

Juniper Networks **SBR Family of RADIUS/AAA Servers for the Enterprise**

The Juniper Networks Steel-Belted Radius family of high-performance RADIUS/AAA servers gives enterprises complete control over how users access their networks. It significantly enhances the security and manageability of any network – centralizing user authentication, configuring the appropriate access level, and ensuring compliance with enterprise security policies. The Juniper Networks SBR family of

RADIUS/AAA servers meets the diverse authentication and security policy management requirements of enterprises of any size, and is a vital component of any organization's security and network management infrastructure. Already in use on some of the world's busiest networks managing millions of user transactions per day, Juniper Networks SBR is the gold standard for RADIUS/AAA servers.

Juniper's SBR enables enterprises to centrally enforce network access and security policies, to control who's authorized to access the network, and to configure restrictions or special characteristics of user access, such as connection time limits or a requirement to meet a certain wireless security level. SBR also ensures that users comply with the AAA specifics of the enterprise's security policies in areas like dual factor authentication, etc. These policies are uniformly applied to all users, whether they're connecting to the network via a remote/VPN or 802.1X-based wireless/wired connection, which significantly eases deployment and streamlines network administration.

Juniper Networks SBR is a complete implementation of the widely used RADIUS (Remote Authentication Dial-In User Service) protocol. It performs three vital functions:

- Authentication – validates any user's login credentials against a central security database to ensure that only individuals with valid credentials will be granted network access.
- Authorization – for each new connection, provides information to the network access device, such as what IP address to use, session time-limit information, or which type of tunnel to set up.
- Accounting – logs all connections, including user names and connection duration, for tracking and billing.

When a user connects to the network via a remote access server, VPN, firewall, router, access point, or any other RADIUS-compliant network access device, that device queries SBR to determine if the user is authorized to connect. SBR accepts or rejects the connection based on user credential information in the central security database, and authorizes the appropriate type of connection or service. When the user logs off, the network access device informs SBR, which in turn records an accounting transaction.

SBR meets all requirements of today's complex networks. It sets up and secures WLAN connections, ensuring full credential and data security over the wireless link; provides at-your-fingertips reporting and statistics on network activity, for readily available diagnostics; easily handles any volume of network traffic, to ensure reliable network access for your users; and includes a powerful replication capability and an intuitive administration program for the fastest set-up.

Value Proposition

Centrally manage and secure network authentication in all environments

- Supports wired and wireless deployments
- Cross platform, multi vendor support
- Supports any authentication method

Lower deployment costs and maintenance overhead

- Easy diagnostics, with dynamic statistics and reports
- Simple to configure and maintain

Centrally manage and secure network authentication in all environments

Juniper Networks OAC runs on a wide variety of Windows desktop and Juniper Networks SBR family lets you ensure that only authorized users can connect to your network, and that their connections are configured correctly – whether they're connecting via WLAN, remote/VPN, or wired 802.1X. Beyond these basic AAA requirements, SBR also meets the specialized requirements of each access method.

Features	Benefits
Cross platform, multi vendor support <ul style="list-style-type: none"> Works seamlessly with a variety of network access equipment, including WLAN, remote/VPN, wired 802.1X, dial-in, outsourced, or any other form of access – in any combination Simple interface with network access equipment from different vendors simultaneously. Customized dictionaries describe each vendor's extensions to the RADIUS protocol. 	Enables best-in-class AAA control for virtually all deployment types and manufactures Seamless operation in a heterogeneous environment simplifies deployment and day-to-day operations
Secure WLAN access supported protocols include: <ul style="list-style-type: none"> EAP-TTLS EAP-PEAP EAP-TLS Cisco's EAP-FAST and LEAP RSA Security's EAP-POTP EAP-MD5. 	Support whatever WLAN protocol is a best fit in your deployment
Complete support for the specialized features of your remote/VPN servers	Enables you to centrally manage remote/VPN access to your network.
Enables wired 802.1X* authentication based on user identity, not Ethernet port <small>*Requires an 802.1X client such as Juniper Network's Odyssey Access Client</small>	Vastly simplifies your administrative tasks and lowering overhead.
Authenticate users against any authentication method or combination of methods you choose, including: Native database of up to 20,000 users and their passwords "Pass-through" authentication to information contained in: <ul style="list-style-type: none"> Windows Domains and UNIX security systems, including Active Directory (with full support for MS-CHAP extensions to support change of expired passwords), UNIX local users and groups, and Solaris Network Information Services+. Token-based authentication systems such as RSA Security's Authentication Manager (SecurID). LDAP directories, including Novell's eDirectory, Sun Java System Directory Server, and open LDAP SQL databases, including Oracle and MySQL. Any ODBC- or JDBC-compliant database TACACS+ authentication Other RADIUS servers, for proxy authentication 	This saves countless hours by allowing you to use the same database to authenticate LAN, WLAN, remote/VPN and wired 802.1X users. Authentication is not limited to just user name/password queries Enables you to take full advantage of the power of an LDAP directory to manage your users.

Lower deployment costs and maintenance overhead

Juniper Networks SBR has a wealth of features that make it easy to deploy and simplifies day-to-day operations, while providing you with all the AAA you expect from a market leader.

Features	Benefits
Easy diagnostics, with dynamic statistics and reports <ul style="list-style-type: none"> View entire history of authentication requests and responses Track length of user connections with RADIUS accounting View statistics on authentication, accounting proxied requests, and more Compile information into informative, searchable reports 	Sophisticated logging, auditing and report features make it easy to view activities from a variety of perspectives
Simple to configure and maintain <ul style="list-style-type: none"> XML-based GUI Simple cut-and-paste server configuration settings Centralized Configuration Management (CCM) Centrally manage multiple copies of SBR Simple replication of primary copy configuration 	Administer the server from any machine Significantly reduce time required to bring devices and users online Saves time and reducing the possibility of configuration errors

Several form factors to ensure the appropriate functionality for your environment

The Juniper Networks SBR family of RADIUS/AAA servers includes different editions of the product, tailored to the requirements of a diverse range of enterprises.

Platform	Function	Appropriate for
SBR Enterprise Edition	Centrally manages and secures network access via access, and enforces a uniform access security policy enterprise-wide.	SBR EE is suitable for small-mid-size enterprises.
SBR Global Enterprise Edition	Extends the capabilities of SBR EE to meet the security and management needs of global enterprises who are managing thousands of remote/VPN or 802.1X-based (wireless or wired) users across multiple sites.	SBR GE is suitable for large enterprises who need SNMP-based management, distributed authentication via proxy RADIUS, and advanced reliability features.
SBR Appliance	SBR EE and SBR GE are available on a dedicated, rack-mountable device that integrates easily into a network closet.	SBR AP is suitable for any enterprise who prefers the convenience of network appliances.

Specialized Edition for Global Enterprises

In addition to the features listed above, the SBR GE RADIUS server includes numerous specialized features to meet the unique AAA requirements of global enterprises managing thousands of users across multiple sites:

- Powerful proxy RADIUS support lets you distribute authentication to any RADIUS server, with numerous powerful features – including directed realms and proxy packet filtering – available to handle different access methods and equipment.
- Advanced reliability features such as load balancing and round-robin ensure high availability, so your users can always connect to the network. Reliable accounting eliminates lost accounting records and duplicate entries, and removes the need for local data backup and batch processing.
- Compatibility with SNMP-based management systems

Technical Specifications

SBR EE and SBR GE System Requirements

- SBR for Windows XP/2000/NT runs on Windows NT 4.0 with Service Pack 6, Windows 2000 (all editions), Windows XP (all editions), and Windows Server 2003 (all editions).
- SBR for Solaris runs on Solaris 8 or 9 running on SPARC or UltraSPARC.
- SBR for Linux runs on the SuSE Enterprise Server 9 (SLES9) and Red Hat (Enterprise and Advanced Server 3) versions of Linux.

SBR is administered via an XML-based administration program which runs on Windows, Solaris, and Linux, and lets you administer any copy of SBR, regardless of platform.

SBR AP Specifications

SBR EE and SBR GE are available as network appliances, with the following specifications:

Hardware:

- Form Factor: 1U rack height
- Dimensions (HxWxD): 1.75x16.7x14 inches
- Processor(s): 2.8 GHz Pentium
- Memory: 512 MB RAM
- Disk space: 80 GB
- Connectivity: On-board dual 100/1000 NIC
- Regulatory: UL1950, CSA22.2 No.950, EN60950, PCC Part 15 Class A, EN55024:1998, EN55022:1998, EN50082-0, VCC V-3/200.4, AS/NZS 3548
- Certifications: cULus, CE, VCCI, FCC Part 15, C-Tick, TUV

Software:

- SBR EE or SBR GE
- Microsoft® Windows® 2000 Professional, Security Hardened
- Secure, browser-based management console

Performance: 1,500 transactions per second



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)1372-385500
Fax: 44(0)1372-385501

Copyright 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.