# Пример настройки AAA с использованием RADIUS-сервера

**AAA** (Authentication, Authorization, Accounting) — это основанная на стандартах структура для контроля того, кому разрешено использовать сетевые ресурсы (через аутентификацию), что им разрешено делать (через авторизацию) и регистрации действий, выполняемых при доступе к сети (посредством учета). В сети используется сервер AAA (TACACS+ или RADIUS), способный аутентифицировать пользователей, обрабатывать запросы на авторизацию и собирать учетные данные.

## Примечание к настройке

Рассматриваемый пример настройки подходит для коммутаторов с D-Link-like CLI.

## Задача

Настроить аутентификацию при доступе к коммутатору по Telnet с использованием RADIUS-сервера.

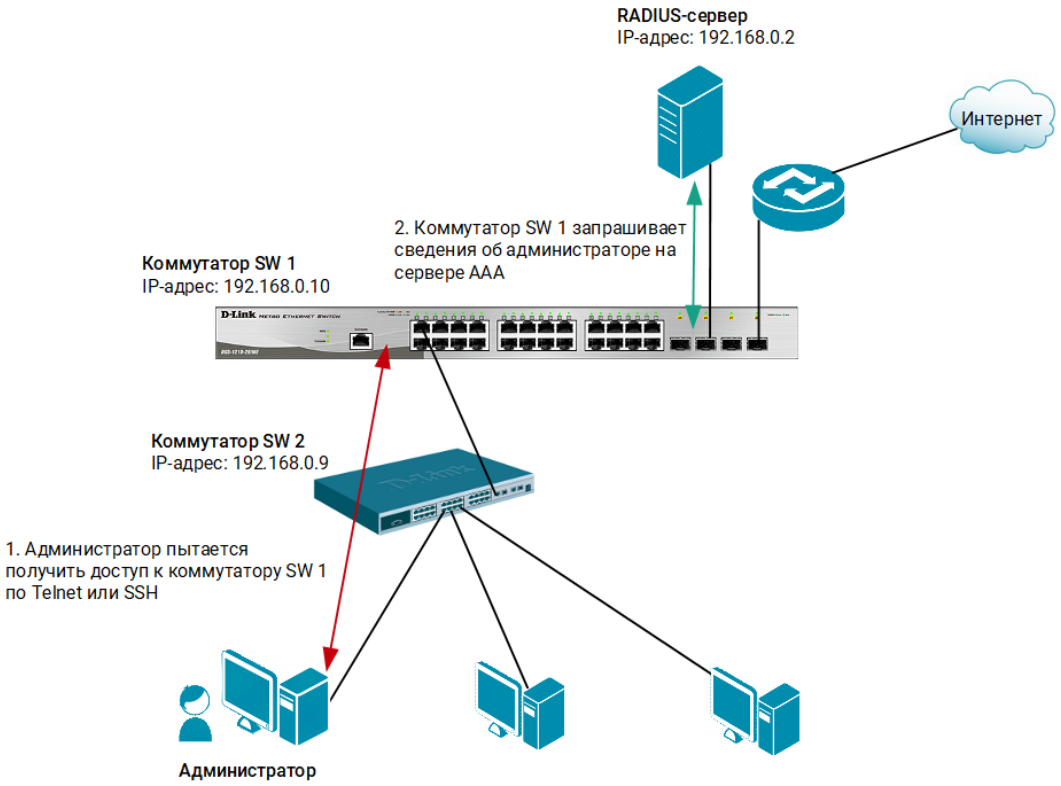


Рис. 1 Схема подключения

## Настройка RADIUS-сервера

В качестве RADIUS-сервера будем использовать пакет **freeradius** для ОС Linux. Команды приведены для дистрибутива **Linux Ubuntu 22.04**.

1. Установите пакет **freeradius**. В терминале введите команду:

```
$ sudo apt install freeradius
```

2. Добавьте информацию о коммутаторе, который будет использовать RADIUS-сервер для аутентификации клиентов. Откройте файл `/etc/freeradius/3.0/clients.conf`. В конце файла добавьте строки:

```
$ sudo gedit /etc/freeradius/3.0/clients.conf

 client 192.168.0.10 {
    secret = dlinkpassword
    shortname = switch
}
```

> **Примечание**
>
> 1. Если при попытке доступа к папке `/etc/freeradius/3.0` появляется сообщение об отказе доступа, то введите команду:
>
> ```
> $ sudo chmod 755 /etc/freeradius/3.0
> ```
>
> 2. При написании текста, необходимо выровнять текст по образцу примера. Для этого, вместо пробела используйте нажатие клавиши **Tab**. Соблюдать форматирование необходимо **во всех** конфигурационных файлах при настройке RADIUS-сервера.

3. Создайте и заполните файл `/etc/freeradius/3.0/dictionary.dlink`:

```
$ sudo gedit /etc/freeradius/3.0/dictionary.dlink

VENDOR  dlink 171
BEGIN-VENDOR  dlink
ATTRIBUTE  dlink-privelege-level    1    integer
END-VENDOR  dlink
```

4. В конфигурационный файл `/etc/freeradius/3.0/dictionary` в конце файла добавьте строку:

```
$ sudo gedit /etc/freeradius/3.0/dictionary

$INCLUDE /etc/freeradius/3.0/dictionary.dlink
```

5. Настройте базу учётных записей пользователей. На коммутаторах с D-Link-like CLI существует четыре уровня прав доступа — **Admin**, **Operator**, **Power User** и **User**. Соответственно, в конфигурационном файле RADIUS-сервера необходимо создать пользователей для каждого уровня доступа — **admin**, **operator**, **power_user**, **user** и **enable**. Пользователь **enable** необходим для получения прав администратора при выполнении команды `enable admin`. Откройте файл `/etc/freeradius/3.0/users`. В начале файла добавьте:

```
$ sudo gedit /etc/freeradius/3.0/users

admin   Cleartext-Password := “admin_password”
        dlink-privelege-level = 5

enable  Cleartext-Password := “enable_password”
        dlink-privelege-level = 5

operator  Cleartext-Password := “operator_password”
        dlink-privelege-level = 4

power_user  Cleartext-Password := “power_user_password”
        dlink-privelege-level = 6

user  Cleartext-Password := “user_password”
        dlink-privelege-level = 3
```

6. Перезапустите RADIUS-сервер:

```
$ sudo systemctl restart freeradius.service
```

7. Чтобы протестировать аутентификацию пользователей локально на RADIUS-сервере, введите команду:

```
$ sudo radtest admin admin_password 127.0.0.1:18120 0 testing123
```

Пример успешной аутентификации пользователя:

```
Sent Access-Request Id 22 from 0.0.0.0:41305 to 127.0.0.1:18120
length 75
 User-Name = "admin"
 User-Password = "admin_password"
 NAS-IP-Address = 127.0.1.1
 NAS-Port = 0
 Message-Authenticator = 0x00
 Cleartext-Password = "admin_password"
Received Access-Accept Id 8 from 127.0.0.1:18120 to 127.0.0.1:41305
length 32
dlink-privelege-level = Admin
```

## Настройка коммутатора SW 1

1. IP-адрес управляющего интерфейса коммутатора должен соответствовать записи в конфигурационном файле /`etc/freeradius/3.0/clients.conf`. Измените IP-адрес интерфейса управления коммутатора:

```
config ipif System ipaddress 192.168.0.10/24
```

2. Активируйте глобально использование политик аутентификации:

```
enable authen_policy
```

3. Создайте запись о RADIUS-сервере, ключ должен совпадать с записью в конфигурационном файле /`etc/freeradius/3.0/clients.conf`:

```
create authen server_host 192.168.0.2 protocol radius port 1812 key
dlinkpassword timeout 5 retransmit 2
```

4. Создайте пользовательский список аутентификации **tel_ext**, в котором предпочитаемым будет RADIUS:

```
create authen_login method_list_name tel_ext
config authen_login method_list_name tel_ext method radius
```

5. Создайте список аутентификации **tel_ext_ena** для получения прав администратора:

```
create authen_enable method_list_name tel_ext_ena
config authen_enable method_list_name tel_ext_ena method radius
```

6. Примените созданные списки аутентификации для доступа к коммутатору по Telnet:

```
config authen application telnet login method_list_name tel_ext
config authen application telnet enable method_list_name tel_ext_ena
```

7. Укажите максимальное количество попыток аутентификации:

```
config authen parameter attempt 3
```