Chapter 10

Integrating RAD-Series RADIUS Server

Use the information in this chapter to integrate the RAD-Series RADIUS Server with JUNOSe routers. See the *SRC-PE Release Notes* for information about compatibility of this SRC release with RAD-Series RADIUS Server releases. The SRC software does not support the use of RADIUS with JUNOS routing platforms.

Topics in this chapter include:

Information about the simpler case of integrating Interlink Networks RAD-Series RADIUS Server with the JUNOSe router (without using the SRC software) is provided.

The SRC software can take advantage of a RADIUS server to authenticate against an LDAP server, which is used to store subscriber and service information, among other items.

System Requirements for the RAD-Series RADIUS Server

The following system requirements are recommended:

- Operating system—Sun Solaris 8 or Sun Solaris 9
- RAM—At least 128 MB of working memory
- Disk—Depends on external database support and storage time of the accounting log files; at least 50 MB of hard-disk space

Installing the RAD-Series RADIUS Server

You need the RAD-Series RADIUS Server software CD to complete this procedure. You can acquire the software from Interlink Networks, Inc. See

http://www.interlinknetworks.com

To install the RAD-Series RADIUS Server software:

1. Log in as `root`.
2. Change the directory to the location where the installation binary is located. Run the command:

   ```
   sh RAD-Series.6.0.solaris.bin
   ```

   The system asks for the product features to be installed. Select at least the following features:

   - RADIUS Binary Components
   - RADIUS Configuration Files
   - Server Manager
   - Remote Control

3. Enter the binary directory. For example:

   /opt/UMC/aaa

4. Enter the configuration directory. For example:

   /opt/UMC/aaa/etc

5. When prompted, enter the data directory. For example:

   /opt/UMC/aaa/var

6. Enter the documentation directory. For example:

   /opt/UMC/aaa/doc

7. Enter the path where you want to install Tomcat. For example:

   /opt/UMC/aaa/tomcat

8. When prompted for the shared secret, type:

   ```
   secret
   ```

9. When prompted for the test user password, type:

   ```
   secret
   ```

10. When prompted for the Server Manager user, type:

    ```
    admin
    ```

11. When prompted for the Server Manager password, type:

    ```
    radius
    ```

    When the installation is complete, the following line appears:

    ```
    Installation Complete
    ```

    The software has been successfully installed to:

    ```
    /opt/UMC/aaa
    /opt/UMC/aaa/etc
    /opt/UMC/aaa/var
    /opt/UMC/aaa/tomcat
    /opt/UMC/aaa/doc
    ```

12. To exit the installer, press Enter.

NOTE: See the Interlink Networks RAD-Series RADIUS Server *Getting Started Guide* for information about configuring the server and verifying the installation. The document is located at: */opt/UMC/aaa/doc/doc/gstarted.pdf*.

LDAP Features for the RAD-Series RADIUS Server

The RAD-Series RADIUS Server package is composed of functional building blocks called authentication/authorization transfer vectors (AATVs). These AATVs perform a specific function, such as UNIX password checking or authentication against an LDAP directory.

LDAP authentication allows all user configurations to be done and stored in the LDAP directory, eliminating the need to edit the server's configuration files to change user information. In addition to being a policy repository, the LDAP directory also replaces the user's file or the UNIX password file as the place to store a user ID and password. Performance is higher when one is dealing with a large number of users.

The ProLDAP AATV is an authentication AATV that performs two functions. First, it checks the validity of the user's ID and password. Second, if authentication is successful, the AATV loads attribute value pairs into the aaaCheck-list, aaaDeny-list, and aaaReply-list in the authentication request. The ProLDAP AATV uses a set of asynchronous LDAP API functions that allow an LDAP search, for example, to be sent out to a directory server without waiting for the search result to come back. Later on, the owner of the search may poll the LDAP client to find out if any result is available from the search.

The ProLDAP AATV is designed to work with different LDAP directory configurations. The directory may be configured to either allow or not allow the user password to be returned to the AAA server in an LDAP search. The ProLDAP AATV may be configured to first try searching for the user in the directory. If the password is returned, the ProLDAP AATV makes a password comparison to authenticate the user. Otherwise, the ProLDAP AATV will try to bind the user to the directory with the given password. ProLDAP may be configured to do a bind or search operation, but only if the directories are known to support those configurations.

Configuration of the LDAP search operations based on realms is described in *Configuring LDAP Authentication for the RAD-Series RADIUS Server* on page 91.

Configuring UDP Ports for the RAD-Series RADIUS Server

The transaction-based RADIUS protocol uses two UDP ports: one for authentication packets and one for accounting packets. The ports must be configured on two sides: RAD-Series RADIUS Server and the RADIUS clients (SRC software and JUNOSe router).

The officially assigned UDP port numbers are:

- 1812 for authentication
- 1813 for accounting

Early deployments of RADIUS used 1645/UDP for authentication packets and 1646/UDP for accounting packets.

Both RAD-Series RADIUS Server and the JUNOSe router use the official ports by default. If you decide to use different ports, you can change the port after you start RAD-Series RADIUS Server. See *Starting and Stopping RAD-Series Server Manager* on page 89.

Starting and Stopping RAD-Series Server Manager

To open RAD-Series Server Manager:

1. Start Tomcat by entering:

   /opt/aaa/tomcat/bin/startup.sh

2. Enter the following URL into your Web browser:

   http://<ip-address of server>:8080/aaa/index.html

3. When prompted for the Server Manager username, enter:

   admin

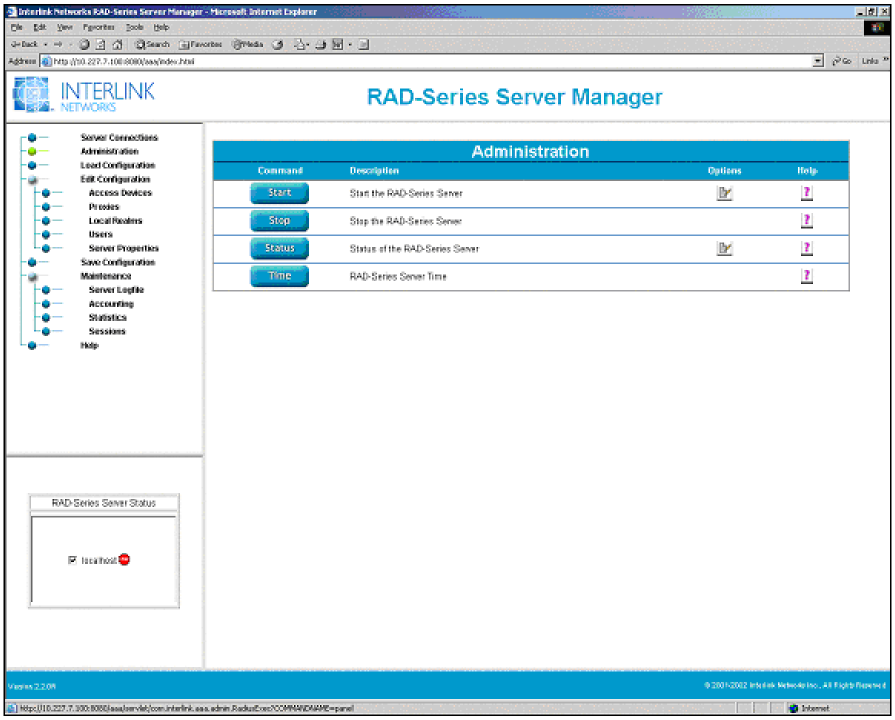
4. When prompted for the Server Manager password, enter:

   radius

NOTE: You must use the same administrator and password that you supplied during the installation.

5. From the navigation pane, click **Administration**.

   The Administration pane appears.



Administration

Command	Description	Options	Help
Start	Start the RAD-Series Server		?
Stop	Stop the RAD-Series Server		?
Status	Status of the RAD-Series Server		?
Time	RAD-Series Server Time		?

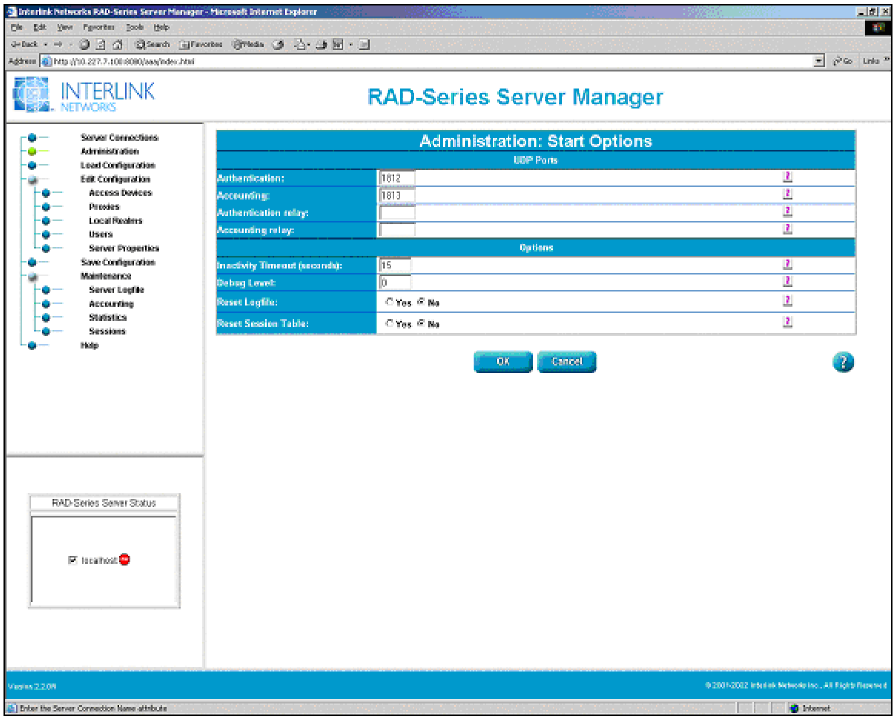
To start or stop RAD-Series Server Manager, click the Start or Stop button. When RAD-Series Server Manager is running, the bullet in the navigation pane turns green. When RAD-Series Server Manager is not running, it is blue.

Changing the UDP Ports

To use UDP ports other than the default ports described in *Configuring UDP Ports for the RAD-Series RADIUS Server* on page 88:

1. Click the **Options** button located to the right of the **Start** button.

   The following pane appears.



Administration: Start Options

UDP Ports

Authentication:	1812
Accounting:	1813
Authentication relay:	
Accounting relay:	

Options

Inactivity Timeout (seconds):	15
Debug Level:	0
Reset Logfile:	○ Yes ● No
Reset Session Table:	○ Yes ● No

2. Under UDP Ports, enter the new Authentication and Accounting port settings.

3. Click **OK**.

Extending Dictionary Files with JUNOSe Parameters for the RAD-Series RADIUS Server

In addition to supporting standard RADIUS attributes, the JUNOSe router supports JUNOSe-specific attributes. These attributes must be introduced to RAD-Series RADIUS Server. You must use the RADIUS attributes for both RAD-Series RADIUS Server–JUNOSe router integration and RAD-Series RADIUS Server–JUNOSe router–SRC integration.

The RAD-Series RADIUS Server package still uses the old Unisphere VSAs in their dictionary file. You must edit the dictionary file (located in */opt/aaa/etc*) and replace the Unisphere attributes with the JUNOSe extensions in the ERX RADIUS Dictionary file. To locate the ERX RADIUS Dictionary file, see the JUNOSe software documentation for the supported release on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/

The next step defines the JUNOSe router as the network access server (NAS) to be recognized by RAD-Series RADIUS Server. This step involves the extension of the vendor file. The vendor file is located in */opt/aaa/etc*.

The vendor file contains a list of zero or more vendor entries. Each vendor entry contains a vendor name and a vendor number. Each entry optionally contains an interim way of mapping external (with respect to the RADIUS server) attribute numbers to internal (with respect to the RADIUS server) vendor-specific attributes. This optional mapping is used on RADIUS requests and responses. Again, RAD-Series RADIUS Server still uses the Unisphere Networks extension. Edit the vendor file and replace Unisphere with Juniper. The ID should remain at 4874.

The modified lines look like the following:

```
# Juniper Networks
Juniper.attr         Juniper.value        4874    Juniper
```

Configuring LDAP Authentication for the RAD-Series RADIUS Server

The SRC software assumes that all RADIUS authentications are performed against the SDX LDAP directory. This section also applies to RAD-Series Server integration with a JUNOSe router if RAD-Series RADIUS Server authenticates against an LDAP directory.

Tasks to configure LDAP authentication for the RAD-Series RADIUS Server are:

- Configuring the RAD-Series Server Manager on page 92
- Configuring Realm Administration on page 94
- Configuring LDAP Settings on page 95
- Configuring RADIUS Profiles with the LDAP Directory on page 95

Configuring the RAD-Series Server Manager

The RAD-Series Server Manager configuration for the ProLDAP AATV is done through the *authfile* file, which is stored in the configuration directory */opt/aaa/etc*. The configuration can be performed either manually by editing the authfile or through the Administration panes of RAD-Series Server Manager. The following methods are to be configured:

- How RAD-Series RADIUS Server authenticates
- Which external database is used for authentication, based on the realm name

Administrators must create a table in the *authfile* file for each realm name.

```
realm PROLDAP description
{
Filter-Type bin | cis

Directory directory-1
{
Host dir1.host.com
Port port-number
Administrator directory-manager-dn
[Password directory-manager-password]
SearchBase realm-search-base-in-directory
Authenticate Auto | Bind | Search
}
...
}
```

where

- realm—Identifies realm name, which is used during PPP login (username@realm). The special value NULL specifies treatment of any incoming access request, where no realm name is submitted during the PPP login.
- PROLDAP—Identifies that this table is valid for the ProLDAP AATV.
- Filter-Type—Identifies the treatment of the user ID. Valid values are either case sensitive (bin) or not case sensitive (cis).
- Directory—Identifies the start of the directory section. Up to four directory sections are supported per realm. If the value contains spaces or tabs, it must be enclosed by either the double-quote or the single-quote character. RAD-Series RADIUS Server uses the round-robin method for those identified directories.
- Host—The value (fully qualified DNS name or IP address) identifies the LDAP directory.
- Port—Identifies the port the LDAP server listens to.
- Administrator—DN, which specifies the user entry that RAD-Series RADIUS Server uses to log in against the LDAP directory. This must be specified if Authenticate is set to Search.

- SearchBase—DN, which represents the starting point of the LDAP search operation for that realm.
- Authenticate—Identifies how RAD-Series RADIUS Server authenticates incoming access requests. Valid values are:
    - Auto—RAD-Series RADIUS Server performs a search as the configured administrator (searches anonymously if no configured administrator), anticipating that the password is in the result. It binds as the user if the password is not available.
    - Bind—RAD-Series RADIUS Server tries to bind with the user ID and password specified during the PPP login.
    - Search—RAD-Series RADIUS Server binds and performs a search operation. LDAP returns the user password, which is compared with the submitted password during the PPP login.

NOTE: The SRC software uses the search option.

The following *authfile* example depicts the treatment of PPP logins without any realms and with the realm name isp1.com.

```
# This is a realm entry for an LDAP Server with PROLDAP with NO Realm
#
NULL  PROLDAP Default-Setting
{
        Filter-Type BIN
        Directory SSC
        {
                Host 123.45.3.1
                Port 389
                Administrator "cn=umcadmin, o=umc"
                Password      "umc"
                SearchBase    "retailerName=default, o=users, o=umc"
                Authenticate  search
        }
}
# This is a realm entry for two LDAP Server with PROLDAP with Realm isp1.com
#
virneo.com  PROLDAP Virneo-Setting
{
       Filter-Type BIN
       Directory virneo
       {
               Host 245.3.4.5
               Port 389
               Administrator "cn=umcadmin, o=umc"
               Password      "umc"
               SearchBase    "retailerName=SP, o=users, o=umc"
               Authenticate  search
       }
```

```
Directory virneo-backup
   {
          Host 245.3.4.6
          Port 389
          Administrator "cn=umcadmin, o=umc"
          Password      "umc"
          SearchBase    "retailerName=SP, o=users, o=umc"
          Authenticate  search
```

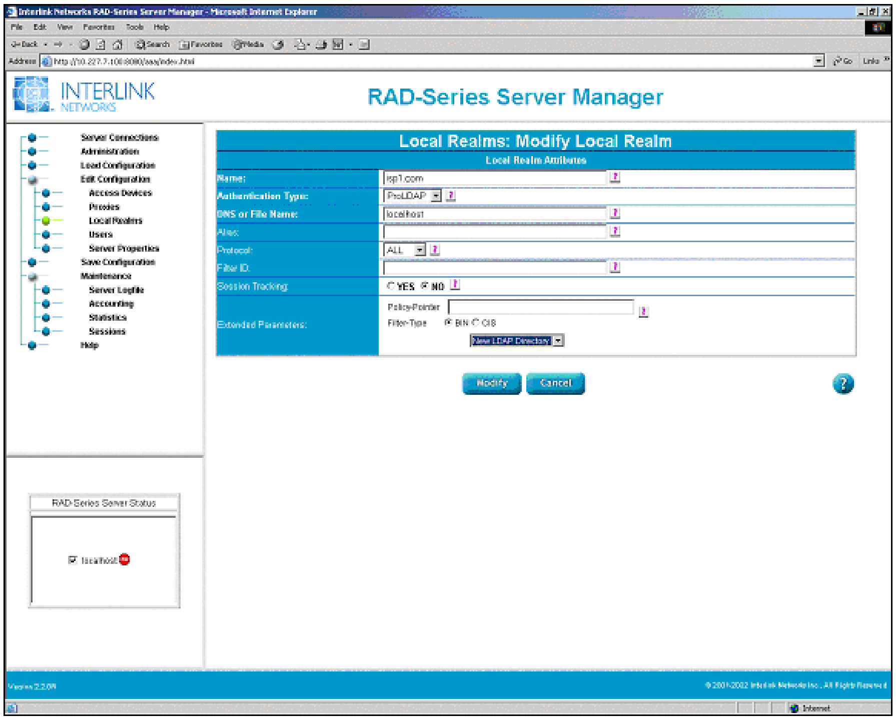
Configuring Realm Administration

The RAD-Series Server Manager allows you to perform realm administration.

To configure realm administration:

1. From the RAD-Series Server Manager navigation pane, click **Edit Configuration** and **Local Realms**.
2. Click on the **New Local Realm** link.

   The Local Realms: Modify Local Realm pane appears.



Local Realms: Modify Local Realm

Local Realm Attributes

Name:	isp1.com
Authentication Type:	ProLDAP
DNS or File Name:	localhost
Alias:	
Protocol:	ALL
Filter ID:	
Session Tracking:	○ YES ● NO
Extended Parameters:	Policy-Pointer Filter-Type ● BIN ○ CIS New LDAP Directory

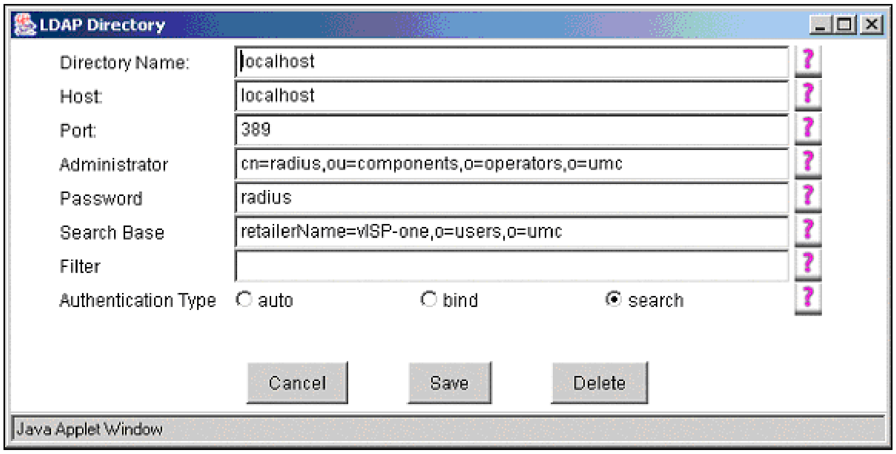
3. Specify the realm attributes.
4. Click **Modify**.

Configuring LDAP Settings

To configure the LDAP settings:

1. Select **New LDAP Directory**.

   The LDAP Directory window appears.



Directory Name: localhost
Host: localhost
Port: 389
Administrator: cn=radius,ou=components,o=operators,o=umc
Password: radius
Search Base: retailerName=vISP-one,o=users,o=umc
Filter:
Authentication Type: ○ auto ○ bind ● search

2. Specify the attributes.

3. Click **Save**.

Configuring RADIUS Profiles with the LDAP Directory

RADIUS servers search objects from the type umcRadiusPerson to authenticate incoming PPP sessions. If RADIUS and JUNOSe-specific attributes must be returned to the JUNOSe router during the authentication process, RAD-Series RADIUS Server expects some special AAA attributes:

- aaaReply—A response sent back from the server (for example, a session time limit)
- aaaCheck—An attribute that must be present in the user entry for the entry to evaluate as True
- aaaDeny —An attribute that must NOT be present in the user entry for the entry to evaluate as True

These attributes are multivalued attributes containing the RADIUS attribute value pairs to be processed by RAD-Series RADIUS Server.

The following example depicts a umcRadiusPerson object, which returns the RADIUS attribute values for Session-Timeout, Idle-Timeout, and Class, and the JUNOSe-specific attribute for the virtual router to be used on the JUNOSe router. This entry is shown in LDIF notation:

```
dn:serviceName=bras,uniqueID=jane,ou=local,retailerName=isp1,o=Users,
o=umc
objectClass: umcRadiusPerson
objectClass: umcServiceProfile
objectClass: top
uid: jane
userPassword: secret
serviceName: bras1
usedService: serviceName=bras,o=Services,o=umc
aaaReply: Virtual-Router-Name=Default
aaaReply: Class=1,uid,bras
aaaReply: Idle-Timeout=2700
aaaReply: Session-Timeout=10800
```

Example: RAD-Series RADIUS Server Accounting Log File Format

The following is an example of an accounting log file generated by the RAD-Series RADIUS Server with:

- Some accounting activity coming from the JUNOSe RADIUS client (tracking the activity of a PPP session).
- Some accounting activity coming from the SRC RADIUS client (a video service being activated, then deactivated).

```
Tue May  1 10:58:42 2001
    Acct-Status-Type = Start
    User-Name = "user1@isp1"
    Event-Time = "May  1 2001"
    Acct-Delay-Time = 0
    NAS-Identifier = "OBIWAN"
    Acct-Session-Id = "erx fastEthernet 3/1::0000022073"
    NAS-IP-Address = 10.227.9.145
    Service-Type = Framed
    Framed-Protocol = PPP
    Framed-IP-Address = 10.227.9.150
    Framed-IP-Netmask = 255.255.255.255
    Framed-Compression = None
    NAS-Port-Type = 15
    NAS-Port = 822083584
    NAS-Port-Id = "fastEthernet 3/1:"
    Ingress-Policy-Name = "unlim"
    Acct-Authentic = RADIUS
    User-Id = "user1"
    User-Realm = "isp1"

Tue May  1 10:59:49 2001
    Acct-Status-Type = Start
    Acct-Delay-Time = 0
    User-Name = "user1@isp1"
    Acct-Session-Id = "sspServiceVideoG:user1:e634da23b6"
    NAS-Identifier = "SSP.lion"
    User-Id = "user1"
    User-Realm = "isp1"
```

```
Tue May  1 11:07:25 2001
    Acct-Status-Type = Stop
    Acct-Delay-Time = 0
    User-Name = "user1"
    Acct-Session-Id = "sspServiceVideoG:user1:e634da23b6"
    Acct-Input-Octets = 10681
    Acct-Input-Gigawords = 0
    Acct-Input-Packets = 94
    Acct-Output-Octets = 0
    Acct-Output-Gigawords = 0
    Acct-Output-Packets = 0
    Acct-Session-Time = 456
    NAS-Identifier = "SSP"
    User-Id = "user1"
    User-Realm = ""
    LAS-Start-Time = 988729189
    LAS-Code = LAS-Notlocal
    LAS-Duration = 456
```

Configuring the RAD-Series RADIUS Server and RADIUS Clients

For RAD-Series RADIUS Server and RADIUS clients (JUNOSe router and the SAE software) to communicate, you must configure both the client and the server.

Configuring the RAD-Series RADIUS Server

The RADIUS server must be able to communicate with the RADIUS clients. The following information about all RADIUS clients connected to the RADIUS server must be known to the RADIUS server:

- IP address of the RADIUS client
- RADIUS shared secret to be exchanged between RAD-Series RADIUS Server and the client
- Model (vendor) of the RADIUS client

Although the Administration panes allow you to create new clients, we recommend that you edit the */opt/aaa/etc/clients* file when creating new access devices. The client file should resemble the following:

```
#Client Name             Key            [type]     [version]       [prefix]
#----------------  --------------- --------------- ---------       --------
# SAE Client             192.23.3.10    secret     type=Juniper:NAS   v1
# Juniper ERX node (Enable the Juniper extensions)
                         192.23.3.1     secret     type=Juniper:NAS   v1
```

NOTE: The Administration panes do use Juniper in the vendor list. Without changing some HTML files, creating the Juniper RADIUS client will not work when you use the Administration panes.

Configuring RADIUS Clients

Each RADIUS client must be able to contact its RADIUS server. The following information is required for client/server communication:

- IP address of the RADIUS server
- RADIUS shared secret to be exchanged between RAD-Series RADIUS Server and the RADIUS client
- UDP ports on which the RADIUS client sends and receives RADIUS authentication and accounting packets. The ports must match the server configuration.

The RADIUS client configuration of the JUNOSe router is described in the *JUNOSe Broadband Access Configuration Guide*.

Testing the RAD-Series RADIUS Server

You can test the RAD-Series RADIUS Server installation by using the radpwst tool. This tool is located in the */opt/aaa/bin* directory and has the following syntax:

```
radpwtst -d <conf directory>  -p <auth port>  -s <server name> -u <auth type>
-x -w < userPassword > <username>
```

where

- -d—Directory of users, clients, authfile, dictionary, etc. Configuration files
- -p—Port number to listen for auth requests on
- -s—IP Address or fully qualified DNS name of server, hosting RAD-Series RADIUS Server
- -u—Authentication-Type, always use *ppp*
- -x—Allows the user to turn on debugging output
- -w—Allows the user to provide a password on the command line and not be prompted

Include the */opt/aaa/lib* path in your LD_LIBRARY_PATH environment.

You can test your setup by typing:

```
/opt/aaa/bin/radpwst -d /opt/aaa/etc -p 1812 -s 'hostname' -u ppp -x -w secret
jane@virneo.com
```