Configuring RADIUS with Livingston Server

This document is intended to assist the first-time RADIUS user in setting up and debugging a RADIUS configuration to a Livingston RADIUS server. It is not an exhaustive description of IOS RADIUS capabilities. Livingston documentation is now on the Lucent Technologies website.

The router configuration would be the same no matter what server is used. Cisco offers commercially available RADIUS code in CiscoSecure NT, CiscoSecure UNIX, or Cisco Access Registrar.

The router configuration below was developed on a router running Cisco IOS Software Release 11.3.3; Release 12.0.5.T and later uses **group radius** instead of **radius**, so statements such as **aaa authentication login default radius enable** would appear as **aaa authentication login default group radius enable**.

For complete information on RADIUS router commands, see Cisco IOS software documentation for your Cisco IOS software release.

Help us help you.

Please rate this et:

○ Excellent
○ Good
○ Average
○ Fair
○ Poor

his et sle::rle:

○ Yes
○ No
○ Just browsing

estis r ireet:

(256 character limit)

□

Send

Authentication

1. Make sure you have compiled RADIUS code on the UNIX server. The server configurations here assume you are using the Livingston RADIUS server code; the router configurations should work with other server code but the server configurations will differ. The code, "radiusd", must be run as root.

2. The Livingston RADIUS code comes with three sample files that a re to be customized for your system: "clients.example", "users.example", and "dictionary". These are all usually found in the "raddb" directory. You can either modify these files or the "users" and "clients" files at the end of this document. All three files will need to be placed in a working directory. Test to be sure the RADIUS server will start with the three files:

   ```
   radiusd -x -d (directory_containing_3_files)
   ```

   Errors in startup should be printed to the screen or the (directory_containing_3_files_logfile). From another server window, check to be sure RADIUS has started:

   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```

   (You should see two "radiusd" processes.)

3. Kill the radius process:

   ```
   kill -9 highest_radiusd_pid
   ```

4. On the router console port, start configuring RADIUS (enter enable mode and type **conf t** before the command set). The following syntax will ensure that you will not be "locked out" of the router *initially*, providing that RADIUS is *not* running on the server:

   ```
   !--- Turn on RADIUS
   aaa new-model
   enable password whatever
   !--- These are lists of authentication methods,
   !--- that is, "linmethod", "vtymethod", "conmethod" are
   !--- names of lists, and the methods listed on the same
   !--- lines are the methods in the order to be tried.  As
   !--- used here, if authentication fails due to the radiusd
   !--- not being started, the enable password will be
   !--- accepted because it is in each list.
   aaa authentication login default radius enable
   aaa authentication login linmethod radius enable
   aaa authentication login vtymethod radius enable
   aaa authentication login conmethod radius enable
   !--- Point the router to the server, that is,
   !--- #.#.#.# is the server IP address.
   radius-server host #.#.#.#
   !--- Enter a key for handshaking
   !--- with the RADIUS server:
   radius-server key cisco
   line con 0
           password whatever
           !--- No time-out to prevent being
           !--- locked out during debugging.
           exec-timeout 0 0
           login authentication conmethod
   line 1 8
           login authentication linmethod
           modem InOut
           transport input all
           rxspeed 38400
           txspeed 38400
           password whatever
           flowcontrol hardware
   line vty 0 4
           password whatever
           !--- No time-out to prevent being
           !--- locked out during debugging.
           exec-timeout 0 0
           login authentication vtymethod
   ```

5. Remain logged in to the router through the console port while checking to be sure you can still access the router through Telnet before continuing. Because radiusd is not running, the enable password should be accepted with any userid.

   Caution: Keep the console port session active and remain in enable mode; this session should not time out. You need to be able to make configuration changes without locking yourself out!

   To see server to router interaction at the router, issue the following commands:

   ```
   terminal monitor
   debug aaa authentication
   ```

6. As root, start RADIUS on the server:

   ```
   radiusd -x -d (directory_containing_3_files)
   ```

   Errors in startup should be printed to the screen or the (directory_containing_3_files_logfile). From another server window, check to be sure RADIUS has started:

   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```

   (You should see two "radiusd" processes.)

7. Telnet (vty) users should now have to authenticate through RADIUS. With debug going on the router and the server (steps 5 and 6), Telnet into the router from another part of the network. The router should produce a "username" and "password" prompt to which you reply:

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Watch the server and the router where you should see the RADIUS interaction, for instance, what is being sent where, responses, and requests, and so on. Correct any problems before continuing.

8. If you also want your users to authenticate through RADIUS to get into enable mode, make sure your console port session is still active and add the following command to the router.

   ```
   !--- For enable mode, list "default" looks to RADIUS
   !--- then enable password if RADIUS not running.
   aaa authentication enable default radius enable
   ```

9. Users should now have to **enable** through RADIUS. With debug going on the router and the server (steps 5 and 6), Telnet into the router from another part of the network. The router should produce a "username" and "password" prompt to which you reply:

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   When entering enable mode, the router sends username "$enable15$" and requests a password, to which you reply:

   ```
   shared
   ```

   Watch the server and the router where you should see the RADIUS interaction, for instance, what is being sent where, responses, and requests, and so on. Correct any problems before continuing.

10. Check for authentication of your console port users through RADIUS by establishing a Telnet session to the router (which should authenticate through RADIUS). Remain Telnetted into the router and in enable mode until you are sure you can login to the router through the console port; log out of your original connection to the router through the console port, and then reconnect to the console port. Console port authentication to login and enable using userids and passwords in step 9 should now be through RADIUS.

11. While remaining connected through either a Telnet session or the console port and with debug going on the router and the server (steps 5 and 6), establish a modem connection to line 1. Line users should now have to login and enable through RADIUS. The router should produce a "username" and

"password" prompt to which you reply:

```
ciscousr (username from users file)
ciscopas (password from users file)
```

When entering enable mode, the router sends username "$enable15$" and requests a password, to which you reply:

```
shared
```

Watch the server and the router where you should see the RADIUS interaction, for instance, what is being sent where, responses, and requests, and so on. Correct any problems before continuing.

Adding Accounting (optional)

1. Accounting does not take place unless configured in the router. In this example, we enable accounting in the router:

   ```
   aaa accounting exec default start-stop radius
   aaa accounting connection default start-stop radius
   aaa accounting network default start-stop radius
   aaa accounting system default start-stop radius
   ```

2. Start RADIUS on the server with the accounting option:

   ```
   radiusd -a (directory_for_accounting) -x -d (directory_containing_3_files)
   ```

3. To see server to router interaction at the router:

   ```
   terminal monitor
   debug aaa accounting
   ```

4. Access the router while observing the server and the router interaction through the debug, and then check the accounting directory for log files.

Test Files

This is the users test file:

```
ciscousr        Password = "ciscopas"
                User-Service-Type = Login-User,
                Login-Host = 1.2.3.4,
                Login-Service = Telnet

$enable15$      Password = "shared"
                User-Service-Type = Shell-User
```

This is the clients test file:

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4         cisco
```

Related Information

- **Cisco IOS Software Configuration**
- **More RADIUS Technical Tips**

Home | What's New | How to Buy | Login | Profile | Feedback | Search | Map/Help