

# Steel-Belted Radius

## Centralized Security for Dial-In Users

For NetWare or Windows NT

*Cimarron Boozer*

*Vice President, Product Marketing*

*Funk Software, Inc.*

**1997 RSA DATA SECURITY CONFERENCE**  
San Francisco, January 28th - 31st, 1997



Funk Software, Inc.  
222 Third Street  
Cambridge, MA 02142  
(617) 497-6339  
<http://www.funk.com>

---

## Introduction

As a Novell or Windows NT network administrator you have increased responsibilities for remote users accessing your enterprise LAN and internetwork. Remote access includes not only dial-in users, but also access from the Internet through your firewall or virtual private network. The challenge is to provide a centralized form of authentication, authorization, and accounting for your entire network, no matter which type of remote access you may have. And you want to use the existing authentication framework you have in place, such as Novell NetWare Directory Services or Microsoft NT Domains or Workgroups.

To meet this challenge, a new standard — RADIUS (Remote Authentication Dial In User Service) — has emerged which is supported by the leading remote access and firewall vendors. And a new product — Steel-Belted Radius — provides the gateway between remote access and NetWare or Microsoft NT based environments.

With Steel-Belted RADIUS, you can:

- ❑ Centralize administration of user information across all your Remote Access Servers performing dial-in and firewall authentication
- ❑ Utilize security information to which your Remote Access Servers would otherwise have no access such as NetWare's Bindery and Directory Services (NDS), or Windows NT Domain and Workgroups
- ❑ Use Remote Access Servers from a variety of vendors while maintaining a common security model and administrative interface
- ❑ Get centralized accounting and reporting of all remote access to your network, and view the real-time status of all currently connected users

---

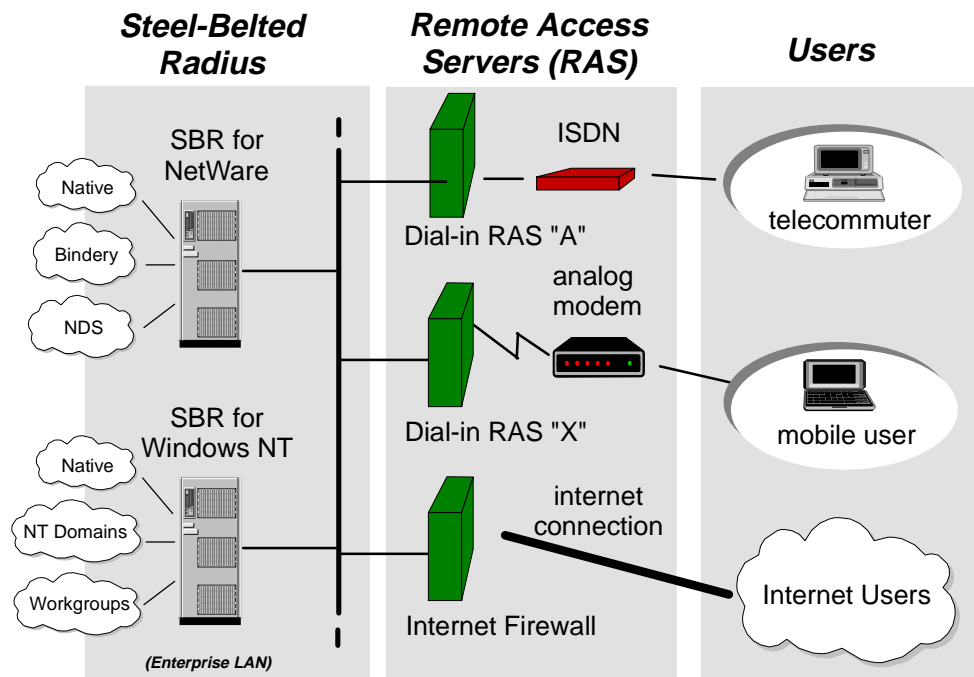
## Product Overview

Steel-Belted Radius is a complete implementation of the RADIUS standard that runs as a native application in your Novell NetWare or Microsoft NT environment. On a Novell server, it runs as a set of NetWare Loadable Modules (NLMs); on a Microsoft Windows NT server, it runs as a set of NT services.

Because Steel-Belted Radius is tightly integrated with NetWare or Windows NT, you can use the passwords and groupings you've already created in the NetWare Bindery, NetWare Directory Services (NDS), Windows NT Domain or Windows NT workgroups as the basis for authenticating remote users dialing in to any of your Remote Access Servers.

Steel-Belted Radius is compatible with Internet Service Providers (ISPs) that support "Proxy Radius" technology. This allows your ISP to outsource dial-in remote access using your organization's RADIUS server. The ISP can therefore provide access without tracking individual account names within your enterprise; this tracking is instead performed by Steel-Belted Radius, and managed by your LAN administrator.

*Figure 1: Steel-Belted Radius provides a gateway between users, multi-vendor Remote Access Servers and NetWare or Windows NT authentication*



## ***Centralize Administration of All Your RAS's***

Using Steel-Belted Radius, you'll be able to enter user profiles that determine which of your users are authorized to dial in or connect via a firewall to the network and what type of connection each user is permitted to make. It is no longer necessary to separately set up user profiles on each Remote Access Server as each RAS relies on Steel-Belted Radius as an authentication server to determine the rights of each user from a single, common database that you can administer easily.

## ***Leverage User Information Already in NetWare or NT***

Not only won't you have to separately administer RAS's, you also won't have to separately administer each user. Because Steel-Belted Radius is tightly woven into the NetWare and Microsoft NT fabric, you'll be able to specify profiles for many users all at once using your existing groupings. Work with the security you've already established: each user can be authenticated via the Bindery, NDS, or Windows NT using his or her current password.

## ***Multi-Vendor Support***

Because RADIUS is a standard, Steel-Belted Radius can be used with any RAS device that implements that standard. It is also possible for individual dial-in or firewall RAS vendors to create proprietary extensions to serve the particular needs of their servers.

Steel-Belted Radius incorporates proprietary extensions from a number of vendors using a flexible technique that allows it to accommodate vendor-specific extensions. All informational tokens that are passed between a RAS and Steel-Belted Radius are described in dictionaries. There is one basic dictionary that describes all standard tokens common to all implementations, and for each RAS vendor a separate dictionary describes the specific extensions of that vendor.

---

## The RADIUS Remote Access Environment

The RADIUS remote access environment has three components: Users, Remote Access Servers, and the RADIUS server. Each user is a client of a RAS; each RAS is both server to the user and client of the RADIUS server.

### ***The User***

The user is the person trying to gain access to the network from home or from the road.

Typically, the user has a SLIP or PPP dialer that allows him or her to dial into a Remote Access Server at the enterprise LAN and become a remote node on the enterprise network, with IP and/or IPX access to network resources.

### ***The Remote Access Server***

The Remote Access Server (or RAS) is a device that:

- ❑ Supports dial-in such as SLIP or PPP dial-in calls, authenticates each user via the RADIUS Server, and then routes that user onto the network.
- ❑ Supports direct connections to the network through a firewall, authenticates each user via the Radius Server, and then grants network access with specific rights.
- ❑ Forwards requests from another RAS using “Proxy Radius;” this is like call-forwarding, where an ISP can direct all authentication and accounting transactions to your LAN’s RADIUS server.

Examples of dial-in RAS’s which support the Radius standard include the Ascend MAX, Bay Networks’ Annex, Shiva LAN Rover, Telebit NetBlazer, and the US Robotics’ Total Control; firewall products include Raptor’s Eagle.

Most RAS devices can handle multiple dial-in users at once, and the corporate network might include a single RAS or multiple RAS’s working in tandem.

### ***The RADIUS Server***

The RADIUS Server accepts authentication requests from one or more Remote Access Servers, performs the authentication, and responds with the result — either an accept or a reject. The RADIUS server also provides Accounting services, if the RAS can support this.

A typical installation will include a single RADIUS server, for example, Steel-Belted Radius, to handle all the Remote Access Servers. Companies with Remote Access Servers at multiple sites could elect to have a separate RADIUS Server at each site; or, if the various sites were linked over a WAN of reasonable speed or over the Internet, a single RADIUS server could be made to handle multiple Remote Access Servers at multiple sites.

---

## RADIUS Authentication

The primary function of the RADIUS server is authentication. This section covers the following areas critical to an understanding of authentication:

- ❑ What happens during the authentication process
- ❑ Types of authentication available
- ❑ RADIUS attribute exchange
- ❑ RADIUS dictionaries

### ***What Happens During Authentication***

It may be instructive to follow the steps involved in a typical transaction in which a user successfully gains access to the network via Radius authentication.

- 1 A user dials in to one of several RAS's and PPP negotiation begins.
- 2 The RAS passes authentication information — username and password — obtained during PPP negotiations to the RADIUS server.
- 3 If the RADIUS server is able to authenticate the user, it issues an accept response to the RAS, along with profile information required by the RAS to set up the connection (this might include IP address, NetWare network number, maximum connect time, and the like).

If the RADIUS server is unable to authenticate the user, it issues a reject response to the RAS, along with a text string indicating the reason.

- 4 Using this information, the RAS completes PPP negotiation with the user:

If the RAS received an accept response, it can now allow the user to begin operating on the network.

If the RAS received a reject response, it terminates the user's connection, possibly passing on the reason for termination for display at the user terminal.

### ***Authentication Types***

During an authentication transaction, password information is transmitted between the RAS and the RADIUS server. The password information is encrypted using a secret key that you enter both at the RAS and at the Radius server.

The password information originally comes from the user, usually as part of PPP negotiations. The RAS is really just an intermediary here, and it is best to think of authentication as being a transaction between the user and the RADIUS server.

### ***Authentication Between the User and RAS***

There are two types of authentication transactions used between a remote access user and RAS. Each represents a method of authentication used in PPP:

- ❑ PAP (Password Authentication Protocol) is very simple. The user sends his or her password to the RADIUS server, and the RADIUS server validates it, either against its own database or against the NetWare Bindery or NDS or the Microsoft NT Domain or Workgroup.

Of the two legs of the journey the password takes between user and RADIUS server, the first leg is usually unencrypted, and the RAS gets the password from

the user in clear text. For the second leg, the RAS encrypts the password and the RADIUS server decrypts it using a shared secret key.

Ultimately, the RADIUS server has the password in clear text form and is able to make use of it directly for authentication.

- ❑ CHAP (Challenge Handshake Authentication Protocol) avoids sending passwords in clear text over any communication link.

With CHAP, the RAS generates a random number (the challenge) and sends it to the user. The user's PPP client creates a "digest" — a one-way encryption — of the password concatenated with the challenge, and sends this digest to the RAS. Because the digest is a one-way encryption, the RADIUS server cannot recover the password from the digest. What it can do is perform the identical digest operation using its own copy of the user's password stored in its database; if the two digests match, the user is authenticated.

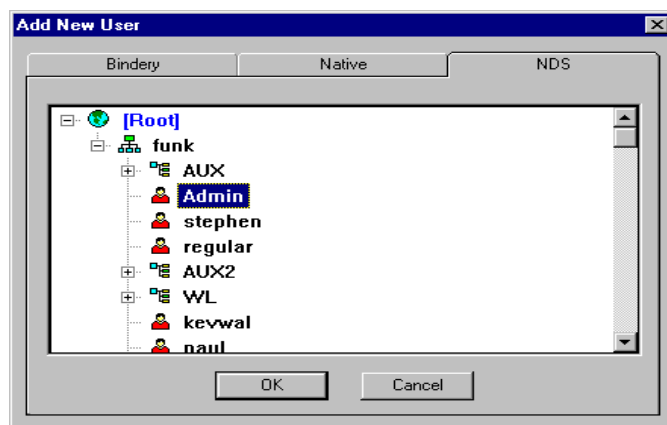
## ***How Steel-Belted Radius Performs Authentication***

Steel-Belted Radius has a number of options for performing the actual authentication. All of the methods that rely on NetWare or Windows NT security for authentication require that the authentication be done with PAP; only Native authentication permits the use of either PAP or CHAP.

You can choose to use one or more of the following authentication methods:

- ❑ Native authentication using a locally-based database on the Steel-Belted Radius server
- ❑ NetWare-based authentication as a:
  - **Bindery User** on a NetWare file server;
  - **Bindery Group** on a NetWare file server;
  - **NDS User** as a distinguished name in the NDS tree;
  - **NDS Group** as a distinguished name of a group in the NDS tree; or
  - **NDS Context** as a distinguished name of a container object in the NDS tree.

*Figure 2: Steel-Belted Radius allows authentication based on a NetWare Bindery User, Group, or as an NDS User, Group or Context*



- Windows NT-based authentication as a:
  - **Domain User** within a Windows NT Domain.
  - **Domain Group** within a Windows NT Domain.
  - **Workgroup User** on a specified workgroup machine.

---

## RADIUS Attribute Exchange

The authentication transaction serves an additional purpose beyond simply authenticating the user.

Along with the authentication information that the RAS includes as part of a RADIUS request, the RAS also passes information about the type of connection the user is trying to establish. The RADIUS server can use this information to further qualify the user, possibly issuing a reject based on this information.

Similarly, the RADIUS server includes additional information as part of the accept response it issues to the RAS. The RAS uses this information to control various aspects of the user's connection.

This aspect of the authentication transaction is called "attribute exchange."

Attribute exchange is controlled by the user's profile. Each profile lists attributes of two types:

### ***Check-list attributes***

Check-list attributes define a set of requirements for the connection. During the authentication transaction, the RAS must send attributes to the RADIUS Server that match the check-list; if they don't, the RADIUS server will issue a reject even if the user can be authenticated.

For example, by including appropriate attributes in the check-list, a variety of rules could be enforced. Only certain users might be permitted to use ISDN connections, or dial in to a particular RAS. Or, Caller ID could be used to validate a user against a list of legal originating phone numbers.

### ***Return-list attributes***

Return-list attributes are the attributes that the RADIUS server sends back to the RAS once authentication is successful. The return-list defines additional parameters that the RAS should assign to the connection, typically as part of PPP negotiations.

For example, specific users could be assigned particular IP addresses or IPX network numbers, IP header compression could be turned on or off, or a time limit could be assigned to the connection.

### ***Dictionary Files***

The RADIUS server uses Dictionary files to establish check-list and return-list attribute values. The Dictionary file contains the RAS-specific, proprietary items which may be set for a user. Steel-Belted Radius provides pre-configured dictionary files for popular RAS products.

## RADIUS Accounting and Reporting

RADIUS Accounting is an additional feature of the RADIUS standard that permits a RADIUS server to track when users start and stop their dial-in connections and to acquire statistics about each session.

Using RADIUS Accounting, the RADIUS server can maintain a:

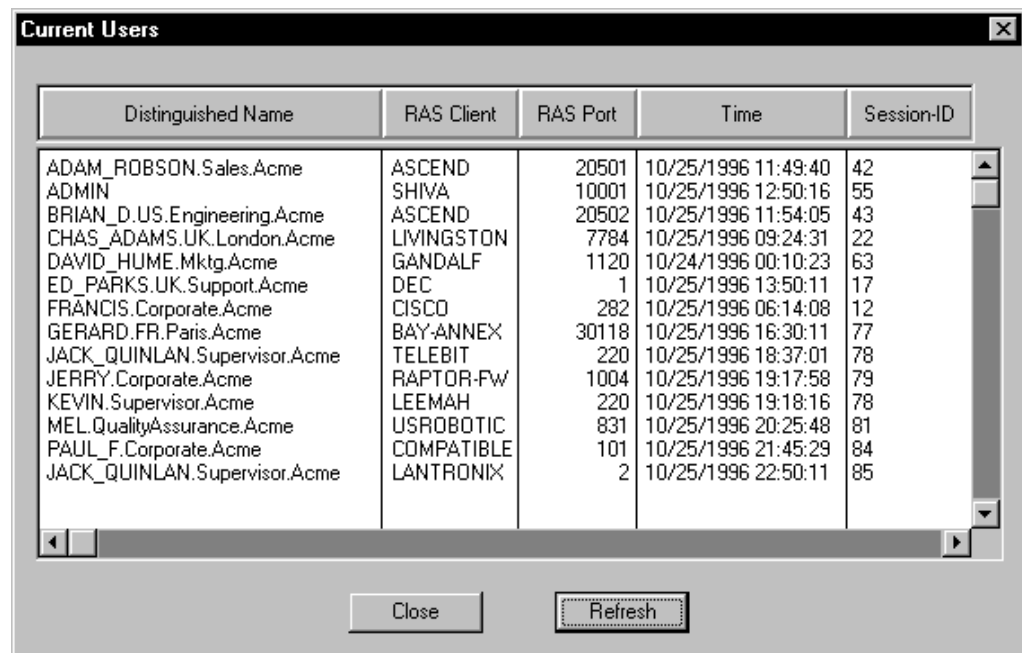
- ❑ History of all user dial-in sessions, indicating start time, stop time, and various statistics for the session
- ❑ Current User list indicating which users are currently connected to which Remote Access Servers

Steel-Belted Radius fully supports RADIUS Accounting. All Accounting transactions are logged to a comma-delimited file that can be imported into standard word processors, spreadsheets, and database programs for report generation and billing

One of the most useful capabilities provided by Steel-Belted Radius is a real-time list of active RADIUS users displayed from the Administrator program in the Current Users dialog. For every active dial-in session, a line is displayed containing the following fields:

- ❑ Distinguished Name shows the full username which was used for the authentication; if the username is part of NetWare Directory Services (NDS), this will represent the NDS common name or container object name prepended with the user name.
- ❑ RAS-Client shows the Remote Access Server (RAS) identification, which will either be the RAS's name or IP address.
- ❑ RAS Port shows the Remote Access Server (or RAS) port number, which represents a unique port number on the RAS.
- ❑ Time contains the date and time which the connection was started, according to the accounting transactions.
- ❑ Session ID contains the unique key for the session generated by Steel-Belted Radius.

*Figure 3: Steel-Belted RADIUS provides a Current Users snapshot showing every current connection made through all RAS devices*



The screenshot shows a window titled "Current Users" with a table of active sessions. The table has five columns: Distinguished Name, RAS Client, RAS Port, Time, and Session-ID. There are 18 rows of data. At the bottom of the window are "Close" and "Refresh" buttons.

Distinguished Name	RAS Client	RAS Port	Time	Session-ID
ADAM_ROBSON.Sales.Acme	ASCEND	20501	10/25/1996 11:49:40	42
ADMIN	SHIVA	10001	10/25/1996 12:50:16	55
BRIAN_D.US.Engineering.Acme	ASCEND	20502	10/25/1996 11:54:05	43
CHAS_ADAMS.UK.London.Acme	LIVINGSTON	7784	10/25/1996 09:24:31	22
DAVID_HUME.Mktg.Acme	GANDALF	1120	10/24/1996 00:10:23	63
ED_PARKS.UK.Support.Acme	DEC	1	10/25/1996 13:50:11	17
FRANCIS.Corporate.Acme	CISCO	282	10/25/1996 06:14:08	12
GERARD.FR.Paris.Acme	BAY-ANNEX	30118	10/25/1996 16:30:11	77
JACK_QUINLAN.Supervisor.Acme	TELEBIT	220	10/25/1996 18:37:01	78
JERRY.Corporate.Acme	RAPTOR-FW	1004	10/25/1996 19:17:58	79
KEVIN.Supervisor.Acme	LEEMAH	220	10/25/1996 19:18:16	78
MEL.QualityAssurance.Acme	USROBOTIC	831	10/25/1996 20:25:48	81
PAUL_F.Corporate.Acme	COMPATIBLE	101	10/25/1996 21:45:29	84
JACK_QUINLAN.Supervisor.Acme	LANTRONIX	2	10/25/1996 22:50:11	85

---

## Conclusion

While remote access offers tremendous opportunities for organizations it brings with it a set of management issues. Most environments today are already using some type of authentication to manage access such as that provided by Novell NetWare or Microsoft Windows NT. It makes sense to use the existing infrastructure to manage all types of remote access for authentication, authorization, and accounting. Plus, this yields increased security, since all access is managed centrally and can be audited with full assurance that all entries into the LAN can be accounted for.

The major remote access and firewall vendors support Steel-Belted Radius, so that your investment in NetWare and Windows NT is protected.

*Figure 4: Steel-Belted Radius provides full support for all vendors who conform to the RADIUS standard*

<b>ACC</b>	<b>IBM</b>
<b>Access Beyond</b>	<b>Lantronix</b>
<b>ADC Kentrox</b>	<b>LeeMah</b>
<b>3Com</b>	<b>Livingston</b>
<b>Ascend</b>	<b>Motorola</b>
<b>Bay Networks</b>	<b>Kasten Chase</b>
<b>Check Point</b>	<b>Perle</b>
<b>Cisco</b>	<b>Raptor Systems</b>
<b>Compatible Systems</b>	<b>Shiva</b>
<b>Digi International</b>	<b>Telebit</b>
<b>DEC</b>	<b>US Robotics</b>
<b>Gandalf</b>	<b>Xyplex</b>

---

## The Steel-Belted Radius Solution

Steel-Belted Radius provides a complete solution to centralizing authentication and accounting for all remote access. Because it integrates dial-in remote node, Internet firewall, and virtual private network access with the existing NetWare or Windows NT databases, it simplifies administration. And because it runs as an NLM or Windows NT service right on the network file server, it does not require expensive and difficult-to-manage hardware devices. Steel-Belted Radius provides the most sophisticated management technologies available today.

For more information about Steel-Belted Radius, please contact us.



Funk Software, Inc.  
222 Third Street  
Cambridge, MA 02142  
(617) 497-6339  
(617) 547-1031 fax  
sales@funk.com  
<http://www.funk.com>

rad-rsa1.doc 96.12.30