Chapter 11

Integrating Steel-Belted Radius/SPE Server

The Juniper Networks Steel-Belted Radius/Service Provider Edition (SPE) server is a carrier-grade RADIUS/AAA solution. It provides the reliability, performance, and specialized technology demanded by carriers, wholesalers, and service providers. Use the information in this chapter to integrate the Steel-Belted Radius/SPE server with JUNOSe routers. Refer to the *SRC-PE Release Notes* for information about compatibility of this SRC release with Steel-Belted Radius/SPE server releases. The SRC software does not support the use of RADIUS with JUNOS routing platforms.

This chapter contains the following sections:

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 information.

System Requirements for the Steel-Belted Radius Server

The Solaris host software package includes:

- The RADIUS server process
- Java-based administration GUI
- A number of dictionary and database files to support various authentication methods

The software package requires:

- Operating system—Solaris 8 and higher
- RAM—At least 64 MB of working memory
- Disk—Depends on external database support; at least 105 MB of hard-disk space
- Browser for GUI—Java-capable browser that understands signed Java applets, such as Netscape 4.08 or later for Solaris

Installing the Steel-Belted Radius/SPE Software

You need the Steel-Belted Radius/SPE software CD and a valid license string. Use the procedure that is appropriate for your installation.

NOTE: For the remainder of the document, we assume that Steel-Belted Radius/SPE is installed in the directory */opt/UMC/SPE*.

Installing the Steel-Belted Radius Software for the First Time

To install the software for the first time:

1. Log in as `root`.
2. Copy files from */cdrom/cdrom0/*Unix to the Sun platforms (for example, to */tmp/funk*), and set your working directory to the directory to which the files were copied.
3. Run the **install.sh** script with the **-all** option. Type:

   sh install.sh -all

   The installation script prompts for the server directory.
4. Type the full pathname:

   /opt/UMC/SPE

   The installation script prompts for the license string.

5. Enter a valid license string.

   The installation script prompts for the type of installation from the following list.

   1. Steel-Belted Radius Enterprise Edition
   2. Steel-Belted Radius Service Provider Edition
   3. Steel-Belted Radius Global Enterprise Edition
   4. Steel-Belted Radius HotSpot Edition

6. Enter selection: [2] Steel-Belted Radius Service Provider Edition

   The installation script prompts for the directory in which the administration user interface should be installed.

7. Type the full pathname:

   /opt/UMC/SPE/radadmin

Installing the Steel-Belted Radius Software over Previous Installations

To install the software over a previous installation:

1. Complete the procedure in the previous section. The **install.sh** script may detect the following items on the machine:

   - RADIUS process already running
   - Steel-Belted Radius/SPE configuration files
   - Steel-Belted Radius/SPE database files

   The **install.sh** script prompts for the following message if the script discovers a running server:

   Server is running with pid <x>
   Stop radius server and unconfig/uninstall before
   Installing new version

2. Change to the installation directory of the Steel-Belted Radius/SPE package. You can find the server directory by typing the following command:

   ps -aef | grep radius

3. Stop the server by typing:

   ./S90radius stop

4. Change to your working directory. Unconfigure the previous installation, which removes the startup script and some entries in the */etc/services* and */etc/inetd.conf* files, which are used by the previously installed Steel-Belted Radius/SPE server. Type:

   sh install.sh -unconfig

5. When prompted, enter the path of the existing server directory.

6. Run the **install.sh** script with the **-all** option again. Type:

   sh install.sh -all

   The script checks for existing Steel-Belted Radius/SPE configuration files. The following prompt appears if files are detected:

   ```
   Previous configuration files exist
   Configuration files exist in <server_directory>
   Do you want to discard them? [n]
   ```

7. If you answer `n`, the previous configuration files are copied into the subdirectory *OLDCONFIG*. Otherwise, the previous files are overwritten.

   The script checks for existing Steel-Belted Radius/SPE database files. The following prompt appears if files are detected:

   ```
   Previous database files exist
   Database files exist in <server_directory>
   Do you want to discard them? [n]
   ```

8. If you answer `n`, the previous configuration files are not overwritten, and the new Steel-Belted Radius/SPE version uses the entire administrative database. Otherwise, the database files are overwritten.

   The script prompts you for the license string.

9. Enter a valid license string.

   The installation script prompts you for the directory in which the administration user interface should be installed.

10. Type the full pathname:

    /opt/UMC/SPE/radadmin

Enabling LDAP Authentication

Use this procedure to enable authentication through the LDAP directories. The SRC software requires that the LDAP be enabled as an external database. The LDAP host is used for authentication.

NOTE: The LDAP is not required for integration with just the JUNOSe router.

To enable an LDAP host as an external database used by the Steel-Belted Radius/SPE server.

1. Log in as `root`.

2. Return to the working directory (directory into which the installation files were originally copied; for example, */tmp/funk*).

3. Unconfigure the initial configuration of Steel-Belted Radius/SPE by running **install.sh** script with the **-unconfig** option. Enter the server directory.

```
# sh install.sh -unconfig
Enter server directory [<working-directory>/radius]: /opt/UMC/SPE
Removing  /etc/rc2.d/S90radius /etc/rc2.d/K90radius
Removing RADIUS entries from /etc/services
Removing RADIUS entries from /etc/inetd.conf
kill -HUP 124
Unconfig completed.
```

4. Configure Steel-Belted Radius/SPE with the external database by running **install.sh** with the **-config** option. You must enter the server directory again. In addition, you must select LDAP as the external database, and you must enter the path */opt/UMC/SPE* as the location of the LDAP libraries. In the following example, no SNMP support is configured (see the Steel-Belted Radius/SPE server manuals for more information about SNMP support).

```
# sh install.sh -config
Enter server directory [[<working-directory>/radius]: /opt/UMC/SPE
Creating S90radius.
Setting the default radius directory /opt/UMC/SPE
Do you want to configure SNMP? [n]: n
Do you want to configure for use with External SQL Databases? [n]: n
Do you want to configure LDAP? [n]: y
Enter path for LDAP library files. [/usr/lib/]: /opt/UMC/SPE
Configuration of LDAP complete. Copying S90radius to /opt/UMC/SPE
Creating link.
Radius server configuration completed. Configuring admin...
Modifying  /etc/services  ...
Modifying  /etc/inetd.conf  ...
kill -HUP 133
Admin configuration completed.
```

5. Copy the dictionary and vendor files (*dictiona.dcm*, *juniper.dct* and *vendor.ini*) for the JUNOSe release from the folder *steel_belted_radius* in the SRC software distribution, into the installation directory (*/opt/UMC/SPE*).

Configuring UDP Ports for Steel-Belted Radius Software

The transaction-based RADIUS protocol uses two UDP ports: one for authentication packets and one for accounting packets. You must configure the ports on both sides—the Steel-Belted Radius/SPE server and the RADIUS clients (SRC software and JUNOSe router). For information about RADIUS client/server configuration, see *Configuring the Steel-Belted Radius/SPE Server and RADIUS Clients* on page 137.

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.

The (ports) section of the RADIUS configuration file *radius.ini* allows you to set the UDP ports used for authentication and accounting and the UDPAuthPort and UDPAcctPort fields for port assignment. You can specify more than one port that the SPE server is listening to; for example:

- UDPAuthPort = 1812
- UDPAuthPort = 1645
- UDPAcctPort = 1813
- UDPAcctPort = 1646

If no port settings are present in the *radius.ini* file, the SPE server attempts to read the port numbers associated with the RADIUS servers from the */etc/services* file.

If no port settings are present in the *radius.ini* file and no RADIUS services are defined in the */etc/services* file, the SPE server listens to UDP ports 1645 and 1812 for authentication and UDP ports 1646 and 1813 for accounting.

Starting the Steel-Belted Radius/SPE Server

To start the RADIUS server:

1. Change to the <*server-directory*> */opt/UMC/SPE*.
2. Enter:

   ./S90radius start

   During startup, the RADIUS server binds to the LDAP server, which requires that the LDAP server be running before the RADIUS server is started. The RADIUS process is automatically started whenever the Solaris host is booted.

Stopping the Steel-Belted Radius/SPE Server

To stop the RADIUS server:

1. Change to the <*server-directory*> */opt/UMC/SPE*.
2. Enter:

   ./S90radius stop

Extending Dictionary Files with JUNOSe Parameters for the Steel-Belted Radius Server

In addition to supporting the standard RADIUS attributes, JUNOSe routers support JUNOSe-specific attributes. You must replace a file to introduce JUNOSe-specific attributes to the Steel-Belted Radius server. Replacing this file is necessary to complete both the Steel-Belted Radius–JUNOSe router integration and the Steel-Belted Radius–JUNOSe router–SRC integration.

To extend dictionary files with JUNOSe parameters, replace the *juniper.dct* dictionary file with 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 Juniper Networks dictionary file is included as part of the SRC installation media.

Configuring LDAP Authentication

The SRC software assumes that all RADIUS authentications are performed against the SDX LDAP directory. The information in this section also applies to the Steel-Belted Radius/SPE server integration with a JUNOSe router, provided that the Steel-Belted Radius/SPE server uses an LDAP server as an external database for authentication.

Integration of the JUNOSe-specific attributes, such as primary Domain Name System (DNS) and virtual router, must be performed. Steel-Belted Radius/SPE server supports such an external authentication method by using several configuration files.

These files tell the RADIUS server:

- How the RADIUS server communicates with an external database (LDAP)
- How the RADIUS server queries the external database for authentication
- How the RADIUS server formulates the response from the query result

You configure LDAP authentication by modifying properties in the *ldapauth.aut* file, which is located in the server directory (*opt/UMC/SPE*). If you do not specify options in this file, the SPE assumes the default values. You can also view a sample *ldapauth.aut* file in the SRC software distribution in the folder *steel_belted_radius*.

The sections of the LDAP authentication file are described below.

[Bootstrap] Section

The [Bootstrap] section specifies information that the Steel-Belted Radius/SPE server uses to load and start the LDAP authentication plug-in. You must set the library used, and you must enable LDAP authentication.

This section should look like:

```
[Bootstrap]
LibraryName=ldapauth.so
Enable=1
InitializationString=LDAP
```

[Settings] Section

The [Settings] section forms a basis for all Bind and Search requests against the LDAP server. The information presented here applies to all LDAP servers specified in this file.

Steel-Belted Radius/SPE supports two kinds of LDAP authentication:

- Bind—Steel-Belted Radius/SPE attempts to bind to the LDAP server, using the username and password from the incoming access request (one authentication is performed at one time).
- BindName—Steel-Belted Radius/SPE binds once with credentials to the LDAP server and performs a Search operation against the LDAP server to validate username and password from the incoming access request (multiple authentications are performed at the same time).

The SRC software supports the BindName option, which must be specified in the [Settings] section. The BindName option requires specifying credentials, which Steel-Belted Radius/SPE uses to bind against the LDAP directory. If you want to use the same credentials for each LDAP directory, specify BindName and BindPassword in the [Settings] section; otherwise, use the [Server/name] sections, as described below:

- LogLevel—Activates LDAP logging, written into the activity log file (<*date*>*.log*)
- PasswordFormat—Identifies whether RADIUS handles clear-text, UNIXcrypt, or SHA1 + Base64 hash-encrypted passwords. The value auto instructs Steel-Belted Radius/SPE to parse each password value that it retrieves from the LDAP server.
    - PasswordCase—Tells SPE whether the password is always converted to uppercase or to lowercase or not converted at all. The default is Original.
    - UpperCaseName—Identifies whether the username is converted to uppercase or not. The default is 0 (no conversion).

The **Search** option specifies a string name, referencing to a section where the LDAP Search request is specified.

The section looks like the following:

```
[Settings]
MaxConcurrent=25
Timeout=20
ConnectTimeout=25
QueryTimeout=10
WaitReconnect=2
MaxWaitReconnect=360
LogLevel = 0
UpperCaseName = 0
PasswordCase=original
PasswordFormat=auto
Search = DoLdapSearch
SSL = 0
```

[Server] Section

The [Server] section lists the LDAP servers that may be used to perform authentication. Optionally, it also can be used to specify multiple LDAP servers for load balancing or backup. If more than one LDAP server is specified, Steel-Belted Radius/SPE always uses round-robin. The following depicts how to list one or more LDAP servers.

The list contains serverName = TargetNumber pairs, where the serverName is used in the [server/serverName] section, described in the next paragraph. TargetNumber is an activation target number that controls when the server is activated for backup. TargetNumber is optional and may be left blank. For example:

```
[Server]
s1=
s2=
s3=
```

[Server/serverName] Section

Each [server/serverName] section contains information about a single LDAP server. You must provide a [server/serverName] section for each server you specify in the [server] section. The value for Host identifies the IP address of the LDAP server, and the value for Port specifies the port used for LDAP communications. By default, any LDAP server listens at port 389. The credentials used by Steel-Belted Radius/SPE to bind to the LDAP server are specified in BindName and BindPassword. The SSL value indicates whether an SSL connection is used for the RADIUS-LDAP connection. If the last three mentioned parameters are not specified, Steel-Belted Radius/SPE takes the configuration out of the [Settings] section.

```
[Server/s1]
Host=127.0.0.1
Port=389
BindName=cn=radius,ou=components,o=operators,o=umc
BindPassword=radius
SSL=0

[Server/s2]
```

```
Host=10.20.2.12
Port=389

[Server/s3]
Host=10.10.40.19
Port=389
```

[Search/name] Section

The referenced [Search/name] section includes the search filter, base object, scope, and attribute list, which are included in the LDAP Search operation. If you reference this section in the [Settings] section, the specified options are valid for all LDAP directories. If you want to specify separate Search options for each LDAP directory, you must reference this section in each [server/name] section. In the following example, "DoLdapSearch" is used as name.

NOTE: This name is referenced in the [Settings] section.

Because the SRC software uses the BindName authentication method, you must ensure that the user's password is included in the attribute list, referenced by the attributes option. In the SRC software case, we would like to search only objects where the LDAP attribute uid matches the specified username, and we therefore set *Filter = uid = < User-Name >* . The location within the directory where the search is started is specified in the Base variable. The SRC software for residential users uses the base *retailerName = default, o = Users, o = umc*. The scope of the search is a subtree search (Scope = 2). The variable *%DN* is used for holding the distinguished name of the LDAP search result. The attribute list is a reference to another section of the *ldapauth.aut* file.

```
[Search/DoLdapSearch]
Base=retailerName=default,o=users,o=umc
Scope=2Filter=uid=<User-Name>
Attributes = AttrList
Timeout = 20
%DN = dn
```

For another authentication strategy, see *Configuring Directed Authentication* on page 136. This strategy is more suited for cases in which the service provider outsources services from retailer ISPs.

[Attribute/name] Section

Within the [Attribute/name] section, the LDAP attributes are determined, which are requested by the LDAP search. If the entry that matches the search filter contains values of these attribute types, these values will be part of the search result; RADIUS uses them in the values for checking and replying purposes. Again, the user password attribute is mandatory in the BindName authentication method, which is used in our case. The [Attribute/name] section looks like the following:

```
[Attributes/AttrList]
userPassword
uid
alternateCliAuthLevel
alternateCliVrouterName
```

ascendFilterCmd
atmMBS
atmPCR
atmSCR
atmServiceCategory
cliAllowAllVRAccess
cliInitialAccessLevel
egressPolicyName
egressStatistics
framedIpRouteTag
igmpEnable
ingressPolicyName
ingressStatistics
ipv6LocalInterface
ipv6PrimaryDNS
ipv6SecondaryDNS
ipv6VirtualRouter
localAddressPool
localInterface
pppoeDescription
pppoeMaxSessions
pppoeUrl
qosProfileName
qosProfileInterfaceType
radiusChapPassword
radiusAcctInterimInterval
radiusCalledStationId
radiusCallingStationId
radiusConnectInfo
radiusFilterId
radiusFramedIPAddress
radiusFramedIPNetmask
radiusReplyMessage
radiusFramedProtocol
radiusFramedRoute
radiusFramedPool
radiusSessionTimeOut
radiusNASIdentifier
radiusNASIPAddress
radiusNASPort
radiusNASPortId
radiusNASPortType
radiusClass
radiusIdleTimeOut
radiusServiceType
redirectVRName
pppAuthenticateProtocol
pppPassword
pppUsername
primaryDNS
secondaryDNS
primaryWINS
saValidate
sdxServiceName
sessionVolumeQuota
secondaryWINS
serviceBundle

```
tunnelAssignmentID
tunnelClientEndPoint
tunnelClientAuthID
tunnelMaximumSessions
tunnelMediumType
tunnelNasPortMethod
tunnelPreference
tunnelTOS
tunnelType
tunnelServerEndPoint
tunnelServerAuthID
tunnelPassword
tunnelVirtualRouter
tunnelBearerType
tunnelDialoutNumber
tunnelInterfaceId
tunnelMaximumBps
tunnelMinimumBps
virtualRouterName
```

[Request] Section

In the [Request] section, the incoming RADIUS attributes (from Access-Request) must be determined and mapped to LDAP attributes. Steel-Belted Radius/SPE places these values in the variable table before moving on to the LDAP Bind and Search requests as defined earlier.

```
[Request]
%UserName = User-Name
NAS-IP-Address = radiusNASIPAddress
NAS-Port = radiusNASPort
Service-Type = radiusServiceType
```

[Response] Section

The [Response] section tells Steel-Belted Radius/SPE what to do with the information that it has retrieved from the incoming access request and from the LDAP database. It completes the authentication and issues an access response to the RADIUS client.

```
[Response]
%Password = userpassword
Acct-Interim-Interval = radiusAcctInterimInterval
Address-Pool-Name = localAddressPool
Alt-CLI-Auth-Level = alternateCliAuthLevel
Alt-CLI-Virtual-Router = alternateCliVrouterName
Atm-MBS = atmMBS
Atm-PCR = atmPCR
Atm-SCR = atmSCR
Atm-Service-Category = atmServiceCategory
Class = radiusClass
CLI-Allow-All-VR-Access = cliAllowAllVRAccess
CLI-Initial-Auth-Level = cliInitialAccessLevel
Egress-Policy-Name = egressPolicyName
Egress-Statistics = egressStatistics
Filter-Id = radiusFilterId
```

Framed-IP-Address = radiusFramedIPAddress
Framed-IP-Netmask = radiusFramedIPNetMask
Framed-Ip-Route-Tag = framedIpRouteTag
Framed-Pool = radiusFramedPool
Framed-Route = radiusFramedRoute
Idle-Timeout = radiusIdleTimeOut
Igmp-Enable = igmpEnable
Ingress-Policy-Name = ingressPolicyName
Ingress-Statistics = ingressStatistics
Ipv6-Virtual-Router = ipv6VirtualRouter
Ipv6-Local-Interface = ipv6LocalInterface
Ipv6-Primary-DNS = ipv6PrimaryDNS
Ipv6-Secondary-DNS = ipv6SecondaryDNS
Local-Loopback = localInterface
Ppp-Authenticate-Protocol = pppAuthenticateProtocol
Ppp-Password = pppPassword
Ppp-Username = pppUsername
Pppoe-Max-Sessions = pppoeMaxSessions
Pppoe-Url = pppoeUrl
Primary-DNS = primaryDNS
Primary-WINS = primaryWINS
Qos-Profile-Interface-Type = qosProfileInterfaceType
Qos-Profile-Name = qosProfileName
Redirect-VR-Name = redirectVRName
Sa-Validate = saValidate
Sdx-Service-Name = sdxServiceName
Sdx-Session-Volume-Quota = sessionVolumeQuota
Secondary-DNS = secondaryDNS
Secondary-WINS = secondaryWINS
Service-Type = radiusServiceType
Service-Bundle = serviceBundle
Session-Timeout = radiusSessionTimeOut
Tunnel-Bearer-Type = tunnelBearerType
Tunnel-Dialout-Number = tunnelDialoutNumber
Tunnel-Interface-Id = tunnelInterfaceId
Tunnel-Maximum-Bps = tunnelMaximumBps
Tunnel-Minimum-Bps = tunnelMinimumBps
Tunnel-Assignment-ID = tunnelAssignmentID
Tunnel-Type = tunnelType
Tunnel-Maximum-Sessions = tunnelMaximumSessions
Tunnel-Medium-Type = tunnelMediumType
Tunnel-Nas-Port-Method = tunnelNasPortMethod
Tunnel-Server-Endpoint = tunnelServerEndPoint
Tunnel-Password = tunnelPassword
Tunnel-Preference = tunnelPreference
Tunnel-Tos = tunnelTOS
Tunnel-Virtual-Router = tunnelVirtualRouter
Virtual-Router-Name = virtualRouterName

Configuring Directed Authentication

Directed authentication is used when the service provider manages retailer ISPs. This means that the service provider holds the ISP's end-customer information in its LDAP server, but is not responsible for the data. This data is stored in a separate subtree within the LDAP server.

It is possible that unique identifiers exist in the retailer ISP realm, which might already exist in the service provider realm, or in some other retailer ISP realm. This authentication method allows you to set a different search base, based on the realm name, which is submitted at login time.

Consider an example where the ISP "Virneo" is handled within the service provider's LDAP directory. The service provider and the ISP agreed to use the realm name *virneo.com*.

To configure directed authentication for this example:

1. Enable the realm feature on the RADIUS server (setting parameter in *radius.ini*):

   [Configuration]
   ExtendedProxy = 1

2. Register the realm name with Steel-Belted Radius/SPE (setting parameter in *proxy.ini*):

   [Directed]
   virneo.com

3. Create a realm configuration file called *virneo.com.dir*

NOTE: The filename must be identical to the realm name specified in the previous step.

4. Register the authentication method (LDAP) with the realm (setting parameter in *isp1.com.dir*):

   [AuthMethods]
   VIRNEO.COM

NOTE: The string specified in the [AuthMethods] section must be identical to the LDAP initialization string from the to-be-created authentication file (virneo.com.aut).

5. Enable directed authentication (setting parameter in *virneo.com.dir*), and strip the realm name:

   [Auth]
   Enable = 1
   StripRealm = 1

6. Enable directed accounting (setting parameter in *isp1.net.dir*):

   ```
   [Acct]
   Enable = 1
   ```

7. Define the LDAP configuration interface for directed authentication (creating authentication file *virneo.com.aut*):

   This step is identical to a step mentioned in the *Configuring LDAP Authentication* section. The initialization string in the bootstrap section must be identical to the authentication method, which is specified in *virneo.com.dir*. For example:

   ```
   [Bootstrap]
   LibraryName=ldapauth.so
   Enable=1
   InitializationString=VIRNEO.COM
   ```

Further details about the proxy configuration and directed realm configurations can be found in the Steel-Belted Radius/SPE manuals.

Customizing the Authentication Log File

The SRC software requires that the RADIUS attribute Class be captured in the accounting files. By default, Steel-Belted Radius/SPE does not include the Class attribute in the accounting files. To accomplish the logging of Class, you must modify the file *account.ini* within the server directory *(/opt/UMC/SPE)* by adding "Class = " to the [Attributes] section:

```
[Attributes]
User-Name=
NAS-Port=
Framed-IP-Address=
Class=
```

Configuring the Steel-Belted Radius/SPE Server and RADIUS Clients

You must configure both the client and server to allow communication between the RADIUS server (SPE 4.0) and the RADIUS clients (the JUNOSe router and the SAE).

Configuring the Steel-Belted Radius Server

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

- IP address of the RADIUS client
- RADIUS shared secret to be exchanged between the Steel-Belted Radius/SPE server and the client
- Model (vendor) of the RADIUS client

You perform these configurations by using SDX Admin.

Configuring RADIUS Clients

Each RADIUS client must be able to contact its RADIUS server. The RADIUS client must have the following information to allow client/server communication:

- IP address of the RADIUS server
- RADIUS shared secret to be exchanged between the Steel-Belted Radius/SPE server and the client
- UDP ports on which the client sends and receives RADIUS authentication and accounting packets. They must match with the server configuration.

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

Using the Radius Administrator to Configure RADIUS Clients

This administration user interface is a Web-based GUI. You use this GUI to configure the JUNOSe router and the SAE as RADIUS clients. Each JUNOSe router and each SAE connected to a Steel-Belted Radius/SPE server must be configured as a RADIUS client.

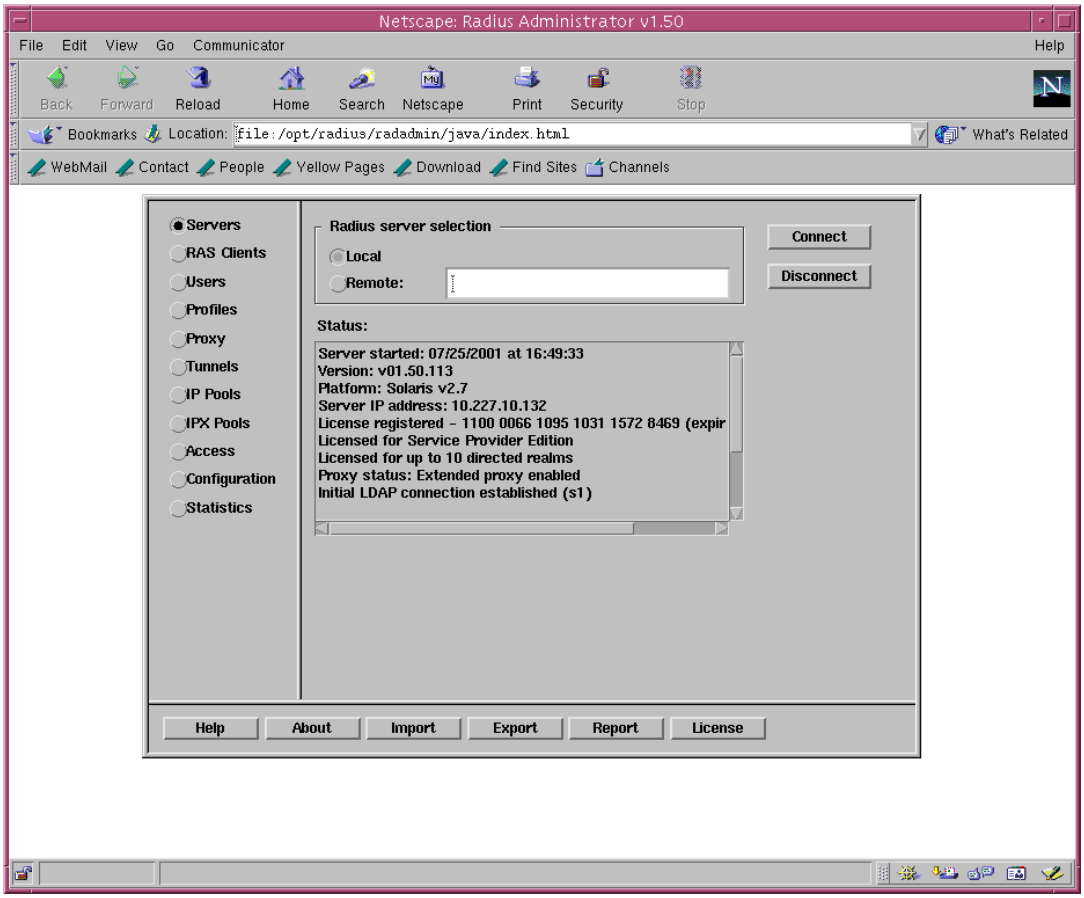
If you have a Netscape browser installed in */opt/netscape*, you must set the Netscape environment variable *MOZILLA_HOME = /opt/netscape* to run Java applets.

After you launch the Netscape browser, choose the URL

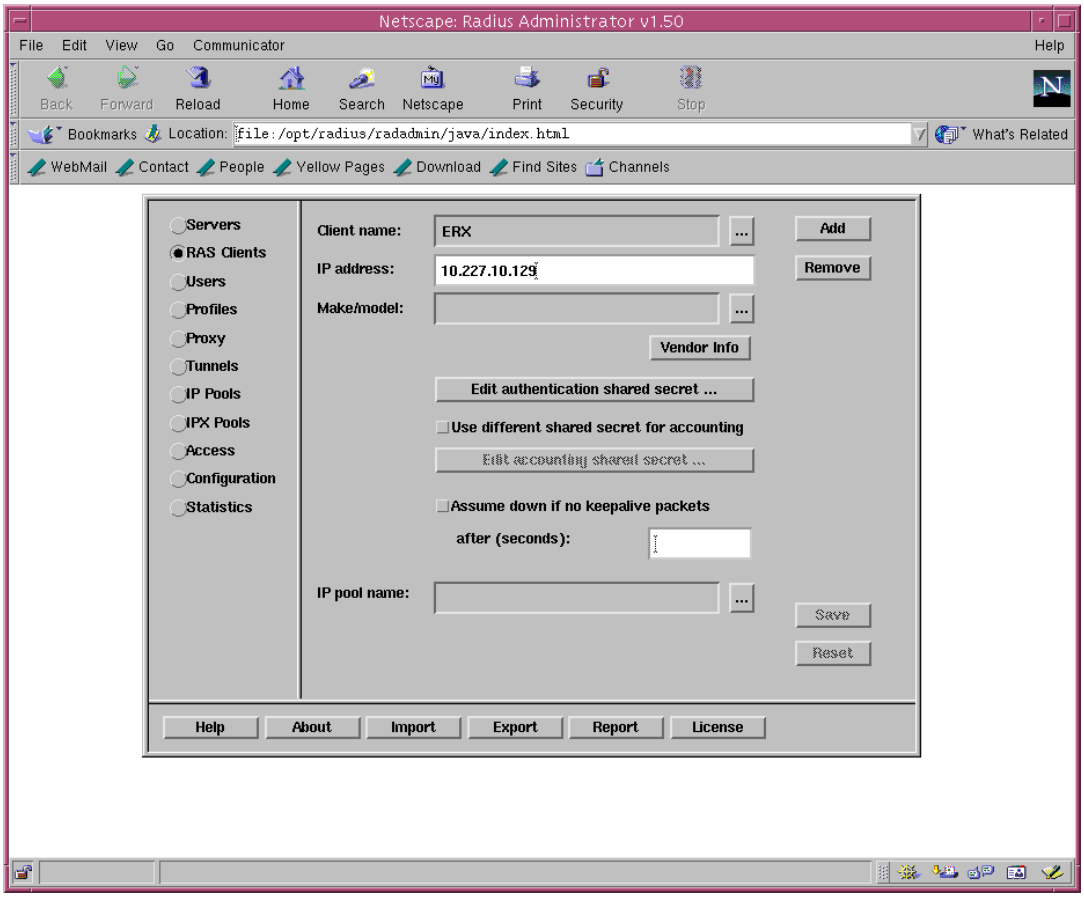
file:///opt/UMC/SPE/radadmin/java/index.html

This file prompts you for authentication credentials when you try to connect to the local server. By default, the username is *admin* with the password *radius*.

After successful authentication, the Web-based GUI is displayed.



To configure a JUNOSe router as a Remote Access Server (RAS) client, select **RAS Clients** on the left-hand side of the window, and click **Add**; then enter the necessary information.



When the Steel-Belted Radius/SPE server is integrated with the SAE, the Steel-Belted Radius/SPE server must know that the SAE server is a RAS client. The SAE server requires some JUNOSe specific attributes; therefore, it must be configured as a JUNOSe RADIUS client.

To specify the authentication method in the Radius Administration window, select **Configuration** on the left-hand side of the screen. The methods Native User, Unix User, and Unix Group must be deactivated. LDAP will be the only activated method.