INTERLINK NETWORKS

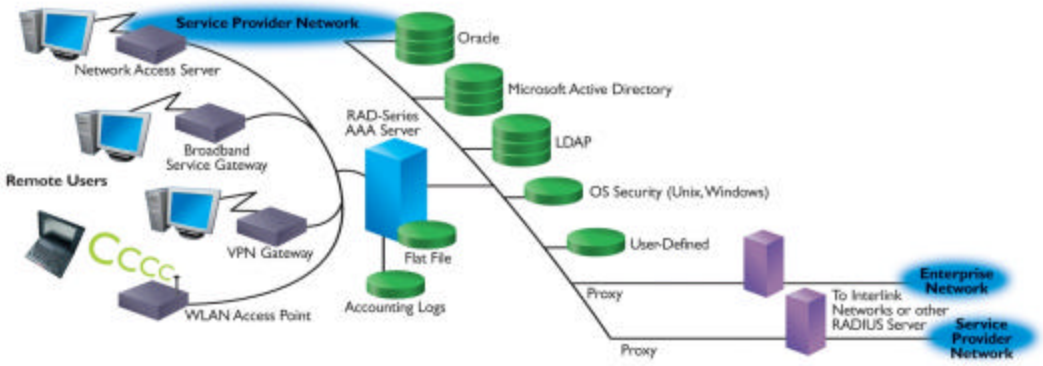
Product Brief

RAD-Series RADIUS Server – Version 7.3

Highly Customizable RADIUS Server for Controlling Access & Security in Wireless & Wired Networks

Interlink Networks' RAD-Series Authentication, Authorization, and Accounting (AAA) RADIUS Server provides standards-based access control and security for mixed access networks – including mobile, wired and wireless networks. The RAD-Series RADIUS Server enables Carriers, Internet Service Providers, and fully networked enterprises to centrally manage the AAA functions for their network users. Because of its high customizability and advanced user features, RAD-Series is ideal for system integrators and OEMs of network equipment.

The RAD-Series is high performance, highly scalable and modular RADIUS server with thousands of installations across the world. The RADIUS server supports the AAA RADIUS protocol with a set of sophisticated capabilities required to manage the business aspects of network access. A unique feature of the RAD-Series RADIUS Server is that it supports user-developed plug-in modules which can be used to enhance the authentication and authorization decision-making process, modify incoming or outgoing packets, and provide interfaces to any external system.



Carrier-Class Reliability and Agility

Based on the widely deployed and proven Merit RADIUS architecture, the RAD-Series RADIUS Server provides a fault-tolerant, scalable, higher-performance solution.

Runs on Red Hat Linux and SUN Solaris Servers

- RADIUS server scalability supports millions of users and delivers high-performance AAA transaction rates up to 2400 authentications per second.
- Provides reliability with failover, load balancing, and redundancy features.
- Supports LDAP and Active Directory databases, allowing you to maintain a single, centralized user database for all applications.
- Optimized for mixed-vendor environments and for use with any remote access device acting as a RADIUS client.

Strong 802.1x Authentication

Network Access Security

The RAD-Series RADIUS Server centralizes the management of network access across all of your networks, allowing you to more easily manage users and secure the information being accessed across the network. Whether you are extending your current network or are deploying a new network, the RAD-Series RADIUS Server provides all of the additional security required for both wireless and wired connections.

- **802.1X Network Security Support:** The RAD-Series RADIUS Server is fully compliant with the 802.1X standard which centralizes the network access management into a single RADIUS server. RAD-Series is compliant with the WPA and WPA2 security standards for enterprise wireless networks.
- **Complete Extensible Authentication Protocol (EAP) Support:** Supports 802.1x-compliant authentication protocols EAP-MD5, Cisco LEAP, EAP-TLS, EAP-TTLS, EAP-PEAP.
- **NEW! EAP-SIM Support** for authentication using the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM). RFC 4186 compliant.
- **Multi-Vendor Compatibility:** Works with access points and switches from vendors such as Cisco, Intel, 3Com, Symbol, Agere, Avaya, Enterasys, D-Link, Proxim, Linksys and other industry leading security solutions and platforms.

Supports Multiple Access Technologies:
- ***Dial-up***
- ***Broadband***
- ***Managed VPN***
- ***Mobile wireless***
- ***Enterprise WLAN***
- ***WLAN Hotspots***

Versatile Service Delivery

The RAD-Series RADIUS Server lets you can define user profiles to assign a set of connection attributes to any user or group of users. User profiles can be standardized across different types of network access equipment and networks, allowing the delivery of the appropriate level of authorization to each individual user, regardless of where they are or how they are connected.

- Supports multiple services: dial-up, wholesale dial-up, broadband, managed VPN, mobile wireless, enterprise WiFi, and WiFi hotspots.
- Supports 802.11 wireless LAN authentication using 802.1x compliant methods.
- Supports delivery of wholesale, outsourcing, and roaming services by proxy RADIUS.
- Interoperates with any other RFC compliant RADIUS server to easily distribute authentication and accounting.

System Integrator/OEM-Specific Customization Features:

Interlink Networks offers several extensibility features or "toolkits" for system integrators and OEMs to differentiate their products, add value to their solutions, and re-brand the RADIUS server and components. The customization options for RAD-Series RADIUS Server include a programmable finite state machine, application programming interfaces, an advanced policy engine, and brand-able documentation.

Programmable Finite State Machine (FSM)

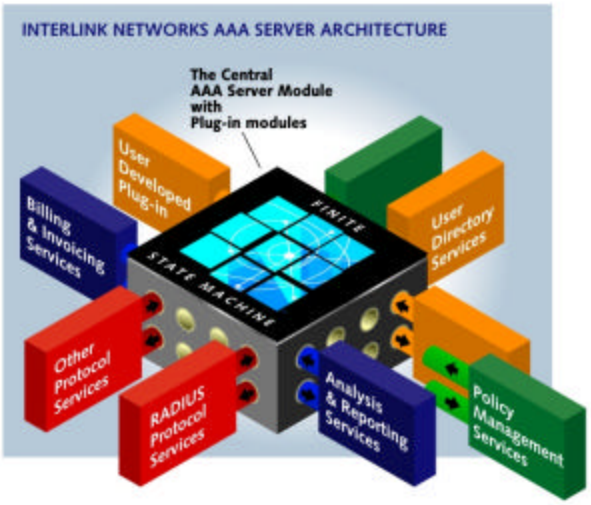
The core Finite State Machine (FSM) engine drives the processes of handling RADIUS requests. These sequential processes can be expanded or modified by changing the FSM without any recoding or recompiling of the engine. The RAD-Series RADIUS Server comes with several predefined solutions from which to choose.

Modular Server Architecture Allows Total Customization

Application Programming Interfaces (APIs)

Authentication API – Used to internally develop extensions to the core RADIUS Server architecture, you can build custom modules for unique authentication, authorization, or accounting methods and plug them in to the RADIUS server to control any part of the AAA process. For example, you can:

- Authenticate users stored in any data source, including off-the-shelf and proprietary databases
- Track and control usage based on unique billing systems
- Implement highly customized authorization schemes



- Add support for unique network access hardware

User Interface API – This branding feature allows OEMs and system integrators to build custom UIs and other RADIUS server management applications tailored to the varied needs of their end-user customers. The API provides a consistent interface to the RADIUS server's configuration and data files, regardless of how or where the information is stored. Allows easy migration and upgrades to new server versions by acting as an abstraction layer between the external interfaces and the core RADIUS functionality. This feature simplifies product localization or "internationalization".

MAJOR ADVANTAGE: Policy Management that combines power and flexibility with ease of use

Advanced Policy Engine

RADIUS Policy, part of the user Authorization process, is a set of rules to administer, manage, and control access to network resources. RADIUS policies are written to accomplish specific tasks such as to set limits and access restrictions, and to define new service levels and QOS.

Interlink's Advanced Policy Engine allows you to easily define and enact custom policies using customizable decision files. Our flexible policymaking capabilities can solve virtually any problem that would traditionally require custom programming. You can modify how authentication requests are handled and control how services are delivered and logged using simple text files with Boolean expressions.

The Policy Engine Allows Complex Policy Decisions Based on RADIUS Attribute Value Pairs / Combinations & Boolean Operations

New! Advanced Policy Features in V7.3

The latest release of the RAD-Series RADIUS Server includes:

- New action functions including modification and deletion of Attribute Value Pairs (AVPs)
- Extended substring handling
- Support for multiple AVP instances
- Support for AVP filtering of RADIUS requests entering and exiting the RADIUS server.

Documentation Re-branding

Interlink Networks offers OEMs and System Integrators the ability to place re-brand the Interlink name throughout the user documentation, white papers, and data sheets with your company name and branding.

Interlink Networks' RAD-Series RADIUS Servers has been re-branded and integrated by a number of major worldwide networking equipment providers.

FEATURES:

RAD-Series RADIUS	Description
Authentication Methods	**Choose your preferred authentication method**
PAP, CHAP and MS-CHAP	Password Authentication Protocol, Challenge Handshake Authentication Protocol, and Microsoft's version of CHAP.
802.1X Compliant Authentication Support	EAP-MD5, GTC, LEAP, TLS, TTLS, PEAP (Cisco and MS versions). EAP-SIM (optional feature)
EAP-SIM Support *(optional module)*	Full support for RFC 4186 including Pseudonyms and Fast Re-authentication. Support for local Authentication Center (AuC) functionality using user secrets (K_i) from any data store and administrator definable A3/A8 algorithms. 3GPP Milenage A3/A8 algorithm reference implementation.
Data Sources	**Store user data and profiles in many places / ways**
Flat File (users file/realm file)	Uses flat files stored internally with server. Supports all authentication and authorization features without requiring an external database or directory. Ideal for small to medium applications.
UNIX User (Password File)	Uses standard existing password files for UNIX systems.
UNIX via Password File:	Uses extended data sources for UNIX systems: NIS, shadow password, HP security, etc. Inherited automatically through support for UNIX passwords.

RADIUS Proxy Authentication & Accounting	Forwards authentication & accounting requests to remote server. Needed for any roaming relationship or large multi-server application.
RSA ACE Server	Support for RSA SecurID token cards.
LDAP	Accesses user profiles in LDAP directories. Standard access, reaches many different LDAP implementations. Includes Interlink schema extensions to support simple authorization policies. Includes load balancing and fail-over capabilities. Includes secure communications over SSL.
Active Directory	Allows authentication against Microsoft Active Directory Server via LDAP.
Authorization Features	**Policy Decisions & Criteria**
Simple RADIUS Policy	Allows or denies network access based on specific attribute values. Sets basic session configuration parameters based on Reply items stored in the user profile.
Advanced Policy Engine *(optional module)*	This powerful configuration engine allows you to develop and enforce custom policies using simple text files with Boolean expressions. Decisions can be based on nearly any attribute value pairs and conditional operations. For example you can authorize across any set of independent parameters including: -System parameters: time/day/date -Edge device parameters: port #, IP address…. -User-specific information: user, group, role You can also create conditional replies for: -Differentiated connection services -Additional security measures
Authorization Reply Items	**Here are some of the outputs possible from the server, which can direct a NAS to take specific action or set specific service levels.**
Idle Time-Out	Controls length of idle-time for user sessions. Disconnects inactive (idle) sessions left typing up network resources.
Session Time-Out Limits	Limits length of user sessions.
IP Address Assignment	Assigns IP address from either static addresses or addresses relayed from DHCP.
Attribute Pruning (filters response AVPs)	Can choose not to pass some data elements to NAS after user has been approved. Example: Server only sends AV pairs appropriate to what the particular NAS supports.
Attribute Mapping	For legacy NAS devices: provides backwards compatibility for early NASs that did not implement vendor specific attributes complaint with the RADIUS RFCs.
QoS	Sets throughput or bandwidth by user.
IP Filter	Uses named filters to limit which protocols are allowed, and/or where user can go.
Compulsory Tunnels	Forces VPN tunnels.
Wireless VLANs	VLANs are used to build “boundaries” to protect sensitive data while enabling access to role-based network resources. Authenticate and assign users to the correct VLAN based on organization unit, application, role, or any other logical grouping.
Extensibility Features	**Tools to create extensions to the server.**
VSA Definitions and RADIUS Dictionary Extensibility	Dictionary contains VSAs for most major networking equipment vendors. In text file format, it can easily be extended to add vendors and their VSAs to support new vendor-proprietary features without a software upgrade.
Programmable Finite State Machine	Makes it possible to redefine the authorization and accounting processes by modifying the finite state machine tables, without recoding or recompiling the engine.
Software Developer’s Toolkit *(optional module)*	Create custom plug-in modules to interface with third party databases, execute custom authentication protocols and algorithms, custom logging, request/response processing, and customization of the user interface.
Advanced Policy Engine *(optional module)*	Develop and enforce custom policies using simple text files with Boolean expressions. Decisions can be based on nearly any attribute value pairs and conditional operations.
RFC Compliance	**Complaint with the following RADIUS standards and extensions:**
Complaint RFCs	RFC 2284, 2548, 2619, 2621, 2716, 2759, 2809, 2865, 2866, 2867, 2868, 2869, 3579, 3580, 3748, 4186

Accounting	RADIUS Accounting Capabilities
Proxy Accounting	Allows accounting records to be forwarded from one RADIUS server to another. Important in roaming or multi-server applications.
Browser View of Accounting Logs (by date, port, user)	View log data from the Server Manager.
Predefined & Customizable Logging Formats	Generates accounting call detail records (CDRs) in Livingston and MERIT formats.
Accounting On/Off Packet Support	Signals NAS start-up or shut-down management.
Management	**RADIUS Server Management Capabilities**
Web-based Server Administration	Simplifies the set up and maintenance of multiple servers from any Web browser. User profiles and server operation, including status and key statistics, can be configured and monitored remotely.
Remote Monitoring	Supports remote monitoring of server status and key statistics. Remotely view access activity and detect authentication problems.
Configuration file generation	Configuration files can be generated via the graphical user interface, command line interface, or scripts.
Session & Event Logging	Logs all events to provide extensive audit trails for troubleshooting or security. Supports Merit and Livingston standard for detailed session logging.
Simultaneous Access Control	Concurrency management allows configuring user or realm for simultaneous sessions.
SNMP Support	Supports standard RADIUS Server MIBs for authentication and accounting.
DHCP Relay Support	Scales beyond one RADIUS server with same IP pool. Allocates IP addresses for pools managed by DHCP server.
Operational Features	**RADIUS Server Performance and Reliability**
High Speed Processing Performance	Performance measured in thousands of authentications per second depending on hardware configuration.
Load Balance and Failover across LDAP	Supports backup LDAP directories with RAD-Series handling failover.
Server Platforms	**RAD-Series RADIUS Server Software runs on:**
Solaris	8, 9, & 10 on Sun Solaris/SPARC hardware.
Red Hat LINUX Red Hat Enterprise Linux	7.2, 7.3, and 8.0 on Intel hardware. ES Release 3.0, 4.0 & 5.0 on Intel hardware.

INTERLINK NETWORKS

Interlink Networks, LLC.
2500 Packard Rd., Suite 202
Ann Arbor, MI 48104

Sales: +1 (734) 821-1238
Fax: +1 (734) 821-1235
www.interlinknetworks.com