Confirm that the Release 7.0 server chassis provides at least the minimum hardware and software requirements.

   See Meeting System Requirements on page 21.

5. Verify root access on the Release 7.0 server.

6. Verify that the Release 7.0 server meets basic network connectivity and DNS requirements:

   - See Verifying Network Connectivity on page 25
   - See Verifying Host Name Resolution on page 25

7. Verify that the Release 7.0 server role in the authentication environment is the same type that the SIM Server 5.4 server was in order to migrate files. The installation script can configure a Steel-Belted Radius Carrier server as:

   - A stand-alone server.
   - The primary server in a group made up of replication servers.
   - A replication server.
     In an environment that uses replication servers, the primary server must be configured first to provide a base for replication.

LDAP

8. (Optional) If the Release 7.0 server will interact with a Lightweight Directory Access Protocol (LDAP) directory service agent, verify or record the path to the LDAP library files (The default path is /usr/lib.)

SQL

9. (Optional) If the Steel-Belted Radius Carrier server will use an external database:

   - Verify database compatibility and interoperability.

     See Setting Up External Database Connectivity on page 24.

ORACLE / SIM / WiMAX

   - If the external database is Oracle, the Steel-Belted Radius Carrier server must be configured as a client of the Oracle server.

     As you set up the client, collect this information, or if the client is already installed, record this information to use while installing SBR Carrier software:

     - Record the path to the local Oracle Home directory (for example: **/opt/10g/app/oracle/product/10.2.0.3**)
     - Record the path to the local Oracle shared library (for example: **/opt/10g/app/oracle/product/10.2.0.3/lib32**)
     - Record the path to the local TNS_ADMIN (for example: **/opt/10g/app/oracle/product/10.2.0.3/network/admin**)

SS7

10. Install a compatible SS7 interface board.

    See Installing Signalware and SS7 Interfaces on page 24 for a list of supported boards, and refer to the documentation that comes with the board for installation instructions.

SIM / WiMAX / SS7

11. Install and configure Signalware 9 with Service Pack 5T software, following the product documentation.

    - See *Chapter 6, Installing Signalware 9,* for an example of a Signalware 9 installation.
    - See *Chapter 7, Configuring SS7/IP Network Communication Files*, for information on editing Signalware configuration files.

NOTE: The SIM Server 5.4 SBR files that reference Signalware and/or the SS7 card can be copied by the Steel-Belted Radius Carrier **configuration** script, but no third-party files are moved.

Refer to the Ulticom documentation for information on whether and how a previous release's configuration files may be used by the Signalware 9 installation.

RSA

12. (Optional) If the Steel-Belted Radius Carrier server will interact with an RSA authorization server, the Steel-Belted Radius Carrier server must be set up as an RSA client. Follow the RSA product documentation for the procedure.

    The Steel-Belted Radius Carrier server should receive a copy of several files from the RSA server. See Setting Up RSA Authorization Client on page 24 for Steel-Belted Radius Carrier requirements and the list of required files.

13. Verify that Steel-Belted Radius Carrier license keys have been assigned by logging in to your Juniper Networks support account.

    Licenses from earlier releases cannot be pulled forward. New Release 7.0 licenses are required.

    If you do not have a key you can go ahead with the installation, but a 30-day trial license with a low maximum session limit is automatically installed.

Installing Steel-Belted Radius Carrier Software

If all items on the "Before You Begin" list have been checked off, you should be ready to install the SBR Carrier software on the Release 7.0 server. These are the key steps:

1. Unpack the Steel-Belted Radius Carrier Software.

   See Unpacking the Steel-Belted Radius Carrier Software on page 29.

   If you are not familiar with UNIX package management commands, you can review a list of Package Management Commands on page 29.

2. Check for running SNMP processes on the server and shut down any that are active.

   See Shutting Down SNMP on page 31.

3. Run the Steel-Belted Radius Carrier **configure** script. As the script runs, enter the information you recorded on the previous pages.

NOTE: When the **configure** script prompts: *Please enter backup or radius directory from which to migrate.*, specify the path to the copy of the SIM Server 5.4 that you created earlier, in "Create a copy of the SIM Server 5.4 SBR installation on the system that will host Release 7.0." on page 8.

See Running the Steel-Belted Radius Carrier configure Script on page 32.

Basic Configuration

After the Steel-Belted Radius Carrier software is installed on the Solaris server, ensure that the base software runs properly and then perform basic configuration steps:

1. Start the Steel-Belted Radius Carrier daemon.

   If you usually do not start and stop the daemon from the command line, the basic commands are below, and you can review Steel-Belted Radius Carrier Server Commands on page 39:

   - Start the RADIUS Server:
     */radiusdir/***sbrd start**
     or restart: */radiusdir/***sbrd restart**

   - Stop the RADIUS Server:
     */radiusdir/***sbrd stop**

   - Display RADIUS Status Information:
     */radiusdir/***sbrd status**

2. Start SBR Administrator.

   Use an HTML browser to address the Steel-Belted Radius Carrier server HTML server. The default page should let you download the Administrator client application and log in as root. You should also confirm that the links to the documentation work.

   Verify that you can download and run the application both from the local host and from a workstation on the network.

3. Configuring the environment. This step includes basic, low-level configuration tasks, such as:

   - Configuring communications between any additional devices and the Steel-Belted Radius Carrier server.

   - Adding additional users to the server.

   For additional information, see Configuring the Server on page 42.

SNMP 4. SNMP configuration. If you elected to configure the Steel-Belted Radius Carrier SNMP agent during software installation and other agents also run on the server (such as the Solaris operating system agent), you will need to adjust the ports the agents use so multiple agents do not contend for the same resource.

   See Configuring SNMP on page 43.

5.4 5. A number of files can be manually migrated from a SIM Server 5.4, but the structure of the Release 7.0 files is different from previous releases because they carry configuration information on new features. Existing SIM Server 5.4 settings from each type of file listed here can be copied and pasted into the corresponding Release 7.0 files:

   - XML configurations

- JRE Extensions
- JavaScript files
- Dictionaries
- Third-party plug-ins and other binaries

Any root certificates that are not tied to a specific server may be moved, manually, to the new server.

See Migrating Files from Earlier Releases on page 44.

Release 6.x Migration Checklist

This checklist lists the recommended steps to migrate an existing Release 6.0 or 6.1 SBR Solaris Server installation to the Release 7.0 platform.

We recommend that the 6.*x* environment be duplicated so far as possible. For instance, if 6.0 or 6.1 uses a specific LDAP server or Oracle database, those should be set up so that the new Release 7.0 installation can access them using the older server's configuration information.

Before You Begin

Before you begin to install the Steel-Belted Radius Carrier software, perform these preliminary tasks or verify that they have been accomplished:

1. Review the Steel-Belted Radius Carrier *Release Notes* for up-to-date information that became available after the Steel-Belted Radius Carrier guides were published.

   Download the most recent Release Notes from:
   http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-rn700.pdf

   If the information in the *Release Notes* differs from the information in any Steel-Belted Radius Carrier guide, follow the *Release Notes.*

2. Create a copy of the 6.*x* SBR installation on the system that will host Release 7.0.

   The recommended method is:

   a. As root on the 6.*x* server, shut down the SBR daemon.
      Execute: */radiusdir/***sbrd stop**.

   b. Create a gzip archive of the 6.*x* *radiusdir* directory, preserving the file structure.

      Change directories to */opt/JNPRsbr/* and execute:
      tar cfE - radius |gzip > 6_radius.tgz

   c. As root on the Release 7.0 host, create a working directory for the archive:

Execute:
mkdir -p /opt/JNPRsbr/6_backup

and:

cd /opt/JNPRsbr/6_backup

d. Use ftp to copy the archive file to the Release 7.0 host.

e. Gunzip the archive in the working directory. This will not create a working installation, just serve as a source of files that can be reused by the Release 7.0 server.

Execute:
gunzip -dc 6_radius.tgz |tar xf -

f. Check the file permissions on the unzipped archive to ensure that the files are writable.

See "Backing Up SIM Server 5.4 or 6.x Release Files" on page 23 for more information.

3. Ensure that the Release 7.0 server chassis is physically secure.

   To review recommendations on the server's characteristics, see Selecting an Appropriate Server on page 20.

4. Confirm that the Release 7.0 server chassis provides at least the minimum hardware and software requirements.

   See Meeting System Requirements on page 21.

5. Verify root access on the Release 7.0 server.

6. Verify that the Release 7.0 server meets basic network connectivity and DNS requirements:

   - See Verifying Network Connectivity on page 25
   - See Verifying Host Name Resolution on page 25

7. Verify the Release 7.0 server role in the authentication environment. The installation script can configure a Steel-Belted Radius Carrier server as:

   - A stand-alone server.
   - The primary server in a group made up of replication servers.
   - A replication server.
     In an environment that uses replication servers, the primary server must be configured first to provide a base for replication.

LDAP

8. (Optional) If the Release 7.0 server will interact with a Lightweight Directory Access Protocol (LDAP) directory service agent, verify or record the path to the LDAP library files (The default path is /usr/lib.)

SQL 9. (Optional) If the Steel-Belted Radius Carrier server will use an external database:

- Verify database compatibility and interoperatability.

  See Setting Up External Database Connectivity on page 24.

ORACLE

- If the external database is Oracle, the Steel-Belted Radius Carrier server must be configured as a client of the Oracle server.

  As you set up the client, collect this information, or if the client is already installed, record this information to use while installing SBR Carrier software:

  - Record the path to the local Oracle Home directory (for example: **/opt/10g/app/oracle/product/10.2.0.3**)
  - Record the path to the local Oracle shared library (for example: **/opt/10g/app/oracle/product/10.2.0.3/lib32**)
  - Record the path to the local TNS_ADMIN (for example: **/opt/10g/app/oracle/product/10.2.0.3/network/admin**)

SS7 10. (Optional) Install a compatible SS7 interface board.

See Installing Signalware and SS7 Interfaces on page 24 for a list of supported boards, and the documentation that comes with the board for installation instructions.

SIM / WiMAX / SS7 11. (Optional) Install and configure Signalware 9 with Service Pack 5T software, following the product documentation.

- See *Chapter 6, Installing Signalware 9,* to see an example of a Signalware 9 installation.
- See *Chapter 7, Configuring SS7/IP Network Communication Files*, for information on editing Signalware configuration files.

NOTE: If the 6.*x* server installation used a version of Signalware released before Signalware 9, refer to the Ulticom documentation on whether and how a previous release's configuration files may be used by the Signalware 9 installation.

6.*x* files that reference Signalware can be copied by the Steel-Belted Radius Carrier installation procedure, but no third-party files are moved.

RSA 12. (Optional) If the Steel-Belted Radius Carrier server will interact with an RSA authorization server, the Steel-Belted Radius Carrier server must be set up as an RSA client. Follow the RSA product documentation for the procedure.

The Steel-Belted Radius Carrier server should receive a copy of several files from the RSA server. See Setting Up RSA Authorization Client on page 24 for Steel-Belted Radius Carrier requirements and the list of required files.

13. Verify that Steel-Belted Radius Carrier license keys have been assigned by logging in to your Juniper Networks support account.

    Licenses from earlier releases cannot be pulled forward. New Release 7.0 licenses are required.

    If you do not have a key you can go ahead with the installation, but a 30-day trial license with a low maximum session limit is automatically installed.

    See Obtaining a License Key on page 26.

Installing SBR Software

If all items on the "Before You Begin" list have been checked off, you should be ready to install the SBR software on the Release 7.0 server. These are the key steps:

1. Unpack the Steel-Belted Radius Carrier Software.

   See Unpacking the Steel-Belted Radius Carrier Software on page 29.

   If you are not familiar with UNIX package management commands, you can review a list of Package Management Commands on page 29.

SNMP

2. Check for running SNMP processes on the server and shut down any that are active.

   See Shutting Down SNMP on page 31.

3. Run the Steel-Belted Radius Carrier **configure** script. As the script runs, enter the information you recorded on the previous pages.

NOTE: When the **configure** script prompts: *Please enter backup or radius directory from which to migrate.*, specify the path to the copy of the 6.*x* server that you created earlier, in "Backing Up SIM Server 5.4 or 6.x Release Files" on page 23.

See Running the Steel-Belted Radius Carrier configure Script on page 32.

Basic Configuration

After the Steel-Belted Radius Carrier software is on the Solaris server, ensure that the base software runs properly and then perform basic configuration steps:

1. Start the Steel-Belted Radius Carrier daemon.

   If you usually do not start and stop the daemon from the command line, the basic commands follow, and you can review Steel-Belted Radius Carrier Server Commands on page 39:

   - Start the RADIUS Server:
     */radiusdir/***sbrd start**
     or restart: */radiusdir/***sbrd restart**

   - Stop the RADIUS Server:
     */radiusdir/***sbrd stop**

- Display RADIUS Status Information:
  */radiusdir/***sbrd status**

2. Start SBR Administrator.

   Use an HTML browser to address the Steel-Belted Radius Carrier server HTML server. The default page should let you download the Administrator client application and log in as root. You should also confirm that the links to the documentation work.

   Verify that you can download and run the application both from the local host and from a workstation on the network.

3. Configuring the environment. This step includes basic, low-level configuration tasks, such as:

   - Configuring communications between any additional devices and the Steel-Belted Radius Carrier server.
   - Adding additional users to the server.

   For additional information, see Configuring the Server on page 42.

4. SNMP configuration. If you elected to configure the Steel-Belted Radius Carrier SNMP agent during software installation and other agents also run on the server (such as the Solaris operating system agent), you will need to adjust the ports the agents use so multiple agents do not contend for the same resource.

   See Configuring SNMP on page 43.

6.0, 6.1 5. A number of files can be manually migrated from a SBR 6.*x* server to 7.0, but the structure of the files is different from previous releases because they carry configuration information on new features added in Release 7.0. Existing Release 6.*x* server settings from each type of file listed here can be copied and pasted into the corresponding Release 7.0 files:

   - XML configurations
   - JRE Extensions
   - JavaScript files
   - Dictionaries
   - Third-party plug-ins and other binaries

   Any root certificates that are not tied to a specific server may be moved, manually, to the new server.

   See Migrating Files from Earlier Releases on page 44.

Chapter 2

Before You Begin

This chapter presents requirements that must be checked and tasks that must be performed before Steel-Belted Radius Carrier is installed.

These topics are in the chapter:

- Reviewing the Release Notes on page 19
- Determining the Server Role on page 20
- Selecting an Appropriate Server on page 20
- Meeting System Requirements on page 21
- Backing Up SIM Server 5.4 or 6.x Release Files on page 23
- Setting Up External Database Connectivity on page 24
- Installing Signalware and SS7 Interfaces on page 24
- Setting Up RSA Authorization Client on page 24
- Verifying Network Requirements on page 25
- Verifying Root Access on page 25
- Obtaining a License Key on page 26

Reviewing the Release Notes

The Steel-Belted Radius Carrier *Release Notes* contain important late-breaking information, such as known software problems. Please review the release notes delivered with your Steel-Belted Radius Carrier software before you install SBR Carrier to ensure you are informed about important information not found elsewhere.

You can download the Release Notes from:
http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/bookpdfs/sw-sbrc-rn700.pdf

Determining the Server Role

Steel-Belted Radius Carrier software can be installed as a stand-alone server, as the primary server in a group of replication servers, or as a replica.

If you are installing in an environment that uses replica servers, make sure that the primary server is fully functional before installing any replicas — the replica servers need to communicate with the primary server during installation and when they start.

5.4, 6.0, 6.1 If you are migrating from an earlier SBR release to Release 7.0, both servers must be the same type. For example, a SIM Server 5.4 primary server can be migrated forward to create a Release 7.0 primary server. Or a stand-alone configuration can be used to set up a new stand-alone. But cross-type migration is not supported.

Selecting an Appropriate Server

Select an appropriate host to run the Steel-Belted Radius Carrier server software. An appropriate RADIUS server has these properties:

- A secure physical location such as a locked server room.
- Root access on the host limited to the system administrator. Restrict logon access to the Steel-Belted Radius Carrier server to system administrators and others who need it. Ideally, the server should have no (or few) user accounts.
- Adequate memory and disk space—See “Meeting System Requirements” on page 21 for information on hardware and software requirements.
- Administrative interface not accessible from outside your network—If your Steel-Belted Radius Carrier server has one network connection, limit access to the ports that it uses for configuration and administration.

  If your Steel-Belted Radius Carrier server has more than one network connection, an administrative network that is physically separate from other networks should be used to configure and administer the server.
- No public network services such as FTP or HTTP. Running public network services or applications unrelated to user authentication on the Steel-Belted Radius Carrier server may adversely affect the performance of Steel-Belted Radius Carrier, since it must compete with other services and applications for the server’s CPU resources. Moreover, running public network services on the authentication server potentially opens the server to malicious attacks. (Steel-Belted Radius Carrier implements its own HTTP service on a different socket port than generic web servers use.)
- A shared secret protects all communications to and from the server, including session keys for wireless data encryption. Configure shared secrets that are long enough and random enough to resist attack Avoid using the same shared secret throughout your network.

Meeting System Requirements

This section describes the hardware and software requirements for running Steel-Belted Radius Carrier on Sun hardware under the Sun Solaris 10 operating system.

Hardware

Recommended Configuration

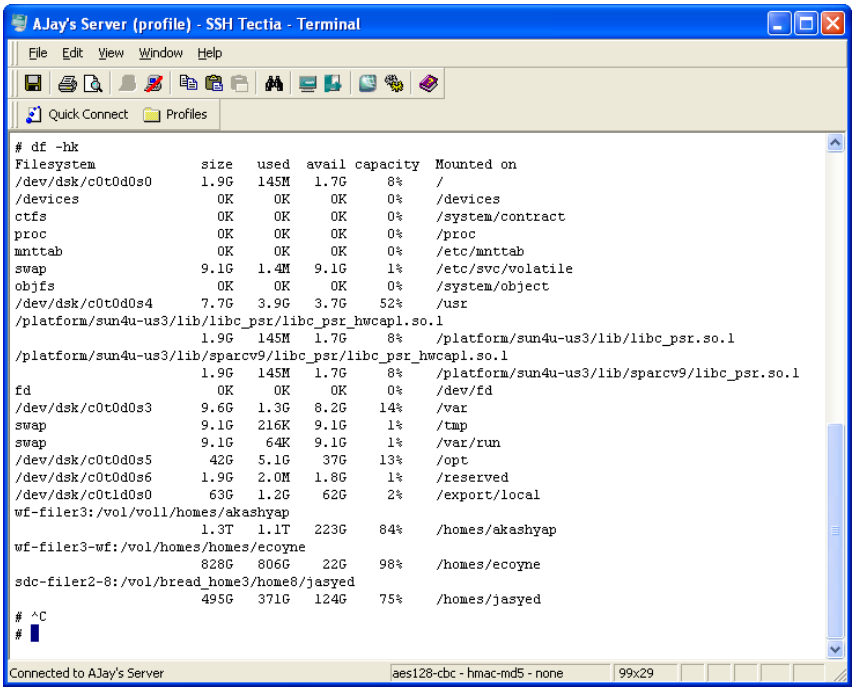
- At least 2 Gb RAM.

Minimum Configuration

- Two-CPU Ultrasparc IIIi processors or better, running at 1.5 Ghz or faster.
- At least 256 Mb RAM; at least 512 Mb for servers with more than 10,000 RADIUS users.
- At least 750 Mb of local hard disk space (not NFS), including about 81 Mb of local disk space for SBR Administrator.

  Use the **df** shell command in a terminal window to check the amount of free space available, as in Figure 1:

Figure 1: Checking Free Disk Space with the df Command



Software

Steel-Belted Radius Carrier server requires Sun Solaris 10 8/07 for SPARC platforms, with the appropriate patches.

Required Patches

These patches (or higher numbered equivalent patches) are required for Solaris 10:

- 117461-08 ld.so
- 119254-44 patchadd
- 119963-08 libC
- 120753-05 libmtsk
- 120900-04 libzonecfg
- 121133-02 zoneadm

Recommended Patches

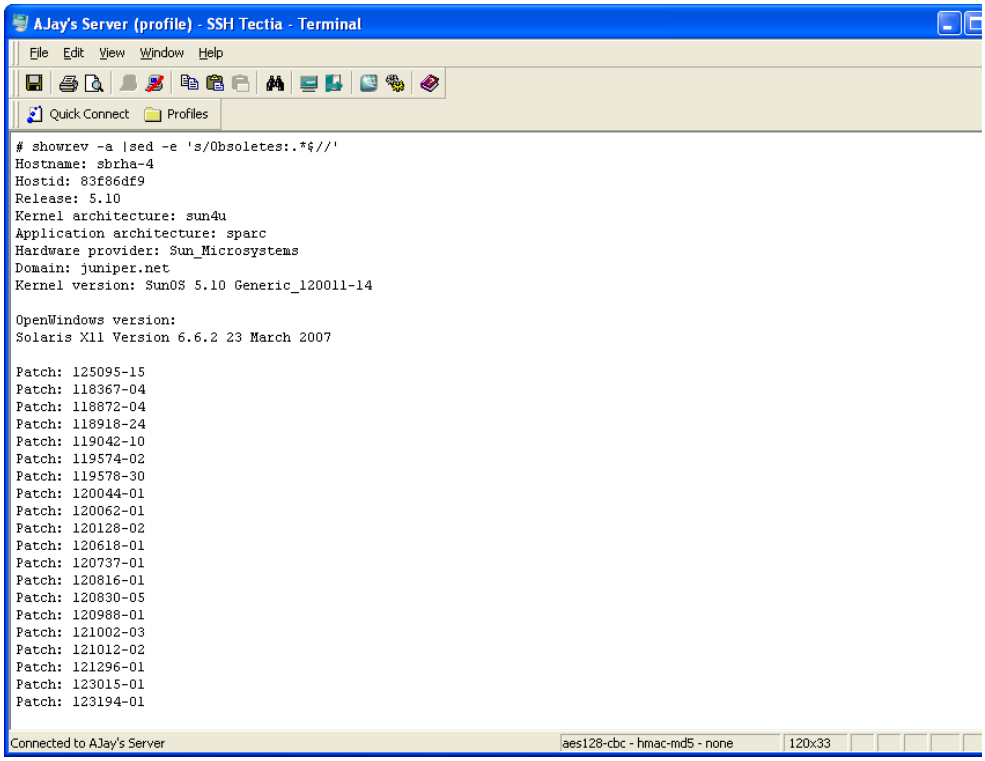
These patches (or higher numbered equivalent patches) are recommended for Solaris 10:

- 113886-48 OpenGL 1.3 32-bit
- 113887-48 OpenGL 1.3 64-bit

Gather the system's patch information by executing the UNIX shell command:

showrev -a |sed -e 's/Obsoletes:.*$//'

Figure 2: Checking Server Patch Status with the showrev Command



This is not a complete listing; many patches are already present because they are bundled with the Sun Solaris 10 8/07 for SPARC platforms,

Perl

Sun ships Solaris 10 with Perl 5.8.4, and Steel-Belted Radius Carrier has been tested with that version. Multiple Perl installations in discrete directories are supported, but attempting to use other versions of Perl with SBR Carrier may cause problems.

After installation, be sure that the first line of the radiusd script specifies the correct path to the Perl 5.8.4executable. For example, if Perl 5.8.4 is installed in the default location, */usr/bin/perl*, then the first line of the radiusd script must be:

```
#!/usr/bin/perl
```

Backing Up SIM Server 5.4 or 6.x Release Files

If SIM Server 5.4, 6.0, or 6.1 is installed on a server and you want to carry these configuration files forward during the Release 7.0 installation, transfer a copy of the existing installation to the machine that will host SBR Carrier.

The recommended procedure is:

1. As root on the existing server, shut down the SBR daemon.
   Execute: */radiusdir*/**sbrd stop**.

2. Create a gzip archive of the *radiusdir* directory, preserving the file structure.

   Change directories to */opt/JNPRsbr/* and execute:
   tar cfE - radius |gzip > radius.tgz

3. As root on the Release 7.0 host, create a working directory for the archive:

   Execute:
   mkdir -p /opt/JNPRsbr/backup

   and:

   cd /opt/JNPRsbr/backup

4. Copy the archive file to the Release 7.0 host.

5. Ungzip the archive in the working directory. This will not create a working installation, just serve as a source of files that can be reused by the Release 7.0 server.

   Execute:
   gunzip -dc radius.tgz |tar xf -

6. Check the file permissions on the unzipped archive to ensure that the files are writable.

Remember the path to the archive directory. During installation, the Release 7.0 configure script will prompt you to supply the location so some configuration files can be migrated into the new installation.

Setting Up External Database Connectivity

Steel-Belted Radius Carrier supports external databases for authentication.

- Oracle 9 and 10 are supported; versions 9.2.0 and 10.2.0 are recommended.
- For the Steel-Belted Radius Carrier to act as an Oracle native client, Oracle client must be set up before installing SBR Carrier because the Oracle server location is used during installation.
- The JDBC plug-in has been tested with Oracle on Solaris and the JDBC plug-in for MySQL.

Installing Signalware and SS7 Interfaces

If the Steel-Belted Radius Carrier server will support the SBR Carrier SIM or WiMAX module, Ulticom Signalware 9 with Service Pack 5T needs to be installed in the server before you install SBR Carrier software.

If the Steel-Belted Radius Carrier server will communicate with any SS7 legacy equipment, the Ulticom SS7 communication board and Signalware 9 with Service Pack 5T should both be installed before you install SBR Carrier software.

The Signalware PH0301 and XH0303 boards are supported.

- See *Chapter 6, Installing Signalware 9,* for an example of a Signalware 9 installation.
- See *Chapter 7, Configuring SS7/IP Network Communication Files*, for information on editing Signalware configuration files.

Setting Up RSA Authorization Client

If you integrate an RSA authentication server with the Steel-Belted Radius Carrier server:

- Ensure that the RSA server runs RSA Authentication Manager 6.1 or later.
- Set up the SBR Carrier server as an RSA client. Part of that procedure requires copying these files from the RSA server to the local SBR Carrier server:
  - failover.dat
  - LICENSE.REC
  - radius.cer
  - radius.key
  - RSA_Note01.txt
  - sdconf.rec
  - SDTI.CER

- SERVER.CER
- SERVER.KEY

When you copy the files to the Steel-Belted Radius Carrier server, make a note of the files' local directory — you will need to enter it during the installation.

Verifying Network Requirements

Basic network connectivity is required to install the Steel-Belted Radius Carrier software.

Verifying Network Connectivity

Use the ping command both to and from another computer to verify that the server on which you are going to install Steel-Belted Radius Carrier can communicate with other devices, such as remote access servers, database servers, DHCP servers, DNS servers, and management workstations on your network, using TCP/IP. For example:

 # ping 192.168.12.54

```
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
```

If the ping command fails, verify that the IP address of the Steel-Belted Radius Carrier host is correct, that is operational, and that all routers between your server and the remote host are operational.

Verifying Host Name Resolution

The server on which you are going to install Steel-Belted Radius Carrier must have a stable, accessible IP address that is mapped in /etc/hosts or the Domain Name System (DNS) server to a resolvable hostname.

To verify that the server has a resolvable hostname, use the ping command with the server's hostname. For example:

 # ping foo.juniper.net

```
Pinging foo.juniper.net [192.168.12.21] with 32 bytes of data:
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
```

Verifying Root Access

You must have access to the root account in order to install Steel-Belted Radius Carrier software.

Obtaining a License Key

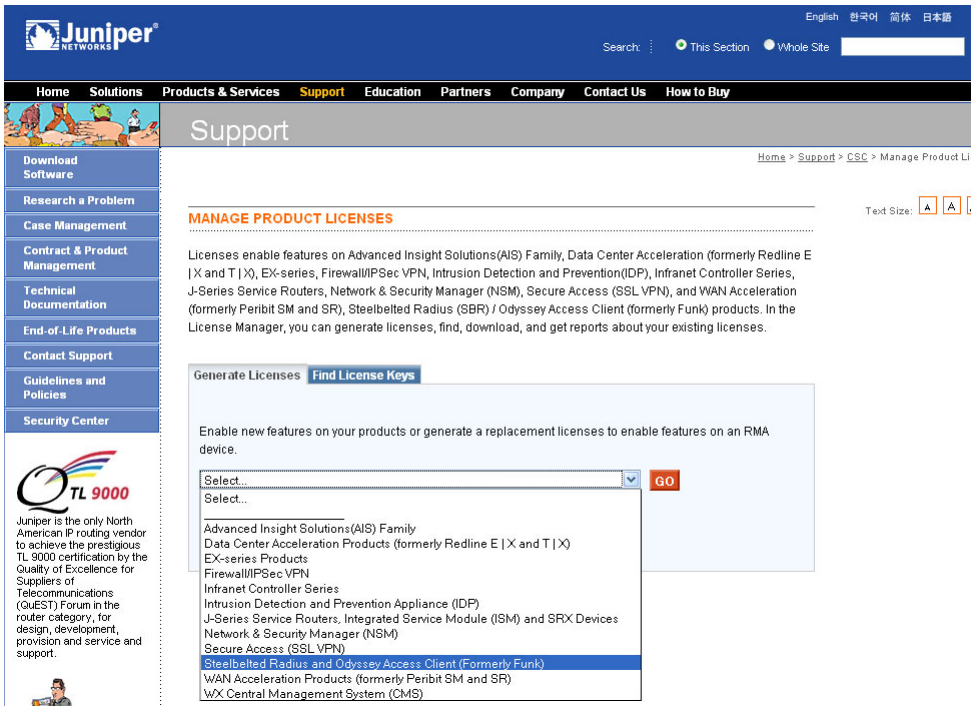
If you want to install the Steel-Belted Radius Carrier server software for a 30-day evaluation, you do not need a license key.

If you want to install a permanent (non-evaluation) copy of Steel-Belted Radius Carrier, you must have a unique single-seat software license key for each server installation.

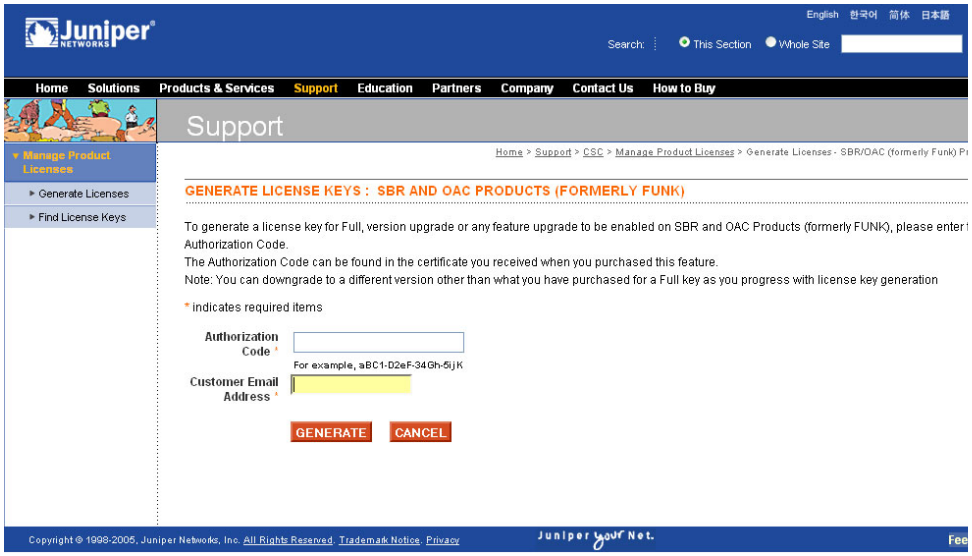
When a license is purchased, a certificate containing an authorization code is issued. Use the authorization code to generate a license key on the Juniper Networks support server.

1. Browse http://www.juniper.net/customers/support/ and select Generate / Manage License Keys. You may be prompted to log in.

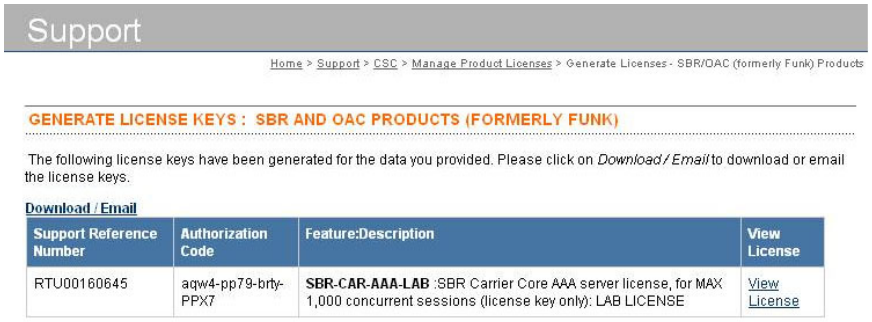
2. On the Manage Product Licenses screen, select Steel-Belted Radius Carrier from the drop-down list and click Go.



3. Enter the authorization code from your certificate and the registered e-mail address. (The e-mail address is used only for account verification at this point; you can elect not to receive the license through e-mail in the next step.)



4. When the key is generated, a success screen is displayed. You can view the license online and record the key number, download it, or have it sent to the e-mail address you entered.



You may deploy the SBR Administrator on as many workstations as you require; it is not licensed.

5.4, 6.1, 6.0 License files from previous versions are moved if an automatic migration is selected when the configuration script is executed, but they are not valid in Release 7.0. You can still set up the Steel-Belted Radius Carrier server, but you will need to install valid Release 7.0 licenses to make the server fully functional and to operate beyond the 30-day evaluation period.

Warning messages that state that the Steel-Belted Radius Carrier is operating with 30-day evaluation licenses are written to the log file if a valid license is not present.

Chapter 3

Installing SBR Software

This chapter documents the configure script that installs Steel-Belted Radius Carrier software on the server.

These topics are in the chapter:

- Unpacking the Steel-Belted Radius Carrier Software on page 29
- Shutting Down SNMP on page 31
- Running the Steel-Belted Radius Carrier configure Script on page 32
- Historic Files on page 37

Unpacking the Steel-Belted Radius Carrier Software

This section assumes that you are installing Steel-Belted Radius Carrier on your Solaris server for the first time or that you are installing Steel-Belted Radius Carrier in a directory other than the one used by previous installations — a clean installation.

Package Management Commands

The installer for the Solaris version of the Steel-Belted Radius Carrier server software uses pkgadd files, which have filenames that include the edition and version of the server software.

Table 5 lists common Solaris package management commands.

Table 5: Useful Package Management Commands

Command	Function
pkginfo -x |egrep "FUNK|JNPR|RSAR"	Report any pre-existing packages and patches.
pkginfo -l JNPRsbr	Report high level description for specified package
pkginfo -r JNPRsbr	Show installed directory
pkgadd -d */path/to/*JNPRsbr.pkg [-a none] JNPRsbr.pkg	Install [at specified */path*]
pkgrm JNPRsbr	Uninstall Steel-Belted Radius Carrier.

To install the Steel-Belted Radius Carrier server software on a Solaris server:

1. Log in to the Solaris server as root.

2. Copy the Steel-Belted Radius Carrier installation files from their download location or CD to the Solaris server. Make sure to copy them to a local or remote hard disk partition that is readable by root.

   This example copies the files from a CD to the /tmp/sbr directory.

   # mkdir -p /tmp/sbr
   # cp -pR /cdrom/sbr/solaris/* /tmp/sbr

3. Extract the Steel-Belted Radius Carrier installation package.

```
# cd /tmp/sbr
# $ls -ltr
total 216240
-rw-r--r--   1 root     root     110712276 Aug 25 09:44 JNPRsbr.7.0.0.sol.pkg.tgz
#gunzip -dc JNPRsbr.7.0.0.sol.pkg.tgz |tar xf -
```

4. Verify that the extraction worked and confirm the name of the package file.

```
# ls -ltr
total 216256
drwxr-xr-x   4 Xtreece  other        370 Aug 24 17:01 JNPRsbr.pkg
-rw-r--r--   1 root     root     110712276 Aug 25 09:44 JNPRsbr.7.0.0.sol.pkg.tgz
```

5. Install the package.

```
# pkgadd -d /tmp/sbr

The following packages are available:
  1  JNPRsbr.pkg     JNPRsbr - Juniper Networks Steel-Belted Radius Carrier
                     (sparc) 7.00.4556

Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]: all
```

6. Type **all** and press Enter.
   The script resumes.

```
JNPRsbr - Juniper Networks Steel-Belted Radius Carrier(sparc) 7.00.4556
(C) Copyright 1996-2008 Juniper Networks, Inc.  See license.txt

The selected base directory </opt/JNPRsbr> must exist before installation is attempted.

Do you want this directory created now [y,n,?,q]
```

7. Confirm that the script should create the directory. Enter **y**.
   The script resumes.

```
Using </opt/JNPRsbr> as the package base directory.
## Processing package information.
## Processing system information.
   48 package pathnames are already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.
```

```
This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <JNPRsbrsp> [y,n,?]
```

8. Confirm that you want to continue to install the package. Enter **y**.

```
**** user will see a scrolling list of all the files being installed. The files shown below are only a
subset*******
.....
/opt/JNPRsbr/radius/openldap/schema/openldap.schema
/opt/JNPRsbr/radius/openldap/slapd
/opt/JNPRsbr/radius/openldap/tools/Examples.txt
/opt/JNPRsbr/radius/openldap/tools/db_recover
/opt/JNPRsbr/radius/openldap/tools/ldapdelete
/opt/JNPRsbr/radius/openldap/tools/ldapmodify
/opt/JNPRsbr/radius/openldap/tools/ldapsearch
/opt/JNPRsbr/radius/openldap/ucdata/case.dat
/opt/JNPRsbr/radius/openldap/ucdata/cmbcl.dat
/opt/JNPRsbr/radius/openldap/ucdata/comp.dat
/opt/JNPRsbr/radius/openldap/ucdata/ctype.dat
/opt/JNPRsbr/radius/openldap/ucdata/decomp.dat
/opt/JNPRsbr/radius/openldap/ucdata/kdecomp.dat
/opt/JNPRsbr/radius/openldap/ucdata/num.dat
/opt/JNPRsbr/radius/optiva.dct
/opt/JNPRsbr/radius/optivity.dct
/opt/JNPRsbr/radius/oracle.ini
/opt/JNPRsbr/radius/orinoco.dct
/opt/JNPRsbr/radius/paceset.dct
/opt/JNPRsbr/radius/parlayPPSPlugin.gen
/opt/JNPRsbr/radius/parlayPPSPlugin.so
/opt/JNPRsbr/radius/passaprt.dct
/opt/JNPRsbr/radius/passport.dct
/opt/JNPRsbr/radius/pathdb.dct
/opt/JNPRsbr/radius/peapauth.aut
/opt/JNPRsbr/radius/peapauth.so
/opt/JNPRsbr/radius/pico.dct
/opt/JNPRsbr/radius/portmstr.dci
/opt/JNPRsbr/radius/portmstr.dct
/opt/JNPRsbr/radius/pprt8000.dct
/opt/JNPRsbr/radius/prepaidAcct.acc
/opt/JNPRsbr/radius/prepaidAcct.so
/opt/JNPRsbr/radius/prepaidAttr.att
/opt/JNPRsbr/radius/prepaidAttr.so
/opt/JNPRsbr/radius/proxy.ini
......
[ verifying class <none> ]
## Executing postinstall script.
Newly installed server directory will be backed up as:
/opt/JNPRsbr/radius/install/backups/2008:08:25-09:47:28

Installation of <JNPRsbrsp> was successful.
```

Shutting Down SNMP

Shut down any running SNMP agents on the server before continuing.

During installation, the Steel-Belted Radius Carrier SNMP agent is installed and started, but it is likely that other SNMP agents are already using the default port. To avoid a conflict, shut down any existing agents before the installation.

Running the Steel-Belted Radius Carrier configure Script

1. Navigate to the directory where you installed the Steel-Belted Radius Carrier package in "Extract the Steel-Belted Radius Carrier installation package." on page 30. In that example, the directory is `/opt/JNPRsbr`.

   # cd /opt/JNPRsbr/radius/install/

2. Execute the configure script to install the Steel-Belted Radius Carrier server software:

   # ./configure

3. Review the Steel-Belted Radius Carrier license agreement.

   Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter **y**.

   Do you accept the terms in the license agreement? [n] **y**

4. Enter a license key for your Steel-Belted Radius Carrier software.

   You can enter a license string or use a one-time 30 day trial license.
   Would you like to enter a license string? [n]
   Installed a 30 day evaluation license.

   - If you purchased Steel-Belted Radius Carrier, type **y** and press Enter. When prompted to do so, enter your license key and press Enter. (Your license key is available online in your juniper.net account area.) The configure script creates a license file that contains the key on the server.
   - If you do not have a license key, type **n** and press Enter. The Steel-Belted Radius Carrier software is installed as a 30-day evaluation package that provides the product's full feature set with a maximum of 50,000 sessions.

5.4, 6.0, 6.1

5. Enter the type of installation.

   The system prompts for the type of installation, either a new installation or a migration from a SIM Server 5.4 or 6.x SBR server:

   ```
   Please enter backup or radius directory from which to migrate.
   Enter n for new configuration, s to search, or q to quit
   [/opt/JNPRsbr/5_4backup]:
   ```

   - For a new installation, enter n.
   - If you are migrating an existing Steel-Belted Radius Carrier installation and have copied a previous release's files to the Release 7.0 server (in "Backing Up SIM Server 5.4 or 6.x Release Files" on page 23), enter the directory path to the copy of the old installation.
   - If you are migrating an existing Steel-Belted Radius Carrier installation and have copied a previous release's files to the Release 7.0 server (in "Backing Up SIM Server 5.4 or 6.x Release Files" on page 23), but you need to search for the directory that contains the Steel-Belted Radius Carrier files, enter s.

NOTE: Steel-Belted Radius Carrier Release 7.0 supports importing a previous version's configuration files only from SIM Server 5.4 and SBR 6.0 and 6.1.

If you select this option, remember that some files require manual editing and updating after installation. This is discussed in Migrating Files from Earlier Releases on page 44.

6. For most installations, do not remove older versions of Steel-Belted Radius Carrier.

   WARNING: Now is the best time to remove any pre-existing versions of the software, as doing so later may destroy certain shared OS resources, such as /etc/init.d scripts in particular, that are about to be configured. Obsolete patches may also be removed.
   Manually remove pre-existing software now? [y]:

   Only answer **y** if a working installation already exists on the server proper — a copy of an installation or one on a different server that is an NFS mount can be ignored. If you respond with **y**, the script terminates so you can back up and remove the previous version.

   If you do need to remove an existing installation, refer to that release's documentation for instructions.

7. Specify the login name of the initial Steel-Belted Radius Carrier administrator.

   The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

   Enter initial admin user (account must have an associated password) [root]:

CAUTION: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

8. Specify whether you want to set up the Steel-Belted Radius Carrier server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

   Configure SBR server as primary (p), replica (r), or standalone (sa) [sa]:

5.4, 6.0, 6.1

NOTE: If you are migrating from a previous release, you may only select a server type that matches the old existing server.

- If you enter **p**, to designate a primary server, you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

If appropriate, enter **y** when you are asked whether you are migrating a primary server. Doing so tells the installer to preserve the server's replication realm information.

- If you enter **r**, to designate a replica server, you are prompted to specify how the replica server can locate the replica.ccmpkg configuration package containing your Steel-Belted Radius Carrier replication settings.
  - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.
  - If you want to specify the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address, and replication secret of the primary server.

  Enter **y** if you are prompted to indicate asked whether you are migrating a replica server. Doing so causes the installer to preserve the replica server's replication settings.
- If you enter sa, to designate a standalone RADIUS server, you do not enter any replication information.

LDAP

9. Specify whether you want to configure Steel-Belted Radius Carrier to use an external LDAP data service.
   - If you do not want to configure Steel-Belted Radius Carrier to use an external LDAP data service, press Enter.
   - If you want to configure Steel-Belted Radius Carrier for use with an external LDAP data service, type **y** and press Enter. You are prompted to enter the path for the LDAP library files:

     Do you want to configure LDAP? [n]: **y**
     Enter path for LDAP library files [/usr/lib]:

   To accept the default path (/usr/lib), press Enter.

Oracle

10. Specify whether you want to configure Steel-Belted Radius Carrier to access an Oracle database.

NOTE: If the server has already been set up with an Oracle client (in "Setting Up External Database Connectivity" on page 24), answer **y**.

If the server will use the jdbc/odbc driver, answer **n**.

Configuring for use with generic database
Do you want to configure for use with Oracle? [n]:

- To accept the default no, press Enter.
- If you will use Oracle, type **y** and press Enter. You are prompted for the Oracle version and path information to the Oracle library files.

Configuring for use with Oracle.
Supported Oracle version: 9, 10
What version of Oracle will be used? [9] **10**
Configuring for use with Oracle 10
Setting the environment variable ORACLE_HOME.
Enter ORACLE_HOME []: **/opt/10g/app/oracle/product/10.2.0.3**
Setting the environment variable LD_LIBRARY PATH.
Enter path for Oracle shared libraries
[/opt/10g/app/oracle/product/10.2.0.3/lib32]:
Setting the environment variable TNS_ADMIN.
Enter TNS_ADMIN [/opt/10g/app/oracle/product/10.2.0.3/network/admin]:

NOTE: Steel-Belted Radius Carrier requires Oracle 10 32-bit executables, which are stored in the /lib32 directory. Steel-Belted Radius Carrier is not compatible with the Oracle 10 64-bit executables stored in the /lib directory.

---

11. Specify whether you want the Steel-Belted Radius Carrier server to communicate with an SS7 system.

    Do you want to configure for use with SS7? [n]: **y**
    Configuring for use with SS7
    Setting the environment variable OMNI_HOME
    Enter OMNI_HOME []: **/opt/ulcm**

SNMP

12. Specify whether you want the Steel-Belted Radius Carrier server to be an SNMP agent.

    Do you want to configure SNMP? [n]:

    - If no, press Enter to proceed to the next prompt.
    - If yes, type **Y** and press Enter. The installer prompts you for the information it needs to configure the jnprsnmpd.conf and startsnmp.sh files.

      a. Provide the community string.

      Choose a community string: **public**

      b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format.

      - To specify that only one host may query the agent, enter the IP address of the host followed by /32.
      - To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

      Specify the range of IPv4 addresses that may query this agent, such as 1.2.3.0/24.
      Address range: **192.168.70.0/24**

      c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink to receive trap information from the SNMP agent on the Steel-Belted Radius Carrier server.

SNMPv2 trap sink: **192.168.70.86**
Configuration of SNMP complete.

RSA 13. Specify whether you want to register your Steel-Belted Radius Carrier server as an Agent Host with RSA Authentication Manager.

Do you want to register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

NOTE: When you register your Steel-Belted Radius Carrier master or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

---

14. Specify whether you want to configure the Steel-Belted Radius Carrier server to autoboot (restart automatically when the operating system is restarted).

Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: **e**

Steel-Belted Radius Carrier stores its autoboot settings in the local \radiusdir\radius\sbrd file.

- If you enter e (enable), the configure script copies the settings in the sbrd file to the /etc/init.d boot script and deletes an existing Steel-Belted Radius Carrier autoboot settings.
- If you enter d (disable), the configure script does not copy the settings in the sbrd file to the /etc/init.d boot script and deletes old Steel-Belted Radius Carrier autoboot settings, disabling autobooting for all versions of Steel-Belted Radius Carrier.
- If you enter p (preserve), the configure script does not copy the settings in the sbrd file to the /etc/init.d boot script or delete old Steel-Belted Radius Carrier autoboot settings, thereby leaving your previous autoboot settings unchanged.

When you finish entering settings, the script configures Steel-Belted Radius Carrier with the settings you specified and then displays:

```
The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete
```

Historic Files

5.4, 6.0, 6.1 When Steel-Belted Radius Carrier Release 7.0 is installed and a previous release's files are migrated forward, the Release 7.0 installation script creates another copy of some critical older files in the /radius/install/backups directory. The data files in Table 6 record version and other operating information that is used by subsequent installations.

CAUTION: Do not move, rename, or otherwise modify these files.

Table 6: Historic Files and Directories

File	Function
radius/install/package.dat	Contains a unique package identifier.
radius/install/preinstall.dat	Contains the absolute path name of the backup directory for your old Steel-Belted Radius Carrier software and configuration files (pre-installation backup).
radius/install/install.dat	Contains the absolute path name of the backup directory for your Steel-Belted Radius Carrier software and configuration files, as shipped without modification (post-installation backup).
radius/install/migrate.dat	Contains the absolute place name of the Steel-Belted Radius Carrier migrate source, if any exist.
radius/install/configure.dat	Contains configuration state data.
radius/install/uninstall.dat	Contains the absolute place name of the backup directory for your Steel-Belted Radius Carrier software and working configuration files (pre-uninstall backup).
radius/install/backups/	Contains the backups referenced by the.dat files.

Chapter 4

Basic Configuration

This chapter contains basic information on setting up a new Steel-Belted Radius Carrier server

This chapter contains these topics:

- Steel-Belted Radius Carrier Server Commands on page 39
- Running SBR Administrator on page 40
- Configuring the Server on page 42
- Configuring SNMP on page 43
- Migrating Files from Earlier Releases on page 44

Steel-Belted Radius Carrier Server Commands

To begin, start the SBR daemon. You should also verify that you can stop it and check the server status from a terminal command line.

Starting the RADIUS Server

Use the following command to start the RADIUS server manually.

cd *radiusdir*
./sbrd start

If you change configuration settings for your Steel-Belted Radius Carrier server, you may need to restart Steel-Belted Radius Carrier to make the changes effective. As an alternative to issuing an sbrd stop command immediately followed by an sbrd start command, you can use the sbrd restart command to restart Steel-Belted Radius Carrier. When you issue the sbrd restart command, Steel-Belted Radius Carrier shuts down and then immediately starts the RADIUS processes.

cd *radiusdir*
./sbrd restart

Stopping the RADIUS Server

Use the following commands to stop the RADIUS server:

cd *radiusdir*
./sbrd stop

When you execute the sbrd stop command, Steel-Belted Radius Carrier allows its subsystems to complete outstanding work and release resources, and then stops the RADIUS processes gracefully.

If Steel-Belted Radius Carrier fails to stop after you issue the sbrd stop command, you can use the optional force argument to terminate all subsystems immediately.

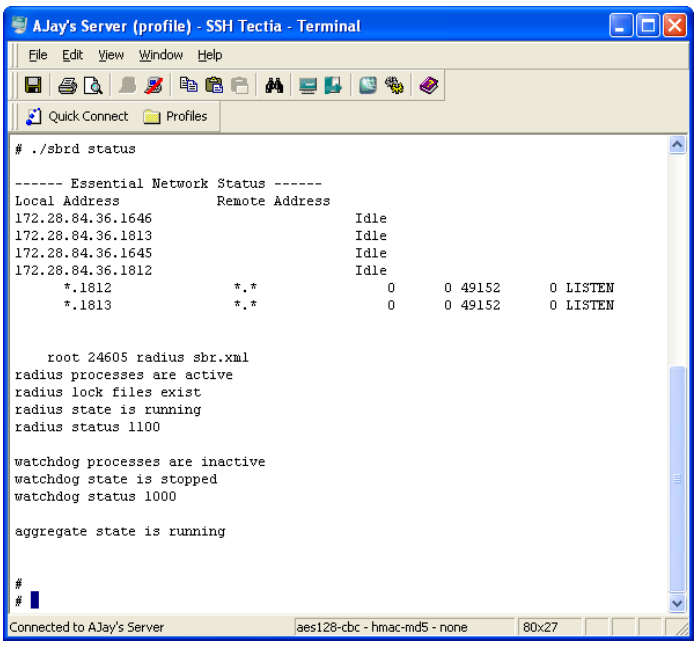
cd *radiusdir*
./sbrd stop force

Displaying RADIUS Status Information

You can use the sbrd status command to display status information for the RADIUS process.

cd *radiusdir*
./sbrd status

Figure 3: Results of the sbrd status Command



Running SBR Administrator

To test whether the server can be accessed by a management workstation, install and run SBR Administrator.

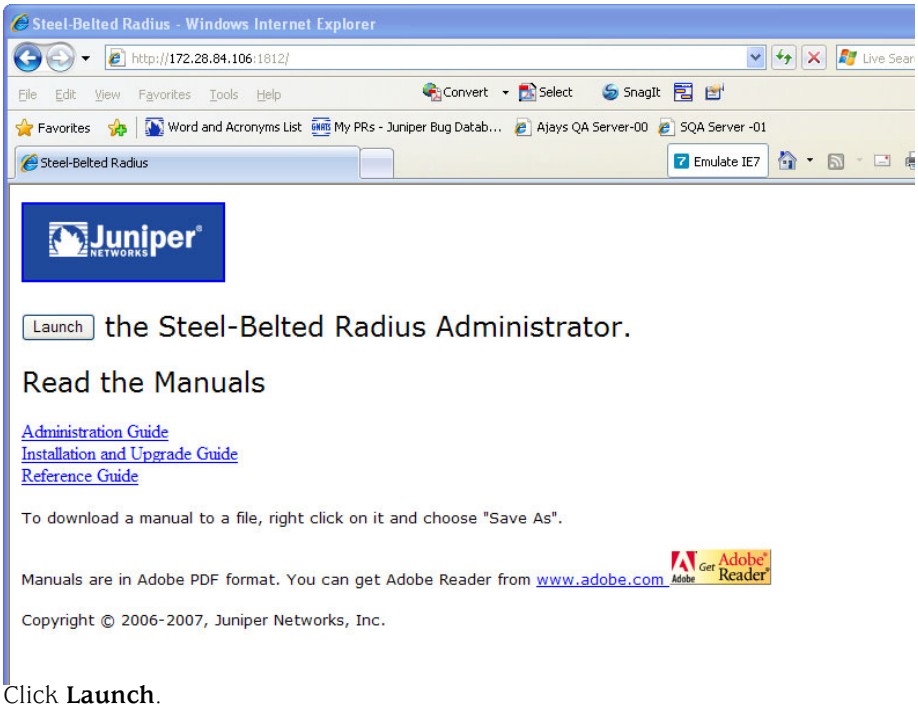
1. Open a browser connection to the Steel-Belted Radius Carrier server.

   - To address the server, on the local host, enter http://localhost:1812/ (The port assignment of 1812 is the application's default TCP port for administration connections).

- To administer a Steel-Belted Radius Carrier server running on a remote host, enter http://*server*:*port*/

  where *server* is the DNS name or IPv4/IPv6 address of the server, and *port* is the TCP port on which the server is listening for administration connections — usually 1812.

  For example:
  http://192.168.24.15:1812/

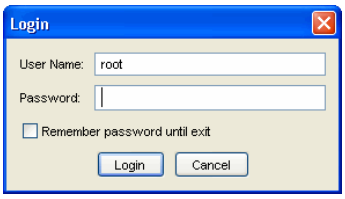


2. Click **Launch**.

   "Applet Deploy started" is displayed in the status bar at the bottom of the screen.

3. An SBR Administrator window and a Login dialog window open.

   Enter your administrator username, root, and the root password.



4. Click **Login**.

When you click **Login**, SBR Administrator establishes an HTTPS connection with the local or remote server. If it cannot establish a connection in 10 seconds, SBR Administrator times out and displays an error message.

NOTE: If a timeout occurs, verify that the Steel-Belted Radius Carrier daemon is running on the target server and that it is listening on the administration port you entered in the URL; that the port is not blocked.

SBR Administrator verifies that the username you entered exists in the access.ini file. If the username is found, SBR Administrator validates the password you entered against a local or remote password database.

When you connect to a server, the **Status** panel lists various features of the running server, such as version, platform on which it is running, IP address, available authentication methods, license information, and any initialization errors that might have occurred.

Configuring the Server

After you have installed the Steel-Belted Radius Carrier software on the server, have added the appropriate licenses, and can work with SBR Administrator, you can begin configuring the software. The specific steps you must perform depend on your network's authentication and accounting needs.

The basic steps for configuring the Steel-Belted Radius Carrier environment includes:

1. Configure each of your RADIUS client devices to communicate with your Steel-Belted Radius Carrier server. To do this, you must log in to each device and run its configuration interface.

2. Use SBR Administrator's RADIUS Clients panel to configure the server to communicate with each RADIUS client. Details are in *Chapter 4, Administering RADIUS Clients and Client Groups* of the *Steel-Belted Radius Carrier Administration and Configuration Guide*.

   If the clients use RADIUS Location Groups or IP Address Pools, each of those entities must exist before the clients are configured. See *Chapter 5, Administering RADIUS Location Groups* and *Chapter 10, Administering Address Pools* of *Steel-Belted Radius Carrier Administration and Configuration Guide* for instructions on setting these up.

3. Use the Users panel to identify the users or groups of users who are permitted to access the RADIUS clients.

   Specify user attributes by selecting them in the Users panel or by creating user profiles in the Profiles dialog.

For more information, refer to the *Steel-Belted Radius Carrier Administration and Configuration Guide*.

Configuring SNMP

Steel-Belted Radius Carrier runs its own SNMP agent, but other SNMP agents run on most servers. In general, only one application can use a socket port; they are not shared resources. This means that SBR Carrier SNMP agent may conflict with Solaris SNMP or any other SNMP agent that uses socket port 161, the default SNMP port.

If you know that other agents already use port 161, change the Steel-Belted Radius Carrier port assignment by editing both *radiusdir*/snmp/conf/jnprsnmpd.conf and *radiusdir*/snmp/bin/testagent.sh. Remember to check your MIB browser to determine whether it also needs adjustment to communicate with the SBR Carrier server.

To change the port, edit the two SBR Carrier SNMP configuration files listed in Table 7:

Table 7: SNMP Configuration Files

File Name	Function
jnprsnmpd.conf	Stores settings for the Steel-Belted Radius Carrier SNMP agent.
testagent.sh	Test script that verifies the Steel-Belted Radius Carrier SNMP agent is operating correctly.

1. Edit *radiusdir*/snmp/conf/jnprsnmpd.conf to change the port number.

   The jnprsnmpd.conf file is self-documenting, and you can also reference *Chapter 14, SNMP Configuration Overview* in the *Steel-Belted Radius Carrier Reference Guide*.

CAUTION: The jnprsnmpd.conf file is very sensitive to stray white space and the order in which sections and parameters appear. Mistakes in this file can disable SNMP.

- Make sure to make a backup copy of the file before making any changes.
- While editing the file, do not to make any unnecessary changes. Follow the embedded examples as closely as possible.
- When specifying networks, as in 172.28.68.0/24 in the com2sec mynetwork 172.28.68.0/24 public line, the trailing 32-x bits of the IP address must be zero as specified by the trailing /x notation. For example, 32-24 = 8 bits in this case.

2. Make the same port number change in *radiusdir*/snmp/bin/testagent.sh script, which is used to test the agent.
3. After making the change, restart either the Steel-Belted Radius Carrier server process or just its SNMP daemon.
4. If necessary, set up your SNMP browser to listen on the new port.

5. To verify that the jnprsnmpd SNMP agent functions, run the *radiusdir*/snmp/bin/testagent.sh script.

NOTE: Refer to the *Steel-Belted Radius Carrier Administration and Configuration Guide* for more information on configuring the SBR SNMP agent.

Migrating Files from Earlier Releases

5.4, 6.0, 6.1 Migrating from SIM Server 5.4 or SBR 6.0 or 6.1 to Release 7.0 requires that some files be manually edited to move existing settings into the corresponding Release 7.0 files, because the new release has a different file structure that must be preserved.

All other files are automatically migrated during the migrate process. You only need to perform these edits if you imported configuration files from a previous release during installation (discussed in Running the Steel-Belted Radius Carrier configure Script on page 32).

Manual Migration of XML Configurations

You must manually move existing settings into the corresponding XML files that are delivered in the new Steel-Belted Radius Carrier software installation.

CAUTION: Do not modify any *.xml files except these four:

- /radius/sbr_administration.xml — Socket port number specified by port = setting
- /radius/sbr_ccm.xml — Socket port numbers specified by port = settings
- /radius/sbr_id.xml — Hostname specified by id = setting
- /system/config/logging_mgr.xml — LogStream events = settings

The IP addresses, hostnames, socket port numbers, and other similar data entries found in these files often have corresponding parameters in the radius.ini file which must be kept in agreement.

Manual Migration of JRE Extensions

Steel-Belted Radius Carrier is shipped with its own Java Runtime Environment (JRE) to facilitate JDBC plug-ins and JavaScript implementation. You can extend the JRE by installing third-party .jar files in the radius/jre/lib/ext subdirectory. You must migrate any third party .jar files by copying them to the new Steel-Belted Radius Carrier software installation.

These .jar files are shipped with Steel-Belted Radius Carrier. Do not migrate earlier versions to the Release 7.0 server:

- dnsns.jar
- funk-sql.jar
- localedata.jar
- sunjce_provider.jar
- sunpkcs11.jar

Manual Migration of JavaScript files

As of SIM Server 5.4, all JavaScript files (*.jsi) are stored in the radius/scripts subdirectory. Any JavaScript files must be migrated manually by copying them into the new Steel-Belted Radius Carrier software installation.

Manual Migration of ROOT Certificates

As of SIM Server 5.4, the storage of root certificates is managed by the Steel-Belted Radius Carrier server and the SBR Administrator is used to add and delete root certificates. You must manually migrate root certificates, using the SBR Administrator to add them from the old root directory.

Manual Migration of Dictionaries

If you have stored any modified or third-party dictionary files (*.dci, *.dcm, *.dct) in the /radius directory, you must manually migrate these either by merging each of the modifications with the corresponding files that are shipped with the new Steel-Belted Radius Carrier software, or by copying the third-party dictionary files to the new /radius directory.

5.4, 6.0, 6.1 If Release 7.0 will support WiMAX, check the vendor.ini to confirm that the WiMAX vendor ID is defined. If the field is blank, restore a file from the /install/backup/<time-stamp> directory.

5.4 If you are migrating from SIM Server 5.4, the /conf/ulcmmg.conf needs to be modified. Replace the Release 5.4 hostname with the Release 7.0 hostname.

Manual Migration of Third-Party Plug-ins and Other Binaries

If you have stored any third-party plug-ins (*.so) and/or other binaries in the radius directory, then you must manually migrate them by copying the files to the new radius directory.

Chapter 5

Removing Steel-Belted Radius Carrier Software

This chapter explains how to remove all Steel-Belted Radius Carrier Release 7.0 software from a server.

CAUTION: Do not uninstall Steel-Belted Radius Carrier if you intend to install another version of the Steel-Belted Radius Carrier software on the same server. If you remove an existing installation, you cannot migrate that data and configuration information forward to the newer version.

These topics are in the chapter:

- Uninstalling the Steel-Belted Radius Carrier Server on page 47
- Uninstalling the SBR Administrator Files on page 49

Uninstalling the Steel-Belted Radius Carrier Server

To uninstall the Steel-Belted Radius Carrier server software from its default location (/opt/JNPRsbr):

1. Log in to the Solaris server as root.

2. Stop the radius process.

   Execute:
   # **cd /opt/JNPRsbr/radius**
   # **./sbrd stop**

3. Back up your Steel-Belted Radius Carrier server directory.

   Create a new archive directory to ensure that you do not overwrite an existing backup.

   # cd /opt/JNPRsbr
   # mkdir /opt/backups
   # tar cf - radius | (cd /opt/backups; tar xfBp -)

4. Display the list of Steel-Belted Radius Carrier software packages installed on your server.

   Execute:
   # **cd /opt/JNPRsbr/radius**
   # **pkginfo |grep -i jnpr**

```
pkginfo |grep -i jnpr
application JNPRsbr      JNPRsbr - Juniper Networks Steel-Belted Radius Carrier
```

5. Initiate the software uninstall.

   Execute:
   pkgrm JNPRsbr

   Two prompts ask you to confirm that you want to remove the package. Enter **y** at each prompt to continue.

   # **pkgrm JNPRsbr**

   The following package is currently installed:

   JNPRsbr JNPRsbr - Juniper Networks Steel-Belted Radius Carrier (sparc) 7.00.4556

   Do you want to remove this package? [y,n,?,q] **y**

   ## Removing installed package instance <JNPRsbrsp>

   This package contains scripts which will be executed with super-user permission during the process of removing this package.

   Do you want to continue with the removal of this package [y,n,?,q] **y**

   After the second prompt, the uninstall displays a message, then the name of each file it removes.

```
## Verifying package <JNPRsbr> dependencies in global zone

## Processing package information.

## Executing preremove script.

Existing server directory will be backed up as:

/opt/JNPRsbr/radius/install/backups/2008:08:18-12:45:40

## Removing pathnames in class <none>
```

   When the uninstall finishes, it displays:

   Removal of <JNPRsbr> was successful.

6. In most environments, you would want to preserve the Steel-Belted Radius Carrier backup directories in case they are required by a future installation, but they may be deleted if necessary.

   If you do want to delete them, use the standard UNIX **rm** command.

For example:
cd /
rm -rf /opt/JNPRsbr

Uninstalling the SBR Administrator Files

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Solaris host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.

2. Delete the SBR Administrator directory.

   Execute:
   rm –r -f $HOME/.junipernetworks/WebDeployer

If you run the SBR Administrator after you delete the /WebDeployer directory, your browser automatically downloads the files it needs to run SBR Administrator from the target Steel-Belted Radius Carrier server.

Part 2

Signalware 9 Support for Steel-Belted Radius Carrier

This part contains chapters that describe installing and configuring Signalware 9 with Service Pack 5T on a Steel-Belted Radius Carrier server.

These chapters are included in this section:

- *Chapter 6, Installing Signalware 9*
- *Chapter 7, Configuring SS7/IP Network Communication Files*

Chapter 6

Installing Signalware 9

Steel-Belted Radius Carrier uses the Ulticom Signalware SS7 networking stack to communicate with SS7 networks. This chapter contains the basic Juniper Networks procedure that we recommend for a new Signalware 9 with Service Pack 5T Installation. The installation example provided here is for your convenience and assumes that this is a "clean" first time installation of Signalware.

These topics are in this chapter:

- Beginning the Installation on page 53
- Developing and Deploying SS7 Services on page 55
- Configuring the Platform on page 60
- Commission Instance on page 62
- Configuring Nodes on page 62
- Installing Signalware Service Pack 5T on page 65

5.4 Signalware provides a utility as part of its OLU packages to back up and save Signalware-specific configuration files. They can be copied into the new Signalware 9 environment on the Release 7.0 server, but they do require manual editing to make the appropriate changes to IP addresses, directory path names, and other entries that change from server to server.

For more complete information about installing Signalware, moving existing configuration files from another server, and re-installation of Signalware 9, refer to the *Signalware Solaris Installation Manual*.

Beginning the Installation

To install Signalware 9 with Service Pack 5T:

1. Log in as root.
2. Copy the Signalware 9 license file to the /etc directory.
   - To obtain a license file for Signalware 9, contact your Juniper Networks representative.

- To find out information about your license, enter liceManViewer at a Solaris prompt.

3. Create a UNIX group called “users” and verify that the group exists.

   To add a group, use the UNIX groupadd command.
   $ groupadd users

   To view a list of existing groups, use the UNIX cat command:
   $ cat /etc/group

4. Create a UNIX user account called “siguser” as a member of the “users” group.

5. Copy the Signalware package from its location in your download directory or from a Signalware CD to a temporary working directory (/export/local/siguser is used in the example below).

6. Start the Signalware installation.

   Execute:
   swsetup

   The script prompts for a user identifier.

7. Enter the unique user that you created in Step 3.

```
X Terminal on sbrha-4.spgma.juniper.net
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
sigusr:x:14588:65536::/export/local/sigusr:/bin/bash
bash-3.00# cd /export/local
bash-3.00# ls
apache-ant-1.5.4  builder          buildsys          lost+found        oracle
bash-3.00# mkdir -p sigusr
bash-3.00# chown sigusr:omni /export/local/sigusr/
bash-3.00# ls -ltr
total 26
drwxr-xr-x   6 Xclev    other        512 Jan 22  2007 buildsys
drwx------   2 root     root        8192 Jun  3 20:30 lost+found
drwxr-xr-x   5 Xcvistoli root         512 Jun  3 21:37 builder
drwxr-xr-x   3 root     root         512 Jun  3 21:37 oracle
drwxr-xr-x   6 root     root         512 Jun  3 21:38 apache-ant-1.5.4
drwxr-xr-x   2 sigusr   omni         512 Jun  4 10:06 sigusr
bash-3.00# su - sigusr
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
-bash-3.00$ pwd
/export/local/sigusr
-bash-3.00$ su
Password:
#
# bash
#
# cd /tmp/omni
# ./swsetup

Preparing system......

 ****************************************************************
 ***                                                          ***
 ***          Signalware Setup Utility                        ***
 ***                                                          ***
 ****************************************************************

Please Enter a unique User Identifier.
It cannot be more than 15 characters long
For example: username-extension (jdoe-1234): sigusr
```

The script prompts for a scheduling priority.

8. Press **Enter** to accept the default value of 10.

   The system checks for previous installations, a valid package file, and updates. Then it prompts for an ECN Update.

9. Enter **N**.

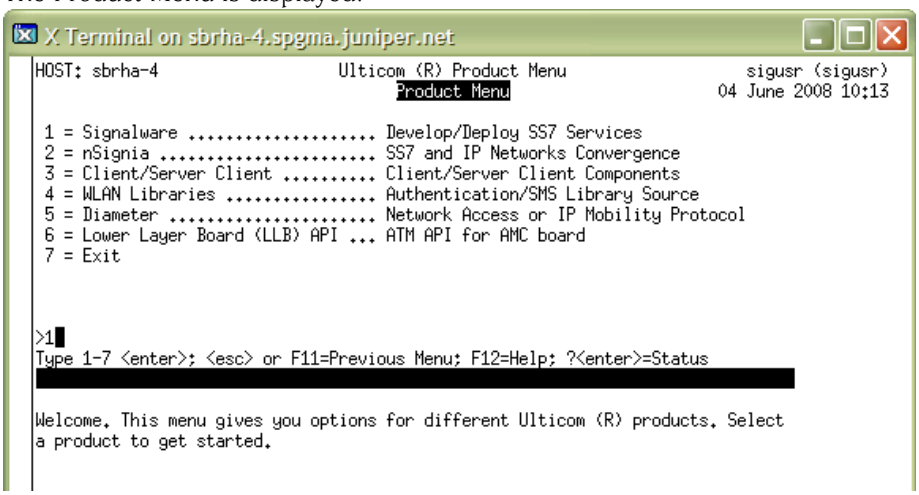
   The Main Menu screen is displayed.

Developing and Deploying SS7 Services

This group of steps installs the required software packages.

1. From the Main Menu, enter **1** to select "Signalware ... Develop/Deploy SS7 Services."

   The Product Menu is displayed.



2. Enter **1** to select Signalware.

The Signalware Main Menu is displayed.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                    Ulticom (R) Product Menu                sigusr (sigusr)
                                   Signalware Main Menu                04 June 2008 10:14

 1 = Install/Configure (Signalware is uninstalled or off-line)
 2 = Online Upgrade (Signalware is installed and running)
 3 = Installation Status and Reports
 4 = Installation Maintenance
 5 = Configuration Maintenance
 6 = Start an Installed Instance of Signalware



>1
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status

Welcome. It does not appear that Signalware has ever been installed on your
system. Select the "Install/configure" option to perform the initial
installation of Signalware. Remember, additional help for each menu is
available by typing F12 or entering "help" at the prompt.
```

3. Enter **1** to select Install/Configure.

   The Install/Configure menu is displayed.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                    Ulticom (R) Product Menu                sigusr (sigusr)
                                      Install/Configure                04 June 2008 10:14

 1 = [ ]Limit Installations to a Single Instance
 2 = [X]Allow Multiple Installation Instances of Signalware
 3 = Perform Initial Signalware Installation and Configuration
 4 = Replace Signalware (replace an existing installation with new GA)
 5 = Upgrade One of the Currently Installed Installation Instances (SP or ECN)
 6 = Clone a Currently Installed Instance and Upgrade the Clone



>3
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status

The default behavior for installation allows multiple installation instances
(Staged Installation). If you wish to restrict this behavior, please select
option 1. Re-enable staged installation by selecting option 2. To install for
the first time, select option 3. To delete and replace an existing instance,
select option 4. To upgrade an instance, select option 5. To clone and upgrade
an instance, select option 6. More detailed descriptions of these options are
available from the help menu. Remember, pressing F12 or typing "help" at any
menu will display additional help.
```

4. Enter **3** to select Perform Initial Signalware Installation.

   The script prompts for host names in a cluster.

5. Press **Enter** because this is a single node installation.

The Initial Install menu is displayed.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                    Ulticom (R) Product Menu                sigusr (sigusr)
                                      Initial Install                 04 June 2008 10:15

 1 = [ ]Install Packages
 2 = [ ]Configure Platform
 3 = [ ]Commission Instance
 4 = [ ]Configure Nodes
 5 = [ ]Start Signalware
 6 = Done


>1
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status

This path will perform the initial installation of Signalware on a clean CE.
Begin by selecting "Install Packages" to install Signalware in the directory of
your choice. Remember, entering an option number followed by -manpage or -help
will display the manpage for the corresponding command.
```

6. Enter **1** to select Install Packages.

   The Select Instance screen is displayed and the script supplies the current (default) target directory.

7. Press **Enter** to accept the default target directory or specify an alternate location and press **Enter**.

   The script asks you to confirm the location.

8. Enter **Y** to continue.

   The packages directory screen is displayed.

9. Enter the full path to the directory containing the packages.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                    Ulticom (R) Product Menu                sigusr (sigusr)
/opt/ulcm                             Package Directory               04 June 2008 10:17

Enter the directory path containing the packages to be installed. This may be a
local or network path or the mount point for a CDROM or DVD-ROM device. If the
packages to install are in more than one directory enter the first directory to
install. You will be prompted for additional directory paths after each set of
packages are installed.



>/tmp/omni
Please enter directory containing the Signalware software []:
```

The packages are validated and installed.
The Protocol Selection menu is displayed.

10. Select each protocol, in turn, that is appropriate to your location and system, and press **Enter**.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                    Ulticom (R) Product Menu                sigusr (sigusr)
/opt/ulcm                           Protocol Selection                 04 June 2008 10:17

 1 = [_] ANSI Protocol
 2 = [_] ITU Protocol
 3 = [_] CHINA Protocol
 4 = [_] JAPAN Protocol
 5 = [_] IMS (SIP)
 6 = [_] WLAN (Authentication, SMS Gateways)
 7 = [_] CLIENT SERVER



>2
1-7 to select,0=done,<esc> or F11/<enter>=Prev/Next Page
                                                                   Options 1-7 of 7

Select the protocols and features you wish to install. Entering the items
number will toggle it between the selected and deselected state.  Enter "none"
to deselect all items on this page or "all" to select all items on the page.
<ESC> will deselect all items on all pages and displays the previous menu.
<F11> will display the previous page. Pressing enter will display the next
page. If on the last page pressing enter will accept your selections and
continue.
```

After each protocol is activated, the screen is displayed again. When all protocols have been selected, type **0** and press **Enter** to continue.

The Interface Selection menu is displayed.

11. Type **1,3** to select SS7 and M3UA (SIGTRAN) because those are the interfaces supported by Steel-Belted Radius Carrier and press **Enter**.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                    Ulticom (R) Product Menu                sigusr (sigusr)
/opt/ulcm                           Interface Selection                04 June 2008 10:19

 1 = [_] SS7 (Ulticom Boards)
 2 = [_] M2PA
 3 = [X] M3UA
 4 = [_] M2UA
 5 = [_] SUA
 6 = [_] ATM



>0
1-6 to select,0=done,<esc> or F11/<enter>=Prev/Next Page
                                                                   Options 1-6 of 6

Select the interfaces you wish to install. Entering the items number will
toggle it between the selected and deselected state.  Enter "none" to deselect
all items on this page or "all" to select all items on the page.  <ESC> will
deselect all items on all pages and return to the previous menu. <F11> will
display the previous page. Pressing enter will display the next page. If on the
last page pressing enter will accept your selections and continue.
```

When the screen is redisplayed, type **0** and press **Enter** to continue.

The first page of the Select Packages menu is displayed.

12. Review the packages to be installed. (Generally, accept the defaults and do not deselect any packages.)

NOTE: The selected packages are based on the choices that you made in prior screens. We recommend that you do not deselect any packages.

13. Type **0** and press **Enter** to accept the default selections and continue.

    A confirmation screen is displayed.

14. Enter **Y** to confirm the selection of all packages and install them.

    Status messages are displayed as the packages are installed.

15. When “Installation Complete” is displayed, press **Enter** to continue.

    The More Packages screen is displayed, and you are prompted to indicate whether you are through installing packages.

16. Enter **Y**.

    The Initial Install screen is displayed.

Configuring the Platform

This group of steps configures the platform.

1. From the Initial Install screen, enter **2** to select Configure Platform.

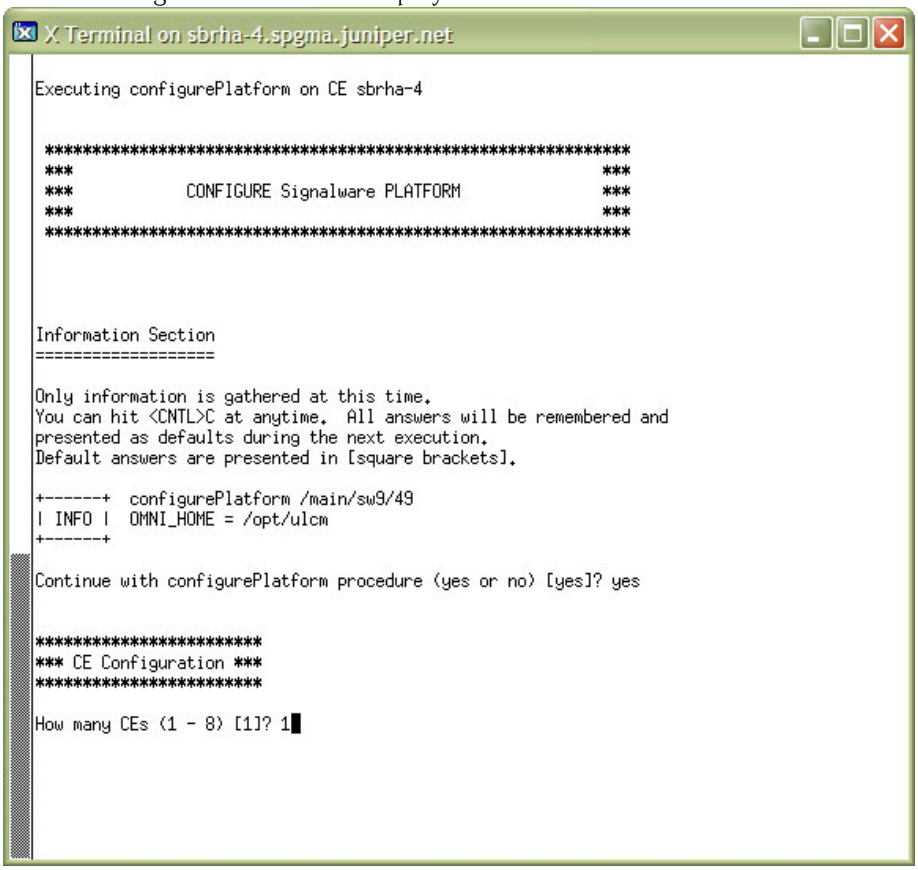
   The Configure Platform screen is displayed.

2. Enter **0** to accept the install directory that you entered earlier.

   The Information Section screen is displayed.

3. Press Enter to accept the default "Yes" to answer the Continue with configurePlatform procedure? prompt.

   The CE Configuration screen is displayed.



4. Enter **1**. (No other entry is supported.)

The UDP/TCP Port Configuration screen is displayed. It prompts you for a UDP port value.

```
X Terminal on sbrha-4.spgma.juniper.net
You can hit <CNTL>C at anytime.  All answers will be remembered and
presented as defaults during the next execution.
Default answers are presented in [square brackets].

+-------+  configurePlatform /main/sw9/49
| INFO |  OMNI_HOME = /opt/ulcm
+-------+

Continue with configurePlatform procedure (yes or no) [yes]? yes


************************
*** CE Configuration ***
************************

How many CEs (1 - 8) [1]? 1


Choose a UDP port base value.  This value will serve as the base
for a block of UDP ports used by Signalware and will be stored
in the /etc/services file (sw_df, sw_mr).  This value must be
identical on all CEs.  The block of ports used will begin with
this base number and end with (base number + 5 + (SHM * 4)).
Ensure that no other services will use UDP ports in this range.
+-------+
| INFO |  CE name is sbrha-4
+-------+


No SS7 boards are installed.




**********************************
*** UDP/TCP Port Configuration ***
**********************************

Signalware UDP port base value (1025 - 65535) [39000]?
```

5. We recommend that you press **Enter** to accept the default UDP port base value, but you may enter an alternate.

   The UDP/TCP Port Configuration screen prompts you for a TCP port value.

6. We recommend that you press **Enter** to accept the default TCP port base value, but you may enter an alternate.

   A confirmation screen prompts to apply the configuration.

   Press **Enter** to accept **yes**, the default.

   A “configurePlatform completed successfully” message is displayed.

7. Press **Enter**.

   The Initial Install Screen is displayed.

Commission Instance

This set of steps installs drivers and configures the Signalware daemons.

1. From the Initial Install screen, enter **3** to select Commission Instance.

   The Commission Instance screen is displayed, showing your install directory.

2. Enter **0** to accept the install directory that you entered earlier.

   Status messages are displayed as the system is commissioned, then a "commission completed Successfully" message is displayed.

3. Press **Enter**.

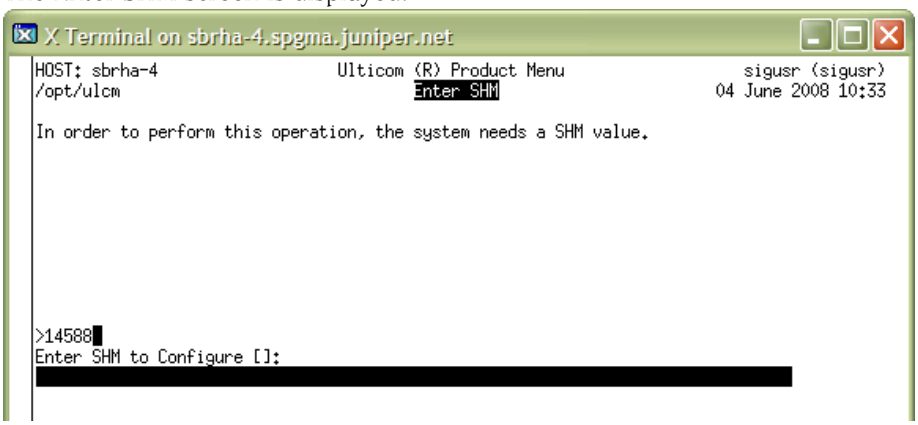
   The Initial Install screen is displayed.

Configuring Nodes

This set of steps configures local nodes.

1. From the Initial Install screen, enter **4** to select Configure Nodes.

   The Enter SHM screen is displayed.



2. Enter the shared memory value based on the user ID of the “siguser” user that you created earlier (in “Create a UNIX user account called “siguser” as a member of the “users” group.” on page 54).

   To determine the user ID, open a new window and **cat** the */etc/passwd* file as in this illustration:

```
X Terminal on sbrha-4.spgma.juniper.net
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
# bash
bash-3.00#
bash-3.00#
bash-3.00# cat /etc/passwd
root:x:0:0:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
smmsp:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
sigusr:x:14588:65536::/export/local/sigusr:/bin/bash
bash-3.00#
```

   The returned uid of 14583 is the value to enter in the Enter SHM screen.

   The Signalware User screen is displayed.

3. Enter the username for running Signalware, **siguser**.

   The Configure Nodes screen is displayed with the previously entered values in place.

```
X Terminal on sbrha-4.spgma.juniper.net
HOST: sbrha-4                Ulticom (R) Product Menu              sigusr (sigusr)
/opt/ulcm                         Configure Nodes              04 June 2008 10:34

 1: Instance Install Directory.......: /opt/ulcm
 2: Shared Memory....................: 14588
 3: Username.........................: sigusr

>0
Type Line Number to Change; Done=0 [0]

You are about to execute configureNodes on an instance. Please verify the above
values are correct. To correct a value, enter its line number. Enter 0 when
done. <Esc> or <F11> to abort the command.
```

4. Enter **0** to accept the values.

   The How Many Nodes screen is displayed.

5. We recommend that you accept the default value of 1.

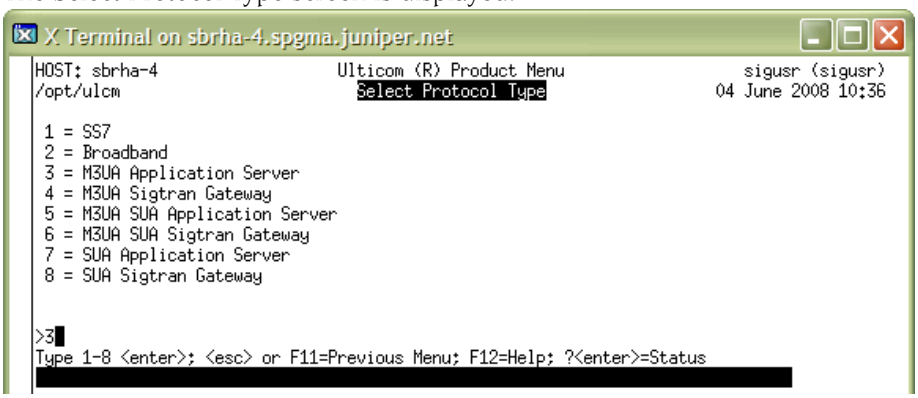
The Enter Node Name screen is displayed.

6. Enter the name of the node.

   The Select Protocol screen is displayed.

7. Enter the protocol for the node.

   The Select Protocol Type screen is displayed.



8. Enter the protocol type for the node. Choose **1** for SS7, **3** for SIGTRAN, or **1,3** for both.

   The Select Options screen is displayed.

9. For most installations, enter **0** to continue.

   Status messages are displayed as the node is configured.

10. The “Configure Nodes completed successfully” message is displayed.

    The Initial Install screen is displayed.

11. Enter **6** to exit from the installation process without starting Signalware. (Do not start Signalware at this point.)

    The Install/Configure menu is displayed.

12. Return to the Main Menu and press **7** to exit.

A “You are about to exit...” confirmation message is displayed.

13. Enter N to exit from the installation process. (You want to exit at this point. You will start Signalware later.)

    A status message is displayed as the program shuts down, then the system prompt returns.

Installing Signalware Service Pack 5T

Installing Service Pack 5T builds on the example of a default Signalware 9 installation earlier in this chapter.

This patch installation example uses the same user (siguser) and user group (users) information and assumes that you have performed the base installation and configuration procedures documented earlier in this chapter.

Installing the Patch Package

To add Service Pack 5T to a Signalware 9 installation:

1. Log in as root.

2. If you have not done so already, download and unpack the Signalware 9 Service Pack 5T file (SIGNALWARE_9_SP5.T_SOLARIS10_UPGRADE.TGZ).

3. Copy the Signalware Service Pack 5T package file from its location in your download directory or from a Signalware CD to a temporary working directory (/tmp/omni/5T is used in the example below).

4. If Signalware is running, shut it down.

5. Start the Signalware installation.

   Execute:
   swsetup

   The script prompts for a user identifier.

6. Enter the unique user that you created in the initial installation: **siguser**.

   The Main Menu screen is displayed.

```
Welcome. This menu gives you options for different Ulticom (R) products. Select
a product to get started.

HOST: mercury                Ulticom (R) Product Menu                    sigusr (uid=0(root)
gid=0(root))
                               Signalware Main Menu                              04 September 2008
18:15

 1 = Install/Configure (Signalware is uninstalled or off-line)
 2 = Online Upgrade (Signalware is installed and running)
 3 = Installation Status and Reports
 4 = Installation Maintenance
 5 = Configuration Maintenance
```

```
 6 = Start an Installed Instance of Signalware



>
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

7. Enter **1** to install the patch.

   The Install/Configure screen is displayed.

```
Welcome. Signalware 9.02 or greater has been installed on your system. All menu
options are available to you. Select an option to get started. Remember,
additional help for each menu is available by typing F12 or entering "help" at
the prompt.

HOST: mercury                 Ulticom (R) Product Menu                    sigusr (uid=0(root)
gid=0(root))
                                 Install/Configure                                 04 September 2008
18:15

 1 = [ ]Limit Installations to a Single Instance
 2 = [X]Allow Multiple Installation Instances of Signalware
 3 = Perform Initial Signalware Installation and Configuration
 4 = Replace Signalware (replace an existing installation with new GA)
 5 = Upgrade One of the Currently Installed Installation Instances (SP or ECN)
 6 = Clone a Currently Installed Instance and Upgrade the Clone



>
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

8. Enter **5** to select the Signalware installation that requires the patch.

   The Product Menu screen is displayed.
   If you are working on a system with the default configuration, only one installation is listed.

```
The default behavior for installation allows multiple installation instances
(Staged Installation). If you wish to restrict this behavior, please select
option 1. Re-enable staged installation by selecting option 2. To install for
the first time, select option 3. To delete and replace an existing instance,
select option 4. To upgrade an instance, select option 5. To clone and upgrade
an instance, select option 6. More detailed descriptions of these options are
available from the help menu. Remember, pressing F12 or typing "help" at any
menu will display additional help.

HOST: mercury                 Ulticom (R) Product Menu
sigusr (uid=0(root) gid=0(root))
Select Instance to Upgrade                            04 September 2008 18:16

 1 = (C) /opt/ulcm


>
Type 1-1 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

9. Enter **1** to select the location of the Signalware 9 installation.

The Upgrade Instance screen is displayed.

```
Select the instance to upgrade.
"(C)" indicates the instance is commissioned while "(D)" indicates
it is decommissioned or was never commissioned.
Please note, if you select the currently running instance, (i.e. the
commissioned instance), you will be asked to terminate Signalware
before installing the packages.

HOST: mercury                Ulticom (R) Product Menu                    sigusr (uid=0(root)
gid=0(root))
/opt/ulcm                        Upgrade Instance                                04 September 2008
18:16

 1 = [ ]Install Packages
 2 = [ ]Configure Platform
 3 = [ ]Commission Instance
 4 = [ ]Configure Nodes
 5 = [ ]Start Signalware
 6 = Done


>
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

10. Enter **1** to install the package.

    The Package Directory screen is displayed.

```
This path will perform an offline upgrade of an existing instance. Begin by
selecting "Install Packages" to install Signalware in the directory of your
choice. Remember, entering an option number followed by -manpage or -help will
display the manpage for the corresponding command.

HOST: mercury                Ulticom (R) Product Menu                    sigusr (uid=0(root)
gid=0(root))
/opt/ulcm                       Package Directory                                04 September 2008
18:16

Enter the directory path containing the packages to be installed. This may be a
local or network path or the mount point for a CDROM or DVD-ROM device. If the
packages to install are in more than one directory enter the first directory to
install. You will be prompted for additional directory paths after each set of
packages are installed.




>/tmp/omni/5T
Please enter directory containing the Signalware software []:
```

11. Enter the path to the patch package file. In the screen above, /tmp/omni/5T is shown as the location.

    The Upgrade Instance screen is displayed after the patch is applied.

```
HOST: mercury           Ulticom (R) Product Menu                    sigusr (uid=0(root) gid=0(root))
/opt/ulcm                        Upgrade Instance                                04 September 2008
18:17
```

```
 1 = [X]Install Packages
 2 = [ ]Configure Platform
 3 = [ ]Commission Instance
 4 = [ ]Configure Nodes
 5 = [ ]Start Signalware
 6 = Done




>
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

At this point, the patch has been applied. When you restart Signalware, the existing configuration is invoked. Check both the Signalware and Steel-Belted Radius Carrier log entries to ensure that everything is working properly.

12. Enter **6 -override** (this is not a choice on the menu) to exit.

    The Install/Configure screen is displayed.

```
>6 -override
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status


You have completed the Configure Nodes step. Signalware is now ready to run on this CE. To start
Signalware, select the "Start Signalware" option. You will need to specify where the Signalware output
is to be displayed. The output may be displayed in a new xterm by supplying a display value, to an
existing xterm or the console by supplying the device file (ex. /dev/console) or to a file by supplying
the file name.

HOST: mercury           Ulticom (R) Product Menu                    sigusr (uid=0(root) gid=0(root))
                                  Install/Configure                         04 September 2008 18:33

 1 = [ ]Limit Installations to a Single Instance
 2 = [X]Allow Multiple Installation Instances of Signalware
 3 = Perform Initial Signalware Installation and Configuration
 4 = Replace Signalware (replace an existing installation with new GA)
 5 = Upgrade One of the Currently Installed Installation Instances (SP or ECN)
 6 = Clone a Currently Installed Instance and Upgrade the Clone




>Press Key "F11"
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

13. Press **F11**.

    The Main Menu screen is displayed.

```
The default behavior for installation allows multiple installation instances (Staged Installation). If
you wish to restrict this behavior, please select option 1. Re-enable staged installation by selecting
option 2. To install for the first time, select option 3. To delete and replace an existing instance,
select option 4. To upgrade an instance, select option 5. To clone and upgrade an instance, select
option 6. More detailed descriptions of these options are available from the help menu. Remember,
pressing F12 or typing "help" at any
menu will display additional help.
```

```
HOST: mercury                        Ulticom (R) Product Menu          sigusr (uid=0(root) gid=0(root))
                                     Signalware Main Menu                       04 September 2008 18:34

 1 = Install/Configure (Signalware is uninstalled or off-line)
 2 = Online Upgrade (Signalware is installed and running)
 3 = Installation Status and Reports
 4 = Installation Maintenance
 5 = Configuration Maintenance
 6 = Start an Installed Instance of Signalware



>Press Key "F11"
Type 1-6 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

14. Press **F11**.

    The Product Menu screen is displayed.

```
Welcome. Signalware 9.02 or greater has been installed on your system. All menu options are available
to you. Select an option to get started. Remember, additional help for each menu is available by typing
F12 or entering "help" at the prompt.

HOST: mercury              Ulticom (R) Product Menu                    sigusr (uid=0(root) gid=0(root))
                           Product Menu                                         04 September 2008 18:34

 1 = Signalware .................... Develop/Deploy SS7 Services
 2 = nSignia ....................... SS7 and IP Networks Convergence
 3 = Client/Server Client .......... Client/Server Client Components
 4 = WLAN Libraries ................ Authentication/SMS Library Source
 5 = Diameter ...................... Network Access or IP Mobility Protocol
 6 = Lower Layer Board (LLB) API ... ATM API for AMC board
 7 = Exit



>7
Type 1-7 <enter>; <esc> or F11=Previous Menu; F12=Help; ?<enter>=Status
```

15. Enter **7**.

    The Product Menu screen is displayed.

```
Welcome. This menu gives you options for different Ulticom (R) products. Select a product to get
started.

HOST: mercury              Ulticom (R) Product Menu                    sigusr (uid=0(root) gid=0(root))
                           Product Menu                                         04 September 2008 18:34

You are about to exit the Signalware Menu System. Are you sure you want to exit?  To continue using the
menu system enter Y.  To exit enter N.
```

```
>
```

16. Enter **N**.

    A confirmation prompt is displayed.

```
Would you like to continue the Signalware Menu System? (Y/N)[Y]:
```

17. Press Enter to exit.

Chapter 7

Configuring SS7/IP Network Communication Files

This chapter discusses configuring Signalware to communicate across SS7 gateways and configuring SIGTRAN (provided as a module of Signalware) to allow SS7 communication over IP networks. These topics are included in this chapter:

- Configuring Communication Files Overview on page 71
- Communication Pathways and Corresponding Files on page 72
- Configuration Activities on page 73
- Signalware MML Commands on page 73
- Defining Links, Link Sets, and Route Sets on page 74
- Configuring the authGateway Application for HLR Communication on page 76
- Loading the MML Configuration Settings on page 83
- SS7 Sample Configuration Files on page 83

Configuring Communication Files Overview

NOTE: Configuring the SS7/IP Network communication is common to both the SIM and SMS authentication module. This release of Steel-Belted Radius Carrier supports only the SIM authentication module.

When configuring the communication pathways between Steel-Belted Radius Carrier and equipment in the SS7 network, you need to configure certain files based on your choices of the following:

- Type of network equipment Steel-Belted Radius Carrier communicates with for processing authorization requests. (See Table 8 for information of which type of equipment is used.)
  - HLR
- Type of network.

- SS7
- SS7 over IP (SIGTRAN)

Table 8: Network Equipment Used for Authorization

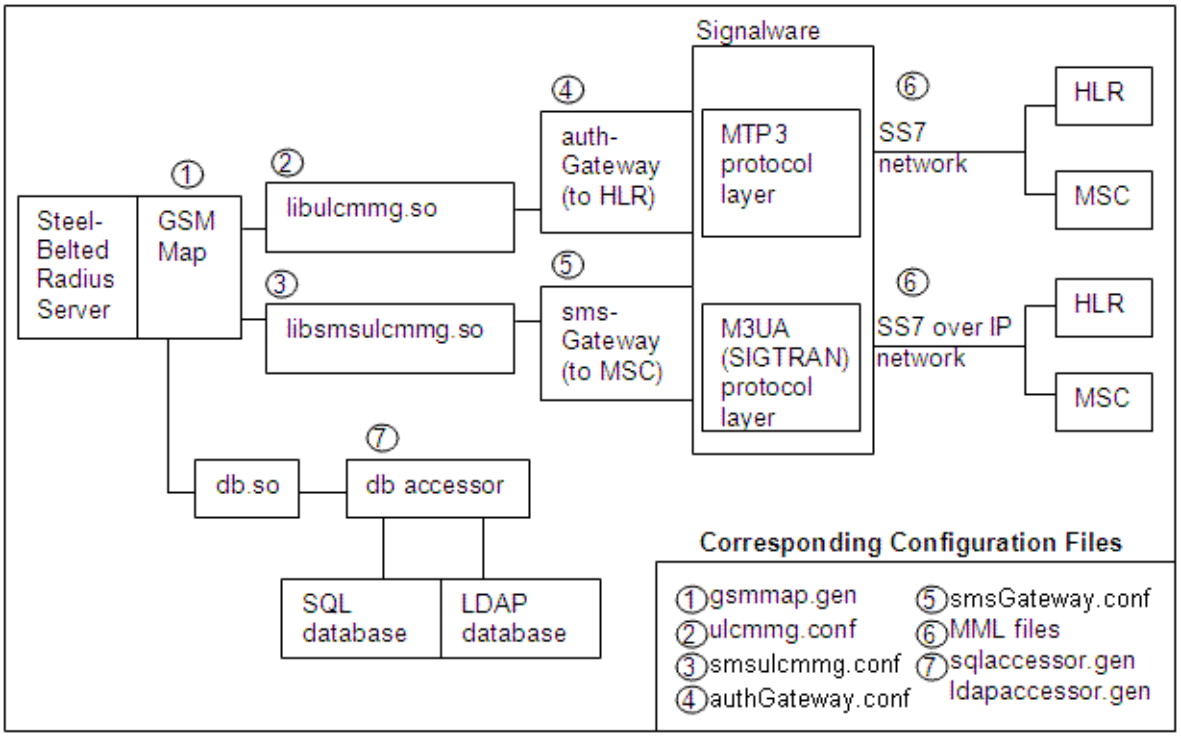
Action Needed to Process Access-Request	Network Equipment
Obtain SIM triplets	HLR
Obtain AKA quintets	HLR
Obtain IMSI (given the MSISDN)	HLR
Obtain MSISDN (given the IMSI)	HLR
Obtain Authorization string	HLR or database

NOTE: If quintets are received but triplets are needed, then Steel-Belted Radius Carrier converts the quintets to triplets according to specification 3G TS 33.102, available at http://www.3gpp.org.

Communication Pathways and Corresponding Files

Figure 4 shows the communication pathways between the Steel-Belted Radius Carrier server and the network equipment. It also lists the files that need to be configured for each segment in the communication pathways.

Figure 4: Steel-Belted Radius Carrier Libraries and Corresponding Configuration Files



NOTE: Figure 4 shows the corresponding files for both the SIM authentication module and the SMS authentication module (smsGateway). This release supports only the SIM authentication module.

Configuration Activities

To configure the communication pathways, perform the following activities.

1. Install Signalware. For details on the recommended procedure to install and run Signalware 9, see *Chapter 6, Installing Signalware 9*.
2. Define links, link sets, and route sets with MML commands for SS7 or SIGTRAN. See Defining Links, Link Sets, and Route Sets on page 74.
3. Configure the authGateway application for HLR communication. See Configuring the authGateway Application for HLR Communication on page 76.
4. Load the MML configuration settings. See Loading the MML Configuration Settings on page 83.
5. Start Signalware.

Signalware MML Commands

After Signalware is installed, you can configure and provision Signalware using commands sent to the Signalware system. For details about installing and running Signalware see *Chapter 6, Installing Signalware 9*.

These commands are in a format called MML (Man-Machine Language). You can input MML commands individually using the SWMML program, or save them in a file. The procedures in this chapter assume that you save the MML commands to .mml text files and execute them as described in Loading the MML Configuration Settings on page 83.

The basic activities that require MML commands are:

- Setting up link sets, links, and routes — See Defining Links, Link Sets, and Route Sets on page 74.
- Configuring the authGateway location and startup information — See Configuring the authGateway Application for HLR Communication on page 76.
- Loading the MML configuration settings — See Loading the MML Configuration Settings on page 83.

You can view a list of all MML commands and definitions by entering:
$ man MML_Intro

You can view specific information about any MML command by typing man *cmdname*. For example:
$ man CRTE-LSET

Defining Links, Link Sets, and Route Sets

Links identify point-to-point connections of an adjacent node. Link sets are sets of parallel links that can be used for load sharing. Routes identify the final node destination. (The order in which they are defined is important.) Figure 5 on page 75 provides a simple example of links, link sets, and route sets. In the case of a SIGTRAN installation, the link set most likely consists of a single link because redundancy might not be needed.

You use MML commands to set up links, link sets, and routes to identify the path between Steel-Belted Radius Carrier, the adjacent link, and the final destination (HLR).

Setting up links, link sets, and route sets involves the MML commands listed in Table 9. For more information about the syntax and usage of the MML commands, see Signalware MML Commands on page 73.

Table 9: MML Commands for Defining Links, Link Sets, and Route Sets

Action	MML Command for SS7 Networks	MML Command for SIGTRAN Networks
Identify the local point code and network indicator (NI)	CRTE-OSPC	CRTE-OSPC
Create a link set and assign it a point code	CRTE-LSET	CREATE-M3UA-LSET
Create one or more links that belong to the link set	CRTE-SLK	CREATE-M3UA-SLK
Create a route set that identifies the final destination	CRTE-RSET	CRTE-M3UA-RKEY
Allow the route set to be used	ALW-RSET	ALW-RSET
Activate the links	ACTV-SLK	ACTV-SLK

Example MML Commands

The examples in this section illustrate the MML commands used to create links, link sets, and route sets.

Figure 5: Links, Link Sets, and Route Sets

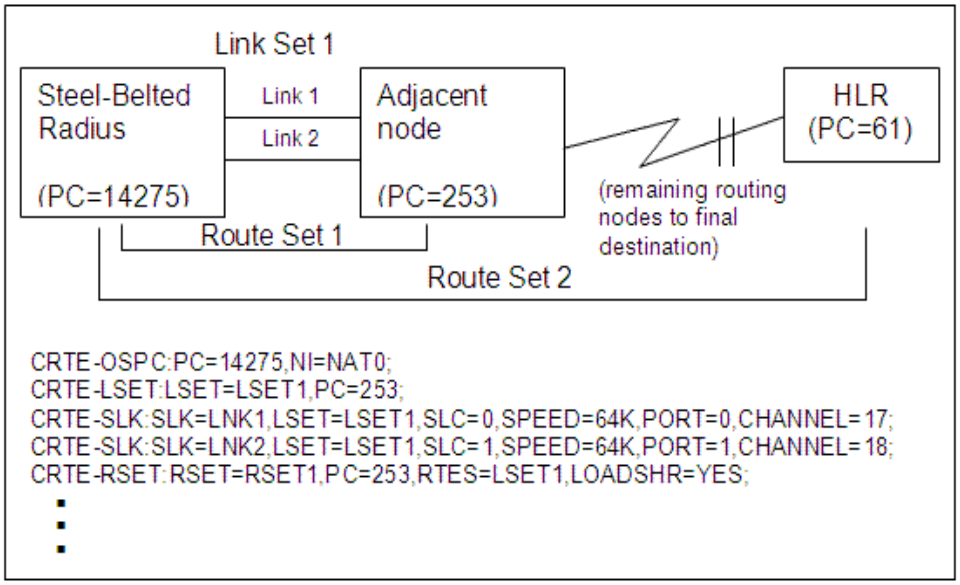
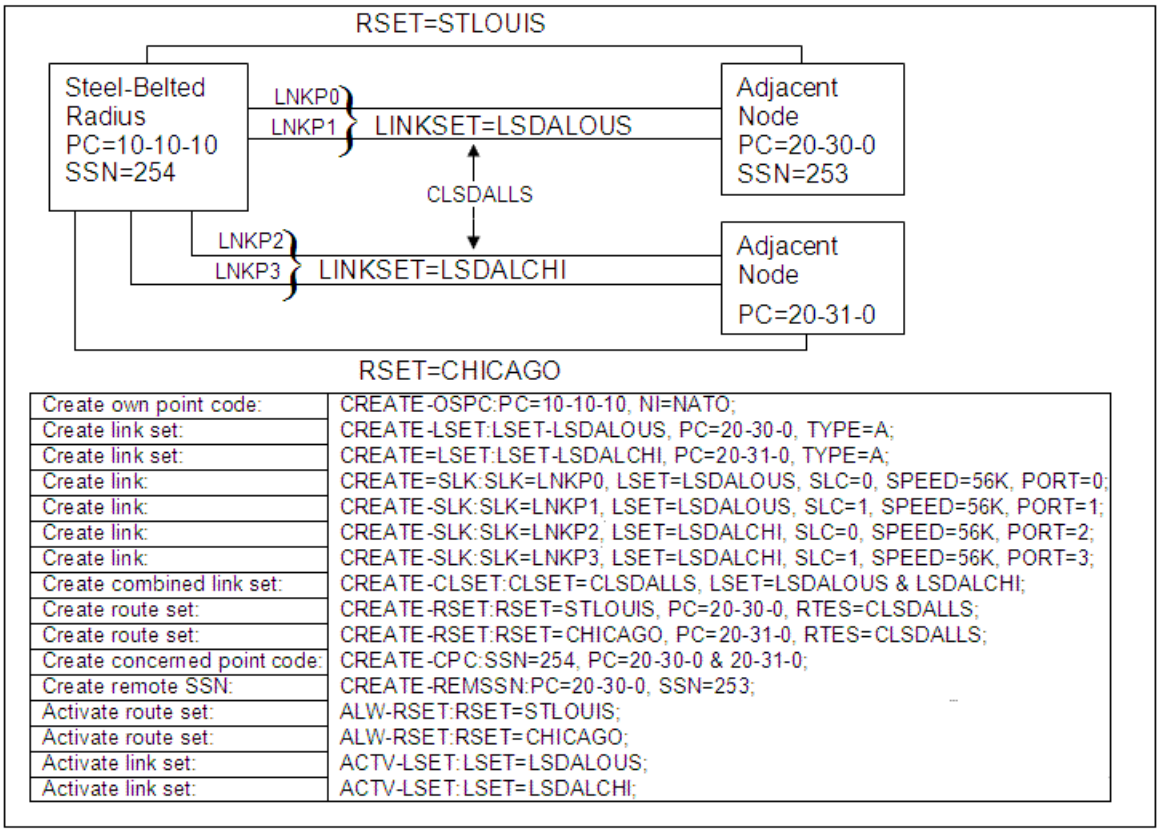


Figure 6: MML Provisioning



Create own point code:	CREATE-OSPC:PC=10-10-10, NI=NATO;
Create link set:	CREATE-LSET:LSET-LSDALOUS, PC=20-30-0, TYPE=A;
Create link set:	CREATE=LSET:LSET-LSDALCHI, PC=20-31-0, TYPE=A;
Create link:	CREATE=SLK:SLK=LNKP0, LSET=LSDALOUS, SLC=0, SPEED=56K, PORT=0;
Create link:	CREATE-SLK:SLK=LNKP1, LSET=LSDALOUS, SLC=1, SPEED=56K, PORT=1;
Create link:	CREATE-SLK:SLK=LNKP2, LSET=LSDALCHI, SLC=0, SPEED=56K, PORT=2;
Create link:	CREATE-SLK:SLK=LNKP3, LSET=LSDALCHI, SLC=1, SPEED=56K, PORT=3;
Create combined link set:	CREATE-CLSET:CLSET=CLSDALLS, LSET=LSDALOUS & LSDALCHI;
Create route set:	CREATE-RSET:RSET=STLOUIS, PC=20-30-0, RTES=CLSDALLS;
Create route set:	CREATE-RSET:RSET=CHICAGO, PC=20-31-0, RTES=CLSDALLS;
Create concerned point code:	CREATE-CPC:SSN=254, PC=20-30-0 & 20-31-0;
Create remote SSN:	CREATE-REMSSN:PC=20-30-0, SSN=253;
Activate route set:	ALW-RSET:RSET=STLOUIS;
Activate route set:	ALW-RSET:RSET=CHICAGO;
Activate link set:	ACTV-LSET:LSET=LSDALOUS;
Activate link set:	ACTV-LSET:LSET=LSDALCHI;

SS7 Example: Creating Links, Link Sets, and Route Sets

```
CRTE-OSPC:PC=14275,NI=NAT0;
CRTE-LSET:LSET=LSET1,PC=253;
CRTE-SLK:SLK=LNK1,LSET=LSET1,SLC=0,SPEED=64K,PORT=0,CHANNEL=17
CRTE-RSET:RSET=RSET1,PC=253,RTES=LSET1,LOADSHR=YES;
CRTE-RSET:RSET=RSET2,PC=61,RTES=LSET1,LOADSHR=YES;
ALW-RSET:RSET=RSET1;
ALW-RSET:RSET=RSET2;
ACTV-SLK:SLK=LNK1;
```

SIGTRAN Example: Creating Links, Link Sets, and Route Sets

```
CREATE-OSPC:PC=4004,NI=INT0;
CREATE-M3UA-LSET:LSET=IPLSET,TYPE=IPSP-IPSP, RADDR=207.46.20.60,PC=5005;
CREATE-M3UA-SLK:SLK=IPSLK,LSET=IPLSET,LADDR=72.5.124.61,RADDR=207.46.20
.60,MODE=CONNECT,LPORT=2906;
ACTIVATE-M3UA-SLK:SLK=IPSLK;

CREATE-RSET:RSET=IPRSET,PC=5005,RTES=IPLSET;
ALLOW-RSET:RSET=IPRSET;

CREATE-M3UA-RKEY:RKEY=RK1,TYPE=STATIC-AS,TRAFFIC-MODE=LOADSHARE,LSET=IP
LSET,DPC=4004,SI=SCCP,SSN=1&251&252;
ACTIVATE-M3UA-RKEY:RKEY=RK1;
```

Configuring the authGateway Application for HLR Communication

The authGateway application manages all communication between Steel-Belted Radius Carrier and the HLR. The authGateway application also implements the MAP (Mobile Application Port) protocol and MAP messages that get sent through the Signalware protocol stack and out to the HLR and back.

Configuration of the authGateway application requires the activities described in the following sections of this chapter:

- Configuring the authGateway Routing Location Information on page 76
- Configuring the authGateway.conf File on page 77
- Configuring the authGateway Startup Information on page 80
- Configuring the ulcmmg.conf File on page 82

Configuring the authGateway Routing Location Information

This activity assigns the local routing options and the remote routing options using the MML commands listed in Table 10.

Table 10: MML Commands for Configuring authGateway Routing Location

MML Command	Description
CREATE-CPC	Identify the concerned point code (CPC), which is the destination point code and the local application (authGateway).

Table 10: MML Commands for Configuring authGateway Routing Location (continued)

MML Command	Description
CREATE-REMSSN	Identify the point code of the HLR and the remote application.
CREATE-GT	Create a global title translation for the remote HLR (if Global Title routing is used).

For more information about the syntax and usage of the MML commands, see Signalware MML Commands on page 73.

Example 1 — Global Title Routing Using Global Title Identification

In the following example, these actions take place:

Line 1 (CREATE-GT): Global Title type translation is used so that digits 22201 are sent to PC,SSN = 61,6. RI = GT tells 61,6 that it needs to find the next routing hop for the request.

```
CREATE-GT:TT=0,NP=ISDN-MOB,NA=INT,DIG="22201",PC=61,SSN=6,RI=GT;
```

Example 2 — PCSSN Routing Using Point Code Identification

In the following example, these actions take place:

Line 1 (CREATE-CPC): authGateway is assigned a subsystem number (SSN) of 7 on the local host and the concerned point code on the HLR is identified as 61.

Line 2 (CREATE-REMSSN): The subsystem number (application) on the remote host is identified as 6.

Line 3 (CREATE-GT): Global Title type translation is used so that digits 22201 are sent to PC,SSN = 61,6. RI = PCSSN indicates that digits 22201 are handled by PC,SSN = 61,6.

```
CREATE-CPC:PC=61,SSN=7;
CREATE-REMSSN:PC=61,SSN=6;
CREATE-GT:TT=0,NP=ISDN-MOB,NA=INT,DIG="22201",PC=61,SSN=6,RI=PCSSN;
```

NOTE: MML commands are saved in MML files, which can be loaded into Signalware. See Loading the MML Configuration Settings on page 83.

Configuring the authGateway.conf File

The authGateway.conf file specifies the remote routing and authorization options for the authGateway application.

- Remote routing options control how the remote HLR is addressed based on the incoming IMSI.
- Authorization options control whether or not a subscriber requesting an account is authorized for WLAN access, and which Steel-Belted Radius Carrier profile or native user is used.

Remote Routing Options

Each line in the authGateway.conf file represents a target HLR, where each HLR has its own routing options and authorization options. Indicate each HLR listed in this file with the initial digits of the subscriber password, specified by the odigits option.

Table 11 lists the remote routing options for the authGateway.conf file.

Table 11: authGateway.conf Remote Routing Options

Option	Purpose
bs	Bearer Service. See Authorization Options on page 79.
msisdn	The msisdn option can be used in place of ndigits and odigits when no translation is required. See Example 2 — authGateway.conf file on page 80.
ndigits	Replacement digits for numbering plan translation (hybrid IMSI).
odb	Operator-Determined Barring. See Authorization Options on page 79.
odigits	Initial digits of IMSI or password for this HLR. For each request, the first digits of the IMSI are compared with odigits. The first line of the configuration file that matches is selected for the current request. If the routing indicator (rri) is 0 (Global Title), the leading digits are replaced with the new digits (ndigits) to perform the numbering plan translation. Example of direct replacement: If the rule is “odigits 12345 ndigits 98765” and the IMSI is 123456789012345, the resulting digits are 987656789012345. Example of wildcard replacement: If the rule is “odigits 12345* ndigits 98765” and the IMSI is 123456789012345, the resulting digits are 98765.
rgti	(Global Title only) GTI value. 4 for C7; 2 for A7. (Usually 4.)
rnai	(Global Title only) Nature of Address Indicator.
rnp	(Global Title only) Numbering Plan. Acceptable values are: 1 — ISDN/Telephony 3 — DATA 4 — TELEX 5 — Maritime Mobile 6 — Land/Mobile 7 — ISDN/Mobile 10 — British Telecom special 1 11 — British Telecom special 2 14 — Private Network
rpc	Remote Point Code. Point Code of HLR.
rri	Routing indicator - 0 for GT (Global Title), 1 for PC/SSN (Point Code/Subsystem Number).
rssn	Subsystem Number of HLR.
rtt	(Global Title only) Translation Type (usually 0).
ts	Teleservice. See Authorization Options on page 79.

Authorization Options

The HLR database includes authorization information that is assigned to each subscriber. Three authorization designations are relevant to Steel-Belted Radius Carrier with the SIM authentication module:

- BS (Bearer Service)
- TS (Teleservice)
- ODB (Operator-Determined Barring)

You can specify subscriber HLR authorization (and barred service) designations in the MAP Gateway authGateway.conf file.

NOTE: You can disable authorization completely from EAP-SIM (not fetch subscriber profile information from the HLR and not perform a SQL/LDAP query). For instructions about disabling authorization, see Disabling Authorization from EAP-SIM in *Chapter 18, Configuring SIM Authentication*, *Steel-Belted Radius Carrier Reference Guide*.

Each line in the authGateway.conf file corresponds to an HLR in your network. Each line also specifies all potential authorization (and barred service) settings for any subscribers on this HLR.

Steel-Belted Radius Carrier with the SIM authentication module uses the service authorization information that you list for each HLR in authGateway.conf:

- When a TS or BS designation is assigned to a subscriber entry in the HLR database, Steel-Belted Radius Carrier with the SIM authentication module permits the subscriber the designated class of WLAN service upon authorization request.
- When an ODB designation is assigned to a subscriber, Steel-Belted Radius Carrier with the SIM authentication module denies the subscriber WLAN service upon authorization request.
- When you do not specify service designations for a HLR listed in authGateway.conf, then all subscribers on that HLR are authorized for WLAN service.
- You can specify up to six authorization strings of each type (TS, BS, or ODB) on any given line of authGateway.conf.

You can specify the service designations in authGateway.conf:

```
bs  n1:auth1
ts  n2:auth2
odb n3:auth3
```

Here, *ni* (i=1,2,3) is a decimal integer that specifies the setting, and *authi* (i=1,2,3) is the string returned from the MAP Gateway to Steel-Belted Radius Carrier with the SIM authentication module.

For example, you might specify the potential subscriber designations on one HLR with the following text in authGateway.conf:

bs 26:B1A ts 33:TS21 odb 128:bar

NOTE: If you require any HLR authorization strings to define different classes of service for your subscribers, you must also specify those TS, BS, and ODB authorization strings in certain files associated with the SIM authentication module. For information on how to match these strings to Steel-Belted Radius Carrier variables, see the [ProfileMap] section in *Chapter 21, Configuring EAP-SIM and EAP-AKA Authentication*, *Steel-Belted Radius Carrier Reference Guide.*

Example 1 — authGateway.conf file

(Note: Lines are wrapped.)

odigits 2310 ndigits 2324 rnai 4 rnp 7 rgti 4 rtt 0 rri 0 rpc 3003 rssn 251 bs 12:gold bs 23:silver ts 91:bronze ts 92:red ts 93:green odb 1:black aqua

odigits 31026 ndigits 32476 rnai 4 rnp 7 rgti 4 rtt 0 rri 1 rpc 3003 rssn 253 bs 23:morning bs 24:afternoon ts 1:night

Example 2 — authGateway.conf file

(Note: Lines are wrapped.)

In this global title example, odigits and ndigits are the same and do not require translation. You can use the msisdn option in place of ndigits and odigits when no translation is required.

msisdn 31026 rnai 4 rnp 7 rgti 4 rtt 0 rri 0 rpc 3003 rssn 251 bs 12:gold bs 23:silver ts 91:bronze ts 92:red ts 93:green odb 1:black aqua

Configuring the authGateway Startup Information

The CREATE-PROCESS and START-PROCESS MML commands start the authGateway (by calling authGatway.conf), using options that you specify.

Table 12 describes the MML commands needed to configure and start authGateway.

Table 12: MML Commands for Configuring the Start of authGateway

MML Command	Description
CREATE-PROCESS	Identify the authGateway configuration file and the authGateway options.
START-PROCESS	Start the process.

For more information about the syntax and usage of the MML commands, see Signalware MML Commands on page 73. See Loading the MML Configuration Settings on page 83 for information about executing the MML commands.

Table 13 lists the options that you can use with the CREATE-PROCESS command.

Table 13: authGateway Process Options Used with CREATE-PROCESS

Option	Description
appctx	MAP protocol revision (2 or 3).
conf	Path and name of the authGateway configuration file. The default file is OMNI_HOME/conf/authGateway.conf.
debug	Sets a debug level. Use the following: -debug 0xff
host	Local hostname.
invkretry	Number of invoke retry.
invktimeout	Duration of invoke timeout in seconds.
lgti	(Global Title only) Local GTI value, usually 4 for C7 and 2 for A7.
lmsisdn	(Global Title only) MSISDN of this local node.
lnai	(GT only) Nature of Address Indicator. Indicates the scope of the address value, such as whether it is an international number (includes country code) or a national number (no country code). 1 Subscriber Number — no area code (example: 5551234 2 unused 3 National Significant Number — no country code (example: 2015551234) 4 International Number — includes country code (example: 12015551234)
lnp	(Global Title only) Local Numbering Plan. Acceptable values are: 1 — ISDN/Telephony 3 — DATA 4 — TELEX 5 — Maritime Mobile 6 — Land/Mobile 7 — ISDN/Mobile 10 — British Telecom special 1 11 — British Telecom special 2 14 — Private Network
lpc	Local Point Code (PC).
lri	Routing indicator - 0 for GT (Global Title), 1 for PC/SSN.
lssn	Local Subsystem Number (SSN) (required).
ltt	(Global Title only) Local Translation Type. Generally in a live network TT is always 0.
max_requests	The maximum number of simultaneous MAP dialogs.
monitor	Activates Message Activity Monitor.
name	Name of the process.
no rst	Disables automatic restart of process.
node	Node name.
port	Port number used by the SCTP association with the client.
prot	Variant used (C7, A7, or CH7).

Table 13: authGateway Process Options Used with CREATE-PROCESS (continued)

Option	Description
trace	Enables debug tracing and displays the trace information on the console. (Consists of a trace of all MAP messages that are formatted and sent down the stack.) Use the tracefile option to capture the trace information to a file.
tracefile	Captures the trace information to a file. The filename follows the -tracefile switch. Include the directory in the filename.

Example—Creating and Starting the authGateway Process

Notice that the SSN = 7 in the CREATE-CPC of the previous example (Example 1 in Configuring the authGateway Routing Location Information on page 76) becomes the lssn (local subsystem number) in the CREATE-PROCESS command of this example. The SSN = 6 in the CREATE-REMSSN command of the previous example (Example 1 in Configuring the authGateway Routing Location Information on page 76) becomes the -rssn (remote subsystem number) in this example.

We recommend that the EXEC command use an absolute (full) pathname.

(Note: Lines are wrapped.)

```
CREATE-PROCESS:NAME="GMT", CE="sbrss7",
EXEC="/opt/JNPRsbr/radius/authGateway-name GMT -port 2000 -host sbrss7
-node MGW -prot C7 -conf /opt/JNPRsbr/radius/conf/authGateway.conf -lri 0 -lpc
14275 -lssn 7 -rssn 6 -lmisdn 393558817298 -lgti 4 -lnp 7 -ltt 0 -lnai 4 -trace";
START-PROCESS:NAME="GMT", CE="sbrss7";
```

NOTE: MML commands are saved in MML files that can be loaded into Signalware. See Loading the MML Configuration Settings on page 83.

Configuring the ulcmmg.conf File

The ulcmmg.conf file establishes the connection between the authGateway application and Steel-Belted Radius Carrier.

The ulcmmg.conf file consists of two lines, as shown in the following example. Modify the ulcmmg.conf file shipped with Steel-Belted Radius Carrier software so that the LOCAL_HOST (Steel-Belted Radius Carrier server) and REMOTE_HOST (Signalware system) values identify their DNS names and TCP port numbers. If you specify a DNS name for a local or remote host, you can enter the host's IP address in brackets as a backup.

Example

```
LOCAL_HOST myhost.com:2001
REMOTE_HOST myhost.com:2000 [172.25.97.230]
```

For additional examples, see Sample authGateway Commands and Files on page 85.

Loading the MML Configuration Settings

The files containing MML commands need to be loaded into Signalware. Enter an SWMML command for each .mml file that you created.

In the following example, three files are loaded into Signalware. The file called links.mml sets up the links, link sets, and routes. The file called config_authgateway.mml configures the authGateway application. The file called start_authgateway.mml configures the authGateway startup information.

These files do not exist and are used here as an example. You need to create your own files for accomplishing the tasks of creating links, configuring the authGateway application, and starting the authGateway application.

Example

```
$ swmml -node MGW -f links.mml
$ swmml -node MGW -f config_authgateway.mml
$ swmml -node MGW -f start_authgateway.mml
```

NOTE: Signalware remembers the MML configuration commands and uses the same configuration each time you start Signalware. To reconfigure the nodes, use the configureNodes command with the -f or -clean or -realclean options.

SS7 Sample Configuration Files

This section shows the sample configuration files for creating the basic SS7 connection to an HLR. These sample files show how to set up one board with two SS7 links.

Basic Provisioning MML File with One Point Code/ Two SS7 Links

CRTE-OSPC:**PC=9619**,NI=NAT0;
CRTE-LSET:LSET=**LSET1,PC=6400;**

Local Signaling Point Code (in decimal format) using national rules.

SPC of SS7 GW where the link is connected.

CRTE-SLK:SLK=LNK1,LSET=**LSET1**,SLC=0,SPEED=64K,PORT=0,CHANNEL=2;
CRTE-SLK:SLK=LNK2,LSET=**LSET1**,SLC=1,SPEED=64K,PORT=1,CHANNEL=3;

Define two SS7 links

CRTE-RSET:RSET=**RSET1**,**PC=6400**,RTES=**LSET1**,LOADSHR=YES;

Define route to SS7 GW.

ALW-RSET:RSET=RSET1;
ACTV-SLK:SLK=LNK1;
ACTV-SLK:SLK=LNK2;

Activate route and links.

CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="**35840211430**",PC=**9619**,SSN=0,RI=**GT**;

CREATE-GT:TT=0,NP=**ISDN-TEL**,NA=INT,DIG="**358**",**PC=6400**,SSN=0,RI=DEF;
CREATE-GT:TT=0,NP=**ISDN-MOB**,NA=INT,DIG="**358**",**PC=6400**,SSN=0,RI=DEF;

Define own GT number and point code for routing. (Routing based on GT.)

Notes:

TT — usually 0.

NP — 1=E.164=ISDN-TEL; 7=E.214=ISDN-MOB
NA — INT
DIG — Enter the first digits of MSISDN/IMSI. The routing decision is made with “best match” method. The PC message is sent towards this Point Code if “digit” matches the item specified as NP (ISDN-Tel).
Point codes — in decimal format.

Routing Based on PC/SSN

CRTE-OSPC:PC=9619,NI=NAT1;

CRTE-LSET:LSET=LSET1,PC=11;

CRTE-SLK:SLK=LNK1,LSET=LSET1,SLC=0,SPEED=64K,PORT=0,CHANNEL=2;
CRTE-SLK:SLK=LNK2,LSET=LSET1,SLC=1,SPEED=64K,PORT=1,CHANNEL=3;

CRTE-RSET:RSET=RSET1,PC=11,RTES=LSET1,LOADSHR=YES;
CRTE-RSET:RSET=RSET2,PC=17,RTES=LSET1,LOADSHR=YES;
CRTE-RSET:RSET=RSET3,PC=18,RTES=LSET1,LOADSHR=YES;

Define route for gateway and for each HLR.

CRTE-REMSSN:PC=17,SSN=6;
CRTE-REMSSN:PC=18,SSN=6;

Attach SSN and PC numbers for PCSSN

ALW-RSET:RSET=RSET1;
ALW-RSET:RSET=RSET2;
ALW-RSET:RSET=RSET3;

ACTV-SLK:SLK=LNK1;
ACTV-SLK:SLK=LNK2;

Inbound GT analysis. One for SIM Authentication module and one for each HLR.

CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="35840299",**PC=961,SSN=7,RI=PCSSN**;
CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="358402111",**PC=17,SSN=6,RI=PCSSN**;
CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="358402112",**PC=18,SSN=6,RI=PCSSN**;

Outbound GT analysis. IMSI ranges go to a specific HLR.

CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="244911",**PC=17,SSN=6,RI=PCSSN**;
CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="244912",**PC=18,SSN=6,RI=PCSSN**;
CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="244913",**PC=18,SSN=6,RI=PCSSN**;
CREATE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="244914",**PC=17,SSN=6,RI=PCSSN**;

Redundant SS7 Links Backing Up Each Other (Two Point Codes)

```
CRTE-OSPC:PC=9619,NI=NAT0;
CRTE-LSET:LSET=LSET1,PC=6400;
CRTE-LSET:LSET=LSET2,PC=6401;
```

Define two link sets using different point codes.

```
CRTE-SLK:SLK=LNK1,LSET=LSET1,SLC=0,SPEED=64K,PORT=0,CHANNEL=2;
CRTE-SLK:SLK=LNK2,LSET=LSET2,SLC=1,SPEED=64K,PORT=1,CHANNEL=3;
CRTE-SLK:SLK=LNK3,LSET=LSET1,SLC=2,SPEED=64K,PORT=16,CHANNEL=2;
CRTE-SLK:SLK=LNK4,LSET=LSET2,SLC=3,SPEED=64K,PORT=17,CHANNEL=3;
```

```
CRTE-RSET:RSET=RSET1,PC=6400,RTES=LSET1&LSET2;
CRTE-RSET:RSET=RSET2,PC=6401,RTES=LSET2&LSET1;

ALW-RSET:RSET=RSET1;
ALW-RSET:RSET=RSET2;

ACTV-SLK:SLK=LNK1;
ACTV-SLK:SLK=LNK2;
ACTV-SLK:SLK=LNK3;
ACTV-SLK:SLK=LNK4;

CRTE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="358402114300",PC=9619,SSN=0,RI=GT;
CRTE-GT:TT=0,NP=ISDN-TEL,NA=INT,DIG="358",PC=6400,SSN=0,RI=GT,
BKUPPC=6401,BKUPSSN=0,BKUPRI=GT;
```

Primary route for PC6400 is LSET1. Backup route is

Attach links from one point code to different links to maximize the redundancy.

Sample authGateway Commands and Files

AS4StartMapGw.mml — One Point Code/ Two SS7 Links

CRTE-PROCESS:NAME="GMT",CE="as1",EXEC="authGateway -name GMT -port 2001 -host as1 *-node* MGW -prot C7 *-conf* conf/authGateway.conf.100 -lri 0 -lgti 4 -lssn 7 -ltt 0 -lnp 1 -lnai 4 -appctx 2 -ldigits 358402114300";

START-PROCESS:NAME="GMT", CE="as1";

AS4StartMapGw.mml — Routing Based on PC/SSN

CRTE-PROCESS:NAME="GMT",CE="as1",EXEC="authGateway -name GMT -port 2001 -host as1 -node MGW -prot C7 -conf conf/authGateway.conf.100 -lri 1 -lssn 7 -appctx 2 -ldigits 358402114300"; START-PROCESS:NAME="GMT", CE="as1";

Table 14: Parameters Used in Create and Start Commands

Parameter	Description
name	Process name
port	Remote port specified in ulcmmg.conf
host	Hostname
node	Node name (used in swmml command)
prot	Variant used (C7, A7 or CH7). C7 in Europe
conf	Location of authGateway.conf file
lri	Routing indicator. 0 = GT, 1 = PC/SSN
lgti	(GT only) Local GTI value, 4 for C7 network; 2 for A7
lssn	Local Subsystem Number (SSN)
lnp	1 = ISDN/Telephony
lnai	Nature of Address Indicator. (4 = INT)
appctx	MAP version (2 or 3) to be used
ldigits	GT number for SIM Authentication module itself
NAME	Process name
CE	Hostname (CE means computing element)
EXEC	Program to be executed

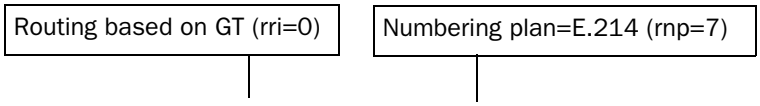
authGateway.conf (Gateway routing configuration file)

Each line of this configuration file describes:

- The parameters used to form the destination SCCP address.
- The decimal value of the bearer service (bs) and/or teleservices (ts) indicating an authorization.
- A string associated with each bs or ts value. If no bs and no ts are specified, no authorization is performed by the authGateway.

For each request, the first digits of the IMSI are compared with odigits. The first line of the configuration file that matches is selected for the current request. If the routing indicator (rri) specifies that the routing is done on GT, the leading digits are replaced with the new digits (ndigits) to perform the numbering plan translation. If a parameter is not present on the line, it is not present in the SCCP destination address. If this is incompatible with the routing indicator, an error message is issued when the MAP authentication Gateway is started.

After modifying this configuration file, the authGateway has to be restarted. Modification of the ndigits value may require the creation of a new GT rule (CREATE-GT command).



odigits **24491** ndigits **35840** rri **0** rgti 4 rssn 6 rtt 0 rnp 7 rnai 4 bs 17:B11 bs 26:B1A ts 33:T21 odb 128:NotAuthorized ss 146:NotAuthorized

odigits **244911** ndigits **244911** rri **1** rpc **17** rssn **6** bs 17:B11 bs 26:B1A ts 33:T21 odb 128:NotAuthorized ss 146:NotAuthorized
odigits **244912** ndigits **244912** rri **1** rpc **18** rssn **6** bs 17:B11 bs 26:B1A ts 33:T21 odb 128:NotAuthorized ss 146:NotAuthorized

Table 15: Parameters Used in Create and Start Commands

Parameter	Description
rri	Routing indicator - 0 for GT (Global Title), 1 for PC/SSN (Point Code/Subsystem Number).
rgti	Local Global Title Indicator value. 4 for C7; 2 for A7. (Usually 4.)
rssn	Subsystem Number of HLR.
rtt	(GT only) Translation Type (usually 0).
rnp	(GT only) Numbering Plan. 1 = E.164 = ISDN-TEL, 7 = E.214 = ISDN-MOB.
rnai	Nature of address indicator. (4 = INT)
bs	bs *dec*:*string* If the specified bearer service exists in HLR SIM-profile, then *string* is returned for further processing (see ProfileMap in simauth.aut).
ts	ts *dec*:*string* If the specified teleservice exists in HLR SIM-profile, then *string* is returned for further processing (see ProfileMap in simauth.aut).

ulcmmg.conf

LOCAL_HOST as1:2000
REMOTE_HOST as1:2001 [192.89.210.12]

Reserve port for authGateway application.