



AuthAgentRADIUS

Remote Authentication Dial-in User Specification

AuthAgent RADIUS is a lean-footprint embedded implementation of the Remote Authentication Dial In User Service as specified by RFC 2865. It relies on a client/server mechanism to carry authentication, authorization and configuration information between a service which needs to grant privileges, and a shared server that has the user and node information required to decide whether such privileges should be granted. It facilitates the use of a server based non-embedded user database with centralized user and configuration administration that is very easy to use with a provisioning system such as an OSS (Operational Support System).

AuthAgent RADIUS

AuthAgent RADIUS is a lean, embedded implementation of the RFC 2865-specified Remote Authentication Dial In User Service for embedded devices. It

implements a client/server mechanism to carry authentication, authorization, and configuration information between a network service granting privileges and a shared server that has the centralized user and node information required to decide whether such privileges should be granted. When used in conjunction with protocols that secure the network path, **AuthAgent RADIUS** provides a powerful, yet simple mechanism to authenticate and authorize access to VPNs, dial-up concentrators, Ethernet switches, and more recently, wireless networks.

RADIUS, originally intended for dial-in use, is now the de-facto standard for remote authentication in both new and legacy applications. The RADIUS protocol specifies the information exchange between a device that provides network access to users (the "RADIUS client") and a device that

Features

- ❖ RFC-compliant, interoperability-tested RADIUS client library
- ❖ Includes a password-based and an EAP authentication client
- ❖ Built-in authentication with PAP, CHAP, MS-CHAP and EAP
- ❖ Supports Microsoft Vendor-Specific attribute format, decryption of MS-MPPE-Recv/Send-Key attributes
- ❖ Supports challenge-response
- ❖ Dynamic shutdown and restart
- ❖ Can be used standalone or with network security protocols
- ❖ Support for multiple CPU types of either endian-ness including PowerPC, MIPS, X86, ARM/Xscale
- ❖ Royalty-free full source distribution

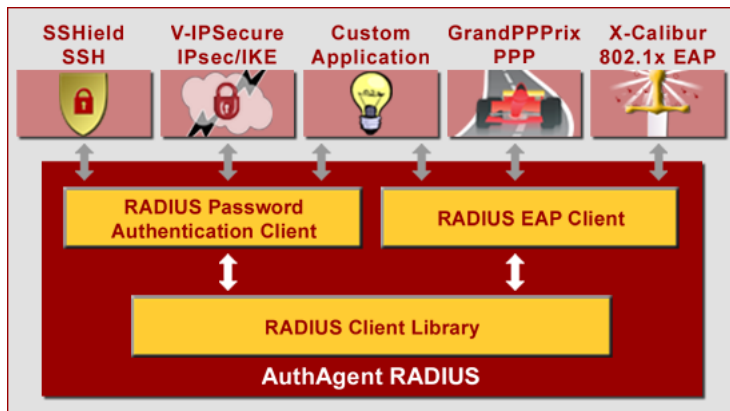


Fig 1: AuthAgent RADIUS Operation

manages authentication information for those users (the "RADIUS server"). Having this separation of roles allows for centralized authentication and administration, which is especially attractive to embedded devices that need to verify user credentials and authorize users, without having the overhead of maintaining and administering a database of sensitive user information. **AuthAgent RADIUS** provides a library to build customized RADIUS client applications, and facilitates this authentication on embedded devices.

Special Features

- ❖ Supports dynamic initialization and de-initialization of RADIUS client library
- ❖ Validated with V-IPSecure (XAUTH) for IKE authentication
- ❖ Enhanced memory management and partition support
- ❖ Enables the processing of attributes using custom mechanisms
- ❖ Supports multiple and redundant RADIUS servers
- ❖ Supports EAP and easily adds new EAP types

RADIUS Security

Security for the RADIUS information exchange is enabled by means of a pre-configured shared secret known only to the client application on the **AuthAgent RADIUS** side (configured using its APIs), and to the RADIUS server in use. All transactions between them are encrypted using this shared secret,

which itself is never sent over the network. In addition, **AuthAgent RADIUS** always encrypts passwords using a stream derived from an MD-5 hash (per RFC 2865), so that only the two ends of the RADIUS link can decode them.

Challenge Response Support

Besides synchronous Accept/Reject access authentication, **AuthAgent RADIUS** also supports challenge-response authentication, in which the server sends back a challenge prompting the user for information such as additional authentication information contained on a smart-card or a two-factor scheme using external tokens to respond to the challenge. **AuthAgent RADIUS** packages and sends the user's response to the server, and authorizes access based on the server's response.

EAP over RADIUS

Extensible Authentication Protocol (EAP) is an IETF protocol (RFC 2248) defined for extensibility of authentication processes with evolving authentication methods, without changing existing applications. In addition to support within Point-to-Point Protocol (PPP), EAP is also supported in the IEEE 802 link layer for wired and wireless switch port authentication using the 802.1X specification. **AuthAgent RADIUS** includes a reference EAP-based client

which negotiates EAP types and transports EAP-Message RADIUS attributes. This provides an interoperable authentication mechanism for wired LANs, and a method of access control and distribution of encryption keys for wireless LANs, such as those used with WEP, TKIP, and CCMP.

Vendor-specific attributes

RADIUS transactions are comprised of variable length Attribute- Length-Value 3-tuples and new vendor-specific attributes can be added without disturbing existing implementations. The flexible library provided by **AuthAgent RADIUS** allows any generic RADIUS attribute, including ones listed in RFC 2865, to be sent and received by a RADIUS client application. In addition, it also provides the APIs to process any Vendor-Specific attribute by parsing the generic portions of the attributes, while the application extracts vendor-specific content. **AuthAgent RADIUS** allows the processing of attributes using custom mechanisms. Specifically, for Microsoft specific attributes, **AuthAgent RADIUS** transparently decrypts the MS-MPPE-Recv-Key and MS-MPPE-Send-Key attributes.

Usage Scenarios

AuthAgent RADIUS can be used standalone or as an add-on for **TeamF1's**

Also Available

- ❖ **AuthAgent Family**
RADIUS, Kerberos, TACACS+ & X.509 agents
- ❖ **SSecure Family**
SSH, SSL, IPsec/IKE

Supported RFCs

- ❖ RFC 2865
- ❖ RFC 2548
- ❖ RFC 2284
- ❖ RFC 3579
- ❖ RFC 3580

Customization Flexibility

- ❖ Flexible APIs for configuring RADIUS server settings including server name/ip address, retry count, NAS identifier and timeouts on a server-specific basis
- ❖ Supports multiple RADIUS servers
- ❖ RADIUS attribute dictionary configures required attributes while ignoring others
- ❖ Can add authentication methods
- ❖ Supports EAP and easily adds new EAP types
- ❖ Supports Vendor-Specific attributes
- ❖ Client configuration via configuration files or, where a file system is not available, directly through APIs

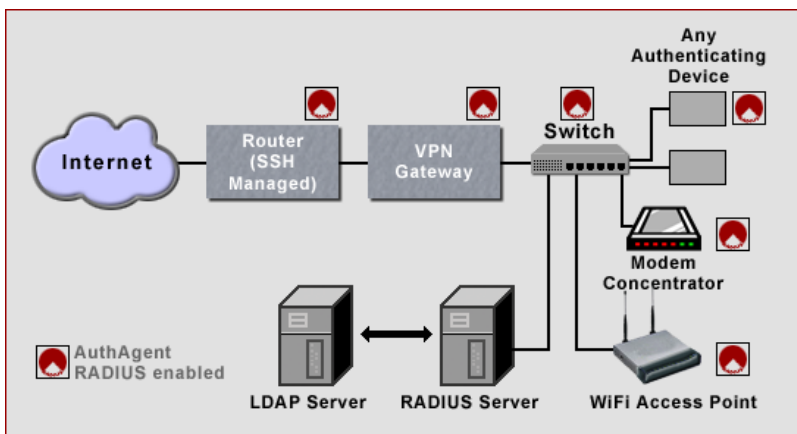


Fig 2: Example AuthAgent RADIUS Usage Scenarios

network security protocols including **SSHield** and **V-IPSecure**. It can also be combined with third-party security protocol implementations, allowing a common centralized back-end authentication server to hold and administer a user-directory that can be used across the board in an enterprise. Further, its made-for-embedded design and dynamic shutdown and restart capabilities make it easy to use with a provisioning system.

Email: sales@TeamF1.com
 Web: www.TeamF1.com
 Ph: 510-505-9931 ext. 5
 Fax: (510) 505-9941



© 2004-2008 TeamF1, Inc.