

# **RADIUS - Server**

## **Contents:**

1. Task
2. Introduction to RADIUS
3. How RADIUS Work
  - 3.1. Authentication
  - 3.2. Authorization
  - 3.3. Accounting
4. Installation and Configuration
  - 4.1. Installation
  - 4.2. Configuring ports
  - 4.3. Starting RADIUS
5. RADIUS Directory Structure
6. Adding a RADIUS Client
  - 6.1. Modifying Cliets file
  - 6.2. Configuring the Access Point with RoamAbout
7. Configuring User Profiles

# 1. Task

The task is to increase security in the wireless network at the John – Moores – University. The main aspect is to confine the users working with the WLAN. One possibility to realize this is to setup a radius server for MAC – Address – Filtering (WLAN)

## 2. Introduction to RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol created by Lucent Remote Access. RADIUS is an Internet draft standard protocol. See RFCs 2138 and 2139 for more information on RADIUS.

User profiles are stored in a central location, known as the RADIUS server. RADIUS clients (such as an Access Point) communicate with the RADIUS server to authenticate users. The server specifies back to the client what the authenticated user is authorized to do. Although the term **RADIUS** refers to the network protocol that the client and server use to communicate, it is often used to refer to the entire client/server system.

### Security:

In large networks, security information can be scattered throughout the network on different devices. RADIUS allows user information to be stored on one host, minimizing the risk of security loopholes. All authentication and access to network services is managed by the host functioning as the RADIUS server.

## 3. How RADIUS Works

The primary functions of RADIUS are authentication, authorization, and accounting.

### - Authentication

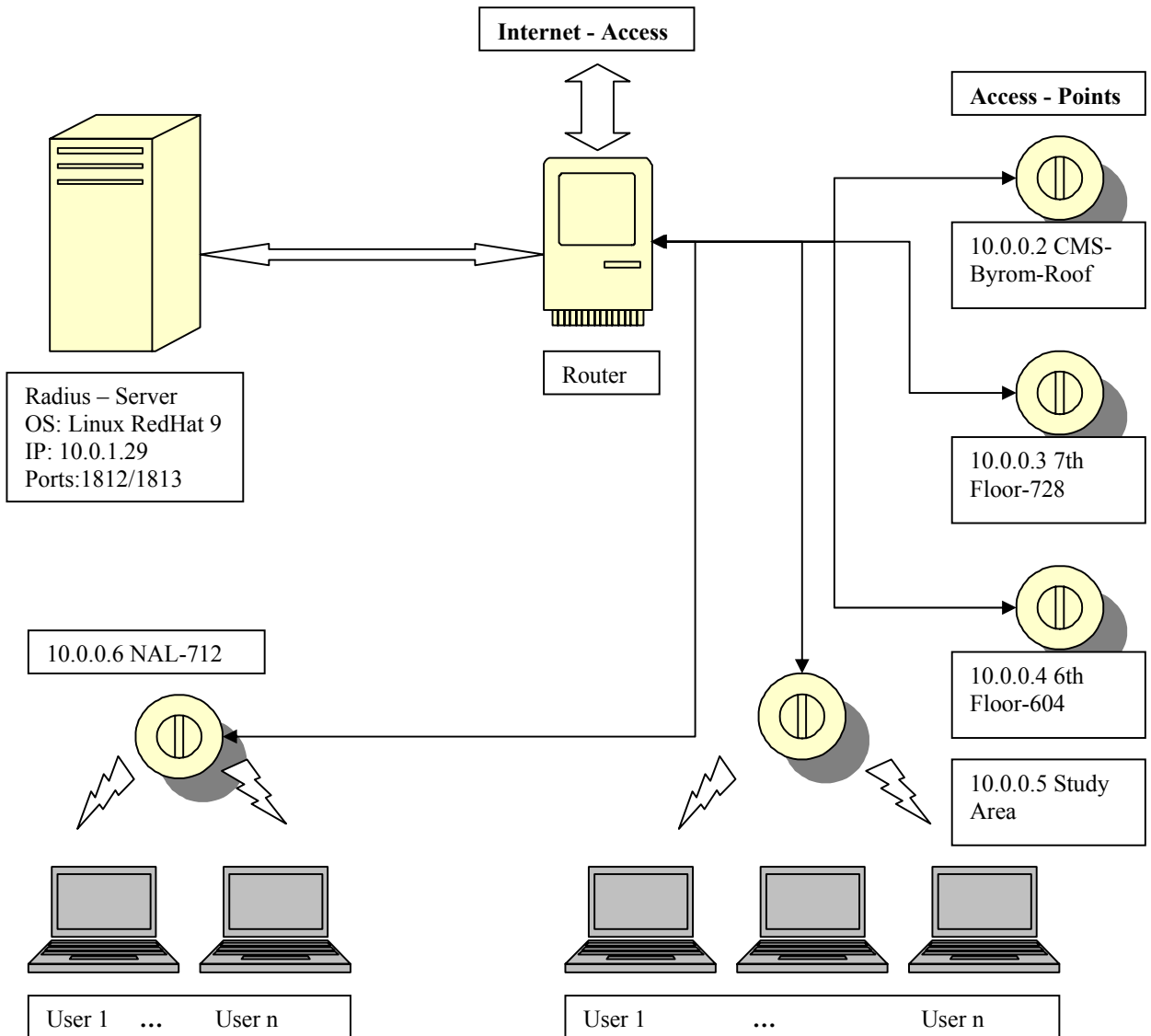
RADIUS determines whether users are eligible to receive requested services. Authentication information is stored in either a local **users** file or database cache, or accessed from external authentication mechanisms such as a UNIX password file.

### - Authorization

Authorization controls access to specific services on the network by configuring the user's session. Once a user is authenticated, RADIUS reports to the Access Point what a user is authorized to access.

- **Accounting**

RADIUS accounting stores usage information for dial-in users. This information is often used for billing purposes. When the user is authenticated and the session has been configured according to the authorization information, an accounting start record is created. When the user's session is terminated, an accounting stop record is created.



Scheme of the wireless network architecture at the NAL - JMU

## 4. Installation and Configuration

Before installing and configuring RADIUS software, select a host with following characteristics:

- Secure physical location
- Root access limited to the system administrator
- Limited number of user accounts, preferably none
- Basic memory and disk space
- Inaccessibility from outside your local network

### Installation RADIUS

To implement a RADIUS server we chose the [FreeRADIUS 0.8.1](http://www.freeradius.org) software which you can download from <http://www.freeradius.org> for free.

Besides to install RADIUS software we used a UNIX server with Redhat Linux 9.0 Shrike as operating system.

### Getting started

- download [FreeRADIUS](http://www.freeradius.org) from <http://www.freeradius.org>
- extract the file → 'freeradius-0.8.1' directory is created
- open a shell and move to this directory
- type the following commands:

```
$ ./configure
$ make
$ su ... //login as root
$ make install
```
- Installation is complete

### Configuring ports

Ports are defined in the `/usr/local/etc/raddb/radiusd.conf`, by default with a 0 (zero)  
→ the radiusd uses the defined ports at the file `/etc/services`

**RedHat 9 Shrike** by default

- authorization port 1812
- authentication port 1813

## Start RADIUS Server

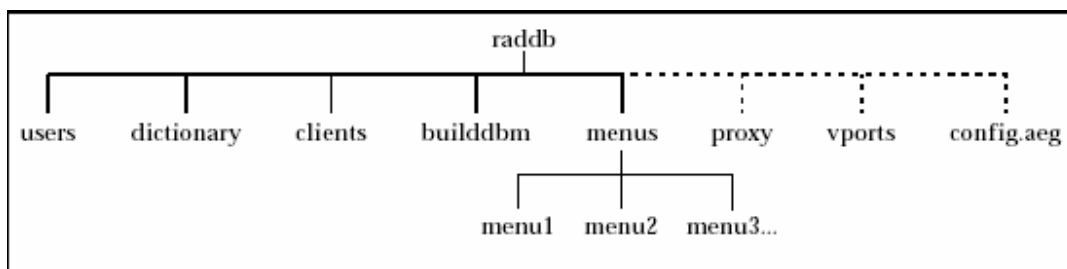
- To start the RADIUS Server manually
  - open a shell like bash\$
  - change into directory **/usr/local/sbin**
  - login as root and type **./radiusd** /\* -x for debugging mode\*/
- To start the RADIUS Server each time the operating system is booted, you have to place the following script in your system start-up script

```
# Start RADIUS
#
if [ -x /usr/local/sbin/radiusd ]; then
    echo "Starting RADIUS – Server for CMS WLAN"
    /usr/local/sbin/radiusd                #add flags here
fi
```

Start-up script for Linux RedHat 9 Shrike is **/etc/rc.d/rc.local**

## 5. RADIUS Directory Structure

RADIUS server files are stored in the **raddb** (RADIUS database) directory. The **raddb** directory is typically placed within the **/usr/local/etc** directory. The **raddb** directory contains files and subdirectories organized as shown in Figure A dotted line indicates an optional file.



Explanation of the most important directories:

- The **users** file stores user profiles, which consist of authentication and authorisation information for all users authenticated with RADIUS
- The **dictionary** file contains information used to pass user access requests and generate responses. It lists attribute numbers, names, and data type expected for attribute values. Attributes appear in client-server communications and accounting records are used to create user profiles. After you modify this file, you must restart RADIUS to apply your changes
- The **clients** file contains the IP addresses of all RADIUS clients and the secrets shared between the clients and the RADIUS server

## 6. Adding a RADIUS Client

To add a RADIUS Client you have to do the following two steps:

1. Modify the clients file to add the Access Point and shared secret.
2. Configure the Access Point with the RoamAbout software and save your changes

### 1. Modifying the clients file

The **clients** file stores information about RADIUS clients, including each client's name or IP address and its shared secret. Use any text editor to edit the **usr/local/etc/raddb/clients** file.

Verify that only root users have read and write access to the clients file.

To add a client, enter the client's name or IP address and the shared secret.

To add a comment line, start the line with the number sign (#).

Shared secrets must consist of 15 or fewer printable, nonspace, ASCII characters.

There is no limit to the number of clients that you can add to this file.

```
#Client Name      Shared Secret
#-----
portmaster1      wP40cQ0
portmaster2      A3X445A
192.168.1.2      wer369st
```

Save your changes!

### 2. Configure the Access Point with RoamAbout

Configure the following in RoamAbout

- Security enabled on all ports
- IP addresses of the primary RADIUS authentication servers; optionally configure an authentication port number different from the default
- IP addresses of the primary RADIUS accounting servers, if accounting is to be performed; optionally configure an accounting port number different from the default
- RADIUS shared secret
- Save your changes
- Reset the Access Point

## Configuration of the Study Area AP with RoomAbout

Authentication

Selected AP:  
10.0.0.5 CMS\_Wireless CMS - Study Area cmsaming@livjm.ac.uk:cmsobue@liv

Authentication Options

Slot 1:  MAC  802.1X  Rapid Rekeying  Deny Non-encrypted Data

Slot 2:  MAC  802.1X  Rapid Rekeying  Deny Non-encrypted Data

RADIUS Settings

Primary Server IP Address: 10.0.1.29

Secondary Server IP Address: 0.0.0.0

Primary Authentication Port: 1812 (1-65535)

Secondary Authentication Port: 1812 (1-65535)

Shared Secret: \*\*\*\*\*

Retry Limit: 5 (0-20 times)

Retry Timer: 5 (2-10 seconds)

RADIUS Accounting

Change Authenticator Change Password

OK Cancel Help

Configuring for Authentication

RADIUS Accounting

Selected AP:  
10.0.0.5 CMS\_Wireless CMS - Study Area cmsaming@livjm.ac.uk:cmsobue

RADIUS Accounting State: Enabled

RADIUS Accounting Settings

Primary Accounting Server

IP Address: 10.0.1.29

UDP Port: 1813 (1-65535)

Retry Limit: 5 (0-20 times)

Retry Timer: 5 (2-10 seconds)

Secondary Accounting Server

IP Address: 0.0.0.0

UDP Port: 1813 (1-65535)

Retry Limit: 5 (0-20 times)

Retry Timer: 5 (2-10 seconds)

Shared Secret: \*\*\*\*\*

Interim Interval: 10 (minutes)

Interim Interval Minimum: 1 (minutes)

OK Cancel Help

Configuring for Accounting

## 7. Configuring User Profiles

The RADIUS **users** file is a flat text file on the RADIUS server. The **users** file stores authentication and authorization information for all users authenticated with RADIUS. Use any text editor to edit the **usr/local/etc/raddb/users** file.

Now the MAC addresses can be entered by the Network Administrator.

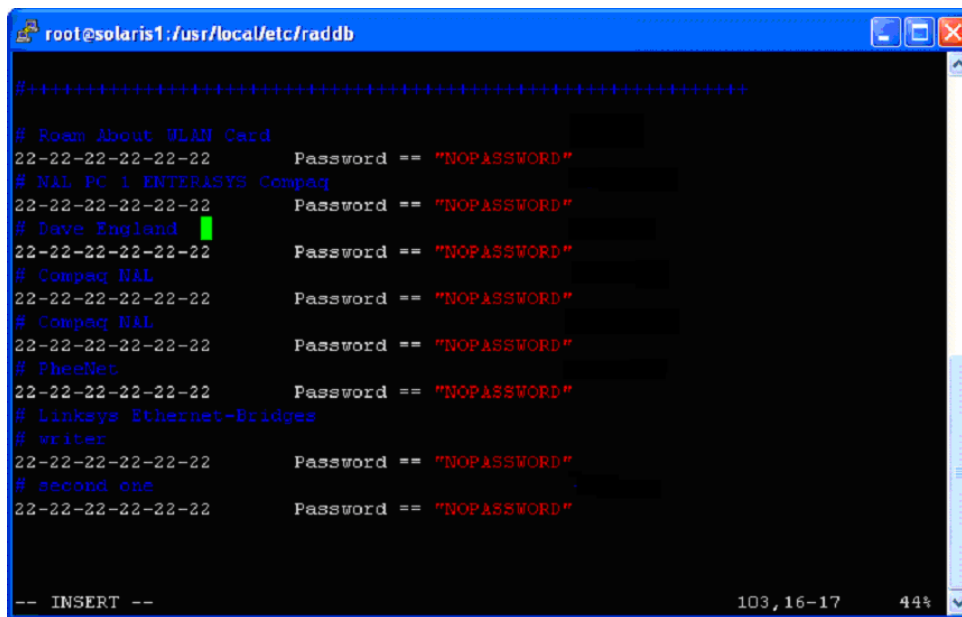
If students want to get network access they have to leave the MAC address of their wireless client (PC-Card/PAM).

### Username:

The Username is the MAC address of the wireless LAN Card.

### Password

For address – filtering you need no passwords, but the RADIUS Server expects one. You can use the Flag “**NOPASSWORD**” in the users file.



```
root@solaris1: /usr/local/etc/raddb
#+++++
# Room About WLAN Card
22-22-22-22-22-22 Password == "NOPASSWORD"
# NAL PC 1 ENTERASYS Compaq
22-22-22-22-22-22 Password == "NOPASSWORD"
# Dave England
22-22-22-22-22-22 Password == "NOPASSWORD"
# Compaq NAL
22-22-22-22-22-22 Password == "NOPASSWORD"
# Compaq NAL
22-22-22-22-22-22 Password == "NOPASSWORD"
# PheeNet
22-22-22-22-22-22 Password == "NOPASSWORD"
# Linksys Ethernet-Bridges
# writer
22-22-22-22-22-22 Password == "NOPASSWORD"
# second one
22-22-22-22-22-22 Password == "NOPASSWORD"
-- INSERT -- 103, 16-17 44%
```

The RADIUS users file, setup for MAC Address Filtering

There is an optimal performance with a number of up to 500 users. If there are more users Database should be createt.

## Configuring the Access Points for WEP (wired equivalent privacy)

The WEP feature encrypts all data transmitted within the wireless network. The encryption uses the RC4 algorithm as defined in the IEEE 802.11 Wired Equivalent Privacy standard.

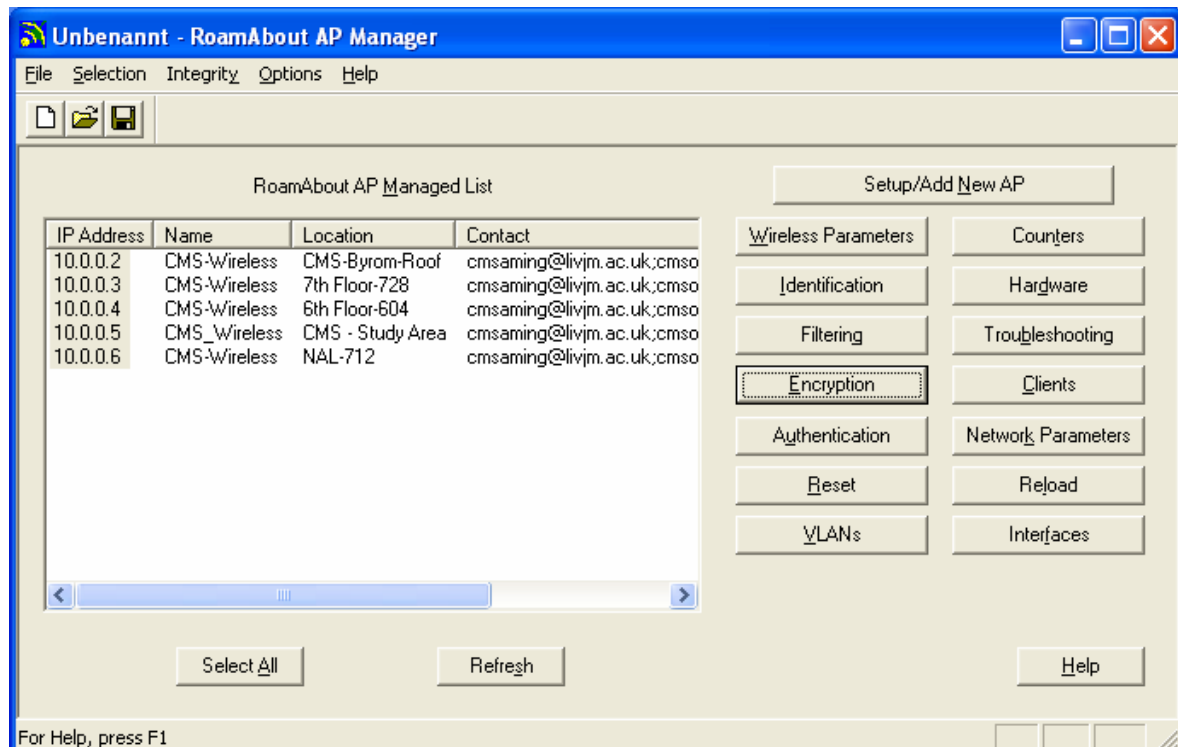
The RoamAbout devices can be configured with four encryption keys. Each key is placed in a specific position (Key 1, Key 2, Key 3, or Key 4). You select one key to encrypt transmitted data. To decipher the data, the receiving wireless device must have the key used to encrypt the data in the same position as the sending device.

The receiving device can transmit data back to the sending device using a different key for transmission, as long as the other device has the transmitting key in the same position.

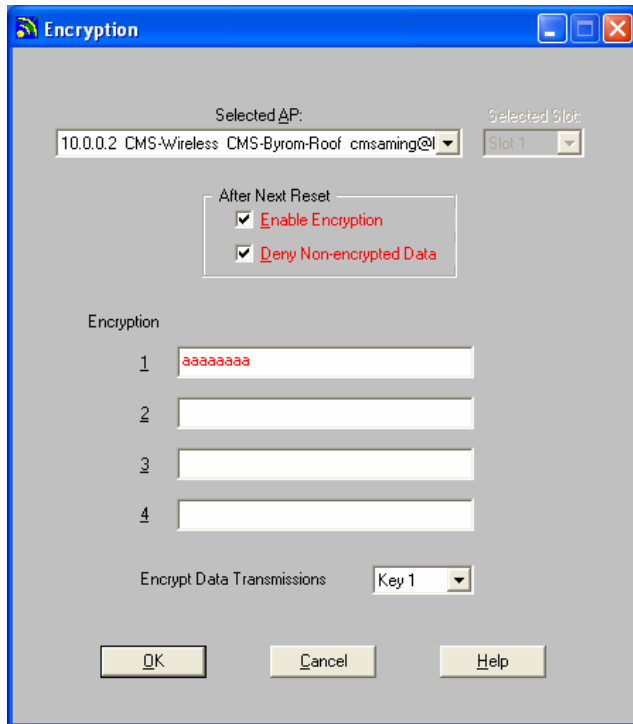
In a wireless infrastructure network, you can configure the APs to:

- Only accept encrypted data from clients. Only clients that have the correct encryption keys can participate in this network.
- Accept encrypted data from clients with encryption enabled, and unencrypted data from clients without encryption enabled. This allows clients who require security to use encryption without preventing other clients from using the network.

To configure the Access – Points for WEP



Selection of all Access Points at the JMU



Entering a shared secret

The disadvantage of WEP is that potential 15.000 users have to share one secret key. So there is probably no secret about it and security doesn't really exist.