Juniper Networks®
Steel-Belted Radius® Carrier

Release Notes

Release 7.0

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

http://www.juniper.net

Part Number: 530-027224-01 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.

StrutLayout Java AWT layout manager Copyright © 1998 Matthew Phillips (mpp@ozemail.com.au).

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library 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 Library 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 © 2008, Juniper Networks, Inc.
All rights reserved. Printed in USA.

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

Revision History
16 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

System Requirements 1
Hardware 2
Software 2
Supported Browsers 3
External Database Requirements 3
Signalware and SS7 Interface Requirements 3
Modified Open-Source Software 4
Migrating from Earlier SBR Releases 4
New Features and Enhancements 4
SBR Carrier Core 4
Optional SIM Authentication Module Features 6
Optional WiMAX Mobility Module Features 6
Known Problems and Limitations 6
Resolved Issues 8
Related Documentation 11
Requests for Comments (RFCs) 11
3GPP Technical Specifications 13
WiMAX Technical Specifications 13
Third-Party Products 13
Obtaining Documentation 13
Documentation Feedback 13
Requesting Technical Support 14
Self-Help Online Tools and Resources 14
Opening a Case with JTAC 14
General Statement of Compliance 15

Steel-Belted Radius Carrier Release 7.0 Release Notes

These release notes support Release 7.0 of Steel-Belted Radius Carrier. Before you install or use your new software, read these release notes in their entirety, especially the "Known Problems and Limitations" section on page 6.

These topics are in the release notes:

- System Requirements on page 1
- Modified Open-Source Software on page 4
- Migrating from Earlier SBR Releases on page 4
- New Features and Enhancements on page 4
- Known Problems and Limitations on page 6
- Resolved Issues on page 8
- Related Documentation on page 11
- Obtaining Documentation on page 13
- Documentation Feedback on page 13
- Requesting Technical Support on page 14
- General Statement of Compliance on page 15

If the information in these Release Notes differs from the information found in the product documentation, follow the Release Notes.

You can find these release notes in Adobe Acrobat (PDF) format on the Juniper Networks Technical Publications Web page, which is located at http://www.juniper.net/techpubs/software/aaa_802/sbr.html.

System Requirements

This section describes the hardware and software requirements for running Steel-Belted Radius Carrier on Sun hardware under the Solaris 10 operating system. For more detailed information, see "Meeting System Requirements" in the *Steel-Belted Radius Carrier Installation Guide*.

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.

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 equivalents) 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 equivalents) are recommended for Solaris 10:

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

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.

Supported Browsers

The SBR Administrator configuration application can be launched from the browsers listed in Table 1:

Table 1: Supported Browsers

Browser	Versions	Operating System
Internet Explorer	6.0, 7.0	Windows XP SP2
Mozilla Firefox	2.0	Windows XP SP2
Mozilla	1.7	Solaris 10 with JRE 1.5.0_11

Java Runtime Environment (JRE) 1.4.2 or newer is required for all browsers, and is available from http://java.sun.com.

External Database Requirements

Steel-Belted Radius Carrier supports:

- Oracle 9 and 10; 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.

Signalware and SS7 Interface Requirements

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

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

CAUTION: Service Pack 5T must be installed, or Steel-Belted Radius Carrier cannot use the Signalware communications stack.

The patch is delivered in the same directory as the SBR and Signalware 9 .tgz files as SIGNALWARE_9_SP5.T_SOLARIS10_UPGRADE.TGZ.

After the base Signalware 9 software is installed, use the Signalware installation program to install the patch. For specific directions, refer to the Signalware documentation. To see a sample procedure for applying the patch, see “Installing Signalware Service Pack 5T” in the *Steel-Belted Radius Carrier Installation Guide*.

The Signalware PH0301 and XH0303 boards are supported.

For more information, see the *Steel-Belted Radius Carrier Installation Guide*.

Modified Open-Source Software

Embedded in this version of Steel-Belted Radius Carrier is open-source software that Juniper Networks, Inc. has modified. The modified software includes:

- LDAP C SDK from The Mozilla Foundation
- HTTPClient from Ronald Tschalär
- sunmd5.c from The OpenSolaris Project

You can obtain the source code for these modifications by requesting them from Juniper Networks Technical Support. See Requesting Technical Support on page 14.

Migrating from Earlier SBR Releases

If you are an existing SIM Server 5.4 or SBR 6.0 or 6.1 customer, you can migrate the SBR database and some settings (stored in configuration and XML files) into a new server while you install the Steel-Belted Radius Carrier Release 7.0 software, provided:

- The previous server is running on a Sun Solaris platform.
- The type of server — standalone, primary, or replica — is the same on both the old and new platforms.

Some files from previous SBR 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 selective 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* — disables new features and improved modules, so this is not supported by the Release 7.0 software. The method used to move forward from earlier versions to the current release is called *migration*.

Be sure to review the *Steel-Belted Radius Carrier Installation Guide* for release-specific instructions about migrating from your existing server.

New Features and Enhancements

Release 7.0 of Steel-Belted Radius Carrier includes a number of new features and improvements in the core software and in optional modules, summarized in this section. For more information, see the *Steel-Belted Radius Carrier Administration and Configuration Guide*.

SBR Carrier Core

Several new features are included with the SBR Carrier core base license:

- 3rd Generation Partnership Project (3GPP) Support
- Native Support for Structured Attributes

- Adding NAD Location Information to Access-Requests
- Included Support for Additional EAP Authentication Protocols

3rd Generation Partnership Project (3GPP) Support

3rd Generation Partnership Project (3GPP) support facilitates the management of mobile sessions and their associated resources through communication with a Gateway GPRS Support Node (GGSN). 3GPP support in Steel-Belted Radius Carrier is based on the specifications given in the *Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)* documentation (TS 29.061), which is available at www.3GPP.org.

The 3GPP support in Steel-Belted Radius Carrier includes support of multiple Packet Data Protocol (PDP) contexts. In order to transmit or receive General Packet Radio Service (GPRS) data, a mobile station (MS) must activate a Packet Data Protocol context (PDP). The PDP context is a set of parameters that consists of all the information required for establishing an end-to-end data connection. Multiple PDP contexts enable a single MS to access multiple services simultaneously.

Native Support for Structured Attributes

Release 7.0 of Steel-Belted Radius Carrier natively supports structured attributes that contain sub-attributes. Sub-attributes like normal RADIUS attribute-value pair (AVPs) consist of the raw encoding of a type field (such as 1 for WiMAX-Release, within the WiMAX-Capability VSA) followed by a length value (such as 5) followed by the value of the attribute (such as 1.2).

Sub-attributes are values in a RADIUS packet that are not stored as a RADIUS AVP, or vendor-specific-attribute (VSA), but rather are packed with other sub-attributes into a RADIUS VSA. In a RADIUS packet, multiple RADIUS VSAs might contain sub-attributes. The RADIUS VSA, which consists of multiple sub-attributes, is sometimes referred to as a *structured attribute* because it contains structured data.

Adding NAD Location Information to Access-Requests

Steel-Belted Radius Carrier core provides an attribute handling feature that allows you to add Network Access Device (NAD) location information to proxied Access-Request messages.

When a mobile device is outside the area of its provider, it roams by sending the request to a local foreign AAA (FAAA) server that is owned by another provider. Service providers might require the location of the mobile device requesting access to their network.

You can configure an Access-Request to include the location of the NAD through which the proxied request was processed. Because the NAD is geographically near the mobile device, it closely approximates the location of the mobile device.

Included Support for Additional EAP Authentication Protocols

The license for the Steel-Belted Radius Carrier core module now includes support for TLS, TTLS, and PEAP EAP authentication protocols. In earlier releases, these were available with a separate license and the addition of the EAP expansion module option.

Optional SIM Authentication Module Features

The optional SIM authentication module enables you to provide IP-based services such as public WLAN and Unlicensed Mobile Alliance (UMA) access to your subscribers, while leveraging your existing customer care and authentication infrastructure. Appropriate for Global System for Mobile Communications (GSM) infrastructures, the optional SIM authentication module provides AAA services for 802.1X and non-802.1X hotspots and Unlicensed Mobile Access (UMA) networks, enabling several new service offerings. You can offer secure hotspot access via 802.1X using the Extensible Authentication Protocol - Subscriber Identity Module (EAP-SIM) or Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) user authentication. Finally, the SIM authentication module extends mobile services over IP access networks for UMA environments, providing the same mobile identity on unlicensed wireless networks as on mobile networks, and enabling roaming and handover between networks.

Optional WiMAX Mobility Module Features

WiMAX (Worldwide Interoperability Microwave Access) is a 802.16-based implementation of a standard broadband wireless access technology used for applications that include mobile broadband, 'last mile' fixed broadband connections, hotspot and cellular backhaul, and high-speed enterprise connectivity for businesses.

Known Problems and Limitations

These issues have been identified in Steel-Belted Radius Carrier Release 7.0. The identifier in parentheses is the Problem Report number in our bug database.

- **The UseMasterDictionary feature may add or allow unknown attributes.** This can result in the dispatch of an incorrect packet. The problem occurs if two vendor-specific dictionaries associate the same attribute number with different types (such as string and integer).
  (PR 248477)

- **A modified filter.ini file may not accurately replicate from a primary server to a replica server.** The default filter.ini does replicate successfully.
  (PR 249955)

- **PEAP with inner TLS may fail with Windows supplicants.** Microsoft technical support reports that in EAP-PEAP phase 2, MS PEAP does not support fragmentation on the outer packets. To prevent this, set the inner TLS packet fragmentation so that no outer fragmentation is necessary during the negotiation.
  Edit tlsauth.aut, and in the [server_settings] section, set TLS_Message_Fragment_Length=900.
  (PR 254219)

- **Stored procedures may prevent correct server initialization.** This may occur if the server is configured to use a stored procedure that has multiple instances of multi-valued attributes as output parameters. If this happens, edit the appropriate dictionary and create several instances of the multi-valued return list attribute.
  (PR 256084)

- **Replica servers that are offline when the primary server publishes configuration data may not update correctly.** To correct this:

  1. Execute on the replica:
     # sbrsetuptool -identity REPLICA -primary *name address secret*
     where:
     name is the DNS name of the primary server
     address is the IP address of the primary server
     secret is the shared secret that authenticates configuration downloads

  2. Restart the replica.
     (PR 284279)

- **WiMAX accounting records are too cryptic in the accounting log.** Because Class attributes are presented in a binary format, some users may prefer not to log them.
  (PR 291646)

- **Some Accounting Start commands are not correctly classified as WiMAX Acct Request in ASN-GW initial accounting-start request, ASN-GW Reauth accounting-start, and accounting-stop.** To avoid this, ensure that the Accounting Request contains the NAS-Identifier or configure the RADIUS client for the specific client (not ANY) and ensure that the configured client name is the expected NAS-Identifier.
  (PR 297773)

- **When a sub-attribute string with a length of 244 characters is specified, the expected response is not returned.** To avoid this, edit the string to reduce the number of characters to fewer than 244.
  (PR 298055)

- **Changing a rule in SBR Administrator with Filter- > Edit Rule from Exclude or Add to Replace has no effect.** Instead of changing the rule type, delete the attribute and then add a new attribute with the correct Replace type.
  (PR 298086)

- **A filter with an index that is configured to replace a parent attribute with multiple instances of a single sub-attribute does not always work correctly.** To avoid this, set up the configuration so that it uses multiple separate attributes that each contain the same sub-attribute.
  (PR 298631)

- **Some hexidecimal values are not displayed when editing in SBR Administrator.** While editing within a hexidecimal string, the string may not appear in the Edit Field Value dialog. If this happens, select and retype the entire value instead of trying to modify just part of the string.
  (PR 300841)

- **During installation of Steel-Belted Radius Carrier as a primary server, false error messages in the log may report that the primary designation did not succeed.** You can safely ignore these error messages.
  (PR 304413)

- **When the optional SIM Module is in use and SIMAUTH is used as an EAP method, changing the order of EAP methods in SBR Administrator does not take effect.** Manually edit the eap.ini file to make the change.
  (PR 306868)

- **When a profile is configured in SBR Administrator, the value entered in a checklist can exceed the maximum length for the value that is specified in the dictionary file.** This does not cause any problems in Steel-Belted Radius Carrier, but if any external applications expect to receive a value with a specific length, the external application may generate an error.
  (PR 306944)

- **When using the SIM authentication module with EAP-helper enabled and a profile check list with sub-attributes is in use, a false authorization can be returned.** There is no work-around. In some cases, you might be able to implement a valid check if the helping authentication method is LDAP, because LDAP scripting may be able to work around the check list issue.
  (PR 310988)

- **The Ulticom Signalware communications stack that is accessed by the SIM and WiMAX modules may generate false error messages in the Signalware log.** When the stack is first accessed, an 8057 message is generated if everything is working properly:

  ```
  > 008057 26-Aug-2008 10:58:25 mercury.POP Info Signalware Application(s)
  > Authorized.
  >
  ```

  After that, messages such as this example may be generated periodically as a countdown timer expires:

  ```
  > 008056 26-Aug-2008 11:00:17 mercury.POP Critical Signalware
  > Application(s) Not Authorized: 60 Minutes Remaining to Authenticate
  >
  ```

  These are false warnings that you can ignore.

Resolved Issues

These issues were identified in previous releases of Steel-Belted Radius and have been resolved in Steel-Belted Radius Carrier. The identifier in parentheses is the Problem Report number in our bug database.

- **TLS CRL files were not deleted.**
  (PR 7823)

- **EAP-Identifier was incorrectly incremented in the EAP-Success message.**
  (PR 7829)

- **Running ldapcompare could cause SBR to crash.**
  (PR 7831)

- **Open SSL vulnerability.**
  (PR 7907)
- **Accounting files greater than 2 GB were not supported.**
  (PR 8304)
- **Replica servers may fail to start.**
  (PR 8434)
- **Replica server statistics may not appear in the Administrator application.**
  (PR 8558)
- **SBR may crash if SSL was used for LDAP authentication.**
  (PR 8729)
- **Root certificates with keys greater than 2048 were not imported.**
  (PR 8754) and (PR 249471)
- **authGateway usage info was incomplete and incorrect.**
  (PR 248715)
- **The Routed Proxy setting required that the %ProxyUserName be uppercase.**
  (PR 249471)
- **Names of location groups were case-sensitive.**
  (PR 249675)
- **Secondary authentication attributes were not added.**
  (PR 249799)
- **When LDAP servers were inaccessible, SBR may crash.**
  (PR 249809)
- **Proxy Target statistics were not displayed correctly in SBR Administrator.**
  (PR 261108)
- **Block = 1 did not work for static accounting realms.**
  (PR 271743)
- **LDAP servers using SSL sometimes failed to initialize.**
  (PR 272528)
- **SIM did not handle an “HLR unavailable” event.**
  (PR 273816)
- **The CDR accounting module failed to initialize when SIM-CDR was enabled.**
  (PR 280006)
- **AKA did not handle an HLR unavailable event.**
  (PR 281601)
- **The client certificate in a TTLS request caused a rejection.**
  (PR 283219)

- **The IPv6 address was not presented when a "Proxy Server Target" was added.**
  (PR 283729)

- **Sigma Administrator did not resolve the IPv6 address when configuring a Proxy Target.**
  (PR 283734)

- **Filters for directed realms were not applied for challenge protocols.**
  (PR 285045)

- **LDAP scripts did not post response attributes on reject.**
  (PR 285778)

- **When 3GPP-IMSI had a data type of** stringnz **in the radius.dct file, it was not passed back in the accept packet.**
  (PR 286845)

- **Specifying an EAP method from SBR Administrator gave a "bad data from server" error.**
  (PR 287054)

- **SBR Administrator did not delete tunnels.**
  (PR 288174)

- **When multi-valued string attributes (both standard and VSA) were inserted in the SQL database, only the last value was recognized.**
  (PR 288198)

- **Counters under statistics for Proxy Target did not show the correct values in SBR Administrator.**
  (PR 288234)

- **The JUNOSe dictionary was not updated correctly.**
  (PR 288237)

- **The column labels on the Add/Edit filters dialog were cut off.**
  (PR 288266)

- **Requests were dropped on a multi-cored server with CPU utilization at 5%.**
  (PR 305144)

- **Authentication failed due to the login limit being exceeded when an ldapauth routed proxy was invoked.**
  (PR 305621)

- **SNMP Get requests failed when TcpControlAddress was configured in radius.ini.**
  (PR 306872)

Related Documentation

Table 2 lists and describes the Steel-Belted Radius Carrier documentation set:

Table 2: 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 3 lists the RFCs that apply to Steel-Belted Radius Carrier.

Table 3: 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 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.

Table 3: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
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.
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.

Table 3: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
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 Steel-Belted Radius Carrier documents, see Table 2 on page 11. For 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.

General Statement of Compliance

Table 4 lists Steel-Belted Radius Carrier Release 7.0 compliance with applicable RFCs.

Table 4: Compliance of Steel-Belted Radius Carrier Release 7.0 with Applicable RFCs

RFC Number	Name	Notes	Drafts	Name	Notes	Protocol	Notes
1155	Structure and Identification of Management Information for TCP/IP-based Internets	—	draft-ietf-radext-digest-auth-03.txt	RADIUS Extension for Digest Authentication	not tested	UDP	—
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	—	draft-sterman-aaa-sip-00.txt	RADIUS Extension for Digest Authentication	not tested	IPv4	—
2058	Remote Authentication Dial In User Service	obsoleted by RFC 2138	—	—	—	IPv6	NAS-server only
2059	RADIUS Accounting	obsoleted by RFC 2139	draft-funk-eap-ttls-v0-00.txt	EAP Tunneled TLS Authentication Protocol Version 0	—	DHCP v2	—

Table 4: Compliance of Steel-Belted Radius Carrier Release 7.0 with Applicable RFCs (continued)

RFC Number	Name	Notes	Drafts	Name	Notes	Protocol	Notes
2107	Ascend Tunnel Management Protocol	—	—	—	—	DHCP v3	—
2138	Remote Authentication Dial In User Service	obsoleted by RFC 2865	—	—	—	LDAP v2	—
2139	RADIUS Accounting	obsoleted by RFC 2866	—	—	—	LDAP v3	not LCI
2271	An Architecture for Describing SNMP Management Frameworks	obsoleted by RFC 2271	—	—	—	JDBC	—
2284	PPP Extensible Authentication Protocol (EAP)	updated by RFC 2484	—	—	—	Oracle (SQL)	—
2433	Microsoft PPP CHAP Extensions	—	—	—	—	XML	configuration
2548	Microsoft Vendor-specific RADIUS Attributes	—	—	—	—	HTTP v1.1	admin
2607	Proxy Chaining and Policy Implementation in Roaming	—	—	—	—	LEAP	—
2618	RADIUS Authentication Client MIB	obsoleted by RFC 4668	—	—	—	WiMAX NWG 1.2.2	*except CRs 801, 823, OMA/DM*
2619	RADIUS Authentication Server MIB	obsoleted by RFC 4669	—	—	—	—	—
2620	RADIUS Accounting Client MIB	obsoleted by RFC 4670	—	—	—	3GPP2	—
2621	RADIUS Accounting Server MIB	obsoleted by RFC 4671	—	—	—	3GPP2 X.S0011-D	—
2716	PPP EAP TLS Authentication Protocol	obsoleted by RFC 5216	—	—	—	—	—
2809	Implementation of L2TP Compulsory Tunneling via RADIUS	—	—	—	—	3GPP	RADIUS only
2865	Remote Authentication Dial In User Service (RADIUS).	—	—	—	—	23.234 (RADIUS)	WLAN UE
2866	RADIUS Accounting	—	—	—	—	29.061 (RADIUS)	G1 and Pk reference points
2867	RADIUS Accounting Modifications for Tunnel Protocol Support	—	—	—	—	—	—
2868	RADIUS Attributes for Tunnel Protocol Support	—	—	—	—	TISPAN	RADIUS only Interface E5

Table 4: Compliance of Steel-Belted Radius Carrier Release 7.0 with Applicable RFCs (continued)

RFC Number	Name	Notes	Drafts	Name	Notes	Protocol	Notes
2869	RADIUS Extensions	—	—	—	—	ES282.001	—
2882	Network Access Servers Requirements: Extended RADIUS Practices	—	—	—	—	ES282.004	—
2903	Generic AAA Architecture	—	—	—	—	ES283.034	—
2904	AAA Authorization Framework	—	—	—	—	ES283.035	—
2905	AAA Authorization Requirements	—	—	—	—	—	—
2906	AAA Authorization Requirements	—	—	—	—	—	—
2977	Mobile IP Authentication, Authorization, and Accounting Requirements	—	—	—	—	—	—
2989	Criteria for Evaluating AAA Protocols for Network Access	—	—	—	—	—	—
3012	Mobile IPv4 Challenge/Response Extensions	—	—	—	—	—	—
3162	RADIUS and IPv6	—	—	—	—	—	—
3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	—	—	—	—	—	—
3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	—	—	—	—	—	—
3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	—	—	—	—	—	—
3748	Extensible Authentication Protocol (EAP)	—	—	—	—	—	—
3770	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks	—	—	—	—	—	—
4005	Diameter Network Access Server Application	—	—	—	—	—	—

Table 4: Compliance of Steel-Belted Radius Carrier Release 7.0 with Applicable RFCs (continued)

RFC Number	Name	Notes	Drafts	Name	Notes	Protocol	Notes
4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option	—	—	—	—	—	—
4017	Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs	—	—	—	—	—	—
4072	Diameter Extensible Authentication Protocol (EAP) Application	—	—	—	—	—	—
4137	State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator	—	—	—	—	—	—
4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)	—	—	—	—	—	—
4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)	—	—	—	—	—	—
4284	Identity Selection Hints for the Extensible Authentication Protocol (EAP)	—	—	—	—	—	—
4334	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	—	—	—	—	—	—
4372	Chargeable User Identity	—	—	—	—	—	—
4590	RADIUS Extension for Digest Authentication	obsoleted by RFC 5090	—	—	—	—	—
4603	Additional Values for the NAS-Port-Type Attribute	—	—	—	—	—	—
4668	h3$umal	previous version (RFC 2618) supported	—	—	—	—	—

Table 4: Compliance of Steel-Belted Radius Carrier Release 7.0 with Applicable RFCs (continued)

RFC Number	Name	Notes	Drafts	Name	Notes	Protocol	Notes
4669	RADIUS Authentication Server MIB for IPv6	previous version (RFC 2619) supported	—	—	—	—	—
4670	RADIUS Accounting Client MIB for IPv6	previous version (RFC 2220) supported	—	—	—	—	—
4671	RADIUS Accounting Server MIB for IPv6	previous version (RFC 2221) supported	—	—	—	—	—
4672	RADIUS Dynamic Authorization Client MIB	not supported	—	—	—	—	—
4673	RADIUS Dynamic Authorization Server MIB	not supported	—	—	—	—	—
4675	RADIUS Attributes for Virtual LAN and Priority Support	not supported	—	—	—	—	—
4679	DSL Forum Vendor-Specific RADIUS Attributes.	not supported	—	—	—	—	—
4746	Extensible Authentication Protocol (EAP) Password Authenticated Exchange	not supported	—	—	—	—	—
4763	Extensible Authentication Protocol Method for Shared-secret Authentication and Key Establishment (EAP-SAKE)	not supported	—	—	—	—	—
4764	The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method.	not supported	—	—	—	—	—
4793	The EAP Protected One-Time Password Protocol (EAP-POTP)	EAP-32	—	—	—	—	—
4818	RADIUS Delegated-IPv6-Prefix Attribute.	not supported	—	—	—	—	—
4849	RADIUS Filter Rule Attribute	not supported	—	—	—	—	—
4851	The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)	—	—	—	—	—	—

Table 4: Compliance of Steel-Belted Radius Carrier Release 7.0 with Applicable RFCs (continued)

RFC Number	Name	Notes	Drafts	Name	Notes	Protocol	Notes
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.	not supported	—	—	—	—	—
4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management	—	—	—	—	—	—
5030	Mobile IPv4 RADIUS Requirements	—	—	—	—	—	—
5080	Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes	—	—	—	—	—	—
5090	RADIUS Extension for Digest Authentication	—	—	—	—	—	—
5106	The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method	—	—	—	—	—	—
5169	Handover Key Management and Re-Authentication Problem Statement	—	—	—	—	—	—
5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	—	—	—	—	—	—
5216	The EAP-TLS Authentication Protocol	previous version (RFC 2716) supported	—	—	—	—	—