

RADIUS

Remote Authentication
Dial In User Service

Dial-In Security with RADIUS

Secure dial-in requires that each Network Access Server has access to a database of allowed users and their attributes. The RADIUS protocol will enable the use of a single more easily maintained database, which is accessed through a client/server model.

The management of dial-in resources such as serial lines and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools by definition create a connection to the outside world, they require careful attention to security, authorization and accounting.

This can be best achieved with a single database of users, which allows for authentication as well as configuration information, detailing the type of service that is available to the user.

Client/Server Model

A Network Access Server (NAS) operates as a RADIUS client. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then return-

ing all configuration information necessary for the client to deliver service to the user.

A RADIUS server is also able to act as a proxy client to other RADIUS servers or other kinds of authentication servers.

Network Security

Transactions between the client and RADIUS server are always authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and the RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

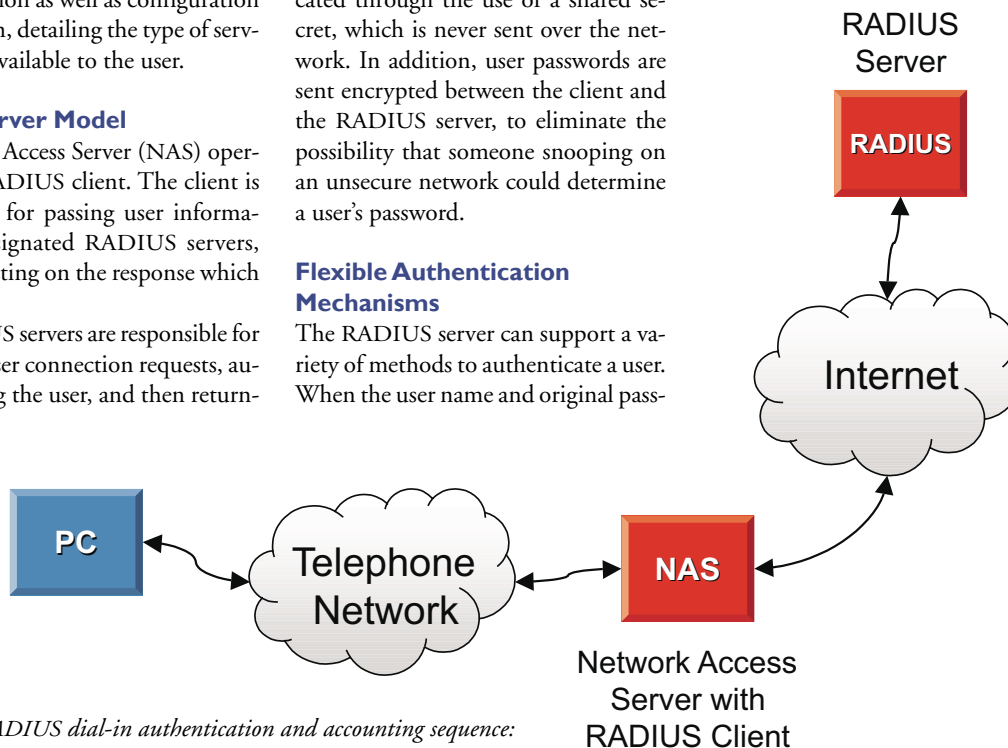
Flexible Authentication Mechanisms

The RADIUS server can support a variety of methods to authenticate a user. When the user name and original pass-

word given by the user are available, it can support PPP PAP or CHAP, as well as other authentication mechanisms.

Extensible Protocol

All transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.



RADIUS dial-in authentication and accounting sequence:

- 1. User dials in.*
- 2. User authenticated and authorized using data in server.*
- 3. Accounting information sent to server.*

Interpeak RADIUS Features

The Interpeak RADIUS client is designed to be used in a wide range of embedded applications. The RADIUS client makes no assumptions on the types of attributes an application may want to send to the server. The RADIUS client therefore contains a comprehensive toolbox of functions to inspect attributes in packets, and to add or change attributes.

Multiple RADIUS Servers

The RADIUS client can handle any number of servers. Servers can be added and removed through the API.

A server may be specified to handle authentication requests, accounting requests or both. The RADIUS client will try servers with matching properties, beginning with the server that was added last. Alternatively, a desired list of servers may be specified for a specific access or accounting request.

The RADIUS client can have at most 256 outstanding requests of the same type (accounting or access) per server. After this, new access requests or accounting sessions must wait until the server has processed more pending access/accounting requests.

Authentication

The RADIUS client requests an authentication by sending an Access-Request packet to the server. The packet contains username, password and other optional attributes which may have been added by the application.

- **RADIUS Authentication**
 - Supports RFC 2865 and RFC 2618*.
 - Authentication with PAP or CHAP
 - Full User Attribute Access
 - Attribute Manipulation Toolset
 - Multiple Servers Handled
- **RADIUS Accounting**
 - Supports RFC 2866 and RFC 2620*.
 - Interim Accounting
 - Separate Servers for Authentication and Accounting
- Delivered in ANSI compliant "C" source code
- Complete ready-to-run RTOS integration with examples, makefiles etc.
- Configured with powerful shell commands

Interpeak RADIUS features.

** MIB support requires integration with SNMP agent software.*

If the RADIUS server is satisfied with the request, it will send an Access-Accept to the RADIUS client. If the server cannot honor the request, it will reply with an Access-Reject packet. The reply will contain a message detailing the reason for the reject.

Accounting

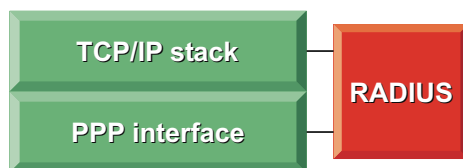
An accounting session is started when the RADIUS client sends an Accounting-Request packet to the server. If interim accounting has been requested,

the RADIUS client will send accounting updates with a selected period.

The default behaviour is to always send interim accounting requests as well as the accounting stop request to the server which initially replied to the accounting start request. This ensures that all records of a particular session will reside on the same server, thus simplifying the work of accounting software.

Using Different Servers

The RADIUS client can also operate in a mode where any server will get the accounting requests. This provides the greatest likelihood that no accounting records are lost. If accounting records from the same session are sent to different servers, the software that uses the accounting records must be able to find connected records on more than one server.



Configuration example where PPP login is managed by means of an Interpeak RADIUS client.

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company's embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage www.interpeak.com.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 1.23-r5. Copyright © 2005, Interpeak AB. All rights reserved.