Configuring RADIUS with Livingston Server

Document ID: 8524

Contents

Introduction

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 Cisco IOS® RADIUS capabilities. Livingston documentation is available from the Lucent Technologies web site.

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

This router configuration was developed on a router that runs 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** appear as **aaa authentication login default group radius enable**.

Refer to the RADIUS information in Cisco IOS documentation for details on RADIUS router commands.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Authentication

Complete these steps:

1. Make sure you compiled RADIUS code on the UNIX server. The server configurations assume you use the Livingston RADIUS server code. The router configurations need to work with other server

code but the server configurations differ. The code, radiusd, must be run as root.

2. The Livingston RADIUS code comes with three sample files that are 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 need to be placed in a working directory. Test to be sure the RADIUS server starts with the three files:

```
radiusd –x –d (directory_containing_3_files)
```

Errors in startup need to be printed to the screen or the directory_containing_3_files_logfile. Check in order to be sure RADIUS started, from another server window:

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

You see two radiusd processes.

3. Kill the radius process:

```
kill –9 highest_radiusd_pid
```

4. On the router console port, start to configure RADIUS. Enter enable mode and type **configure terminal** before the command set. This syntax ensures that you are not locked out of the router initially, given that RADIUS does not run 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 you check in order to be sure you can still access the router through Telnet before you continue. Because radiusd is not running, the enable password needs to be accepted with any userid.

⚠️ **Caution:** Keep the console port session active and remain in enable mode. Ensure that this session does not time out. Do not lock yourself out while you make configuration changes.

Issue these commands in order to see server to router interaction at the router:

```
terminal monitor
debug aaa authentication
```

6. As root, start RADIUS on the server:

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

Errors in startup are printed to the screen or the directory_containing_3_files_logfile. Check to be sure RADIUS started from another server window:

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

You need to see two radiusd processes.

7. Telnet (vty) users now have to authenticate through RADIUS. With debug on the router and the server, steps 5 and 6, Telnet into the router from another part of the network. The router produces 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 need to see the RADIUS interaction, for instance, what is being sent where, responses, and requests, and so forth. Correct any problems before you continue.

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 this 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 need to 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 needs to produce a username and password prompt to which you reply:

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

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

```
shared
```

Watch the server and the router where you need to see the RADIUS interaction, for instance, what is being sent where, responses, and requests, and so forth. Correct any problems before you continue.

10. Check for authentication of your console port users through RADIUS by the establishment of a Telnet session to the router, which needs to 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 through the use of userids and passwords in step 9 need to now be through RADIUS.

11. While you remain 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 need to now have to login and enable through RADIUS. The router needs to produce a username and password prompt to which you reply:

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

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

```
shared
```

Watch the server and the router where you need to see the RADIUS interaction, for instance, what is being sent where, responses, and requests, and so forth. Correct any problems before you continue.

Adding Accounting

Adding accounting is optional.

1. Accounting does not take place unless configured in the router. Enable accounting in the router like in this example:

```
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:

```
Start RADIUS on the server with the accounting option:
```

3. In order to see server to router interaction at the router:

```
terminal monitor
debug aaa accounting
```

4. Access the router while you observe 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

- **Remote Authentication Dial–In User Service (RADIUS)**
- **Requests for Comments (RFCs)** ↗
- **Technical Support & Documentation – Cisco Systems**

Updated: Aug 25, 2006   Document ID: 8524