# Лабораторная работа Настройка локального механизма AAA

### Общая информация

#### О лабораторной работе

Аутентификация, авторизация и учет (AAA) — механизм управления сетевой безопасностью.

AAA предоставляет следующие функции:

* Аутентификация: проверка наличия у пользователей разрешения на доступ к сети.
* Авторизация: проверка полномочий пользователей на использование определенных услуг.
* Учет: регистрация сетевых ресурсов, используемых пользователями.

Пользователи могут использовать одну или несколько служб безопасности, предоставляемых AAA. Например, если компании требуется аутентификация сотрудников, которые обращаются к определенным сетевым ресурсам, то сетевому администратору необходимо только настроить сервер аутентификации. Если компания также хочет регистрировать операции, выполняемые сотрудниками в сети, необходимо настроить сервер учета.

Таким образом, механизм AAA будет разрешать сотрудникам использовать определенные ресурсы и записывать их операции. Механизм AAA получил широкое применение, поскольку отличается хорошей масштабируемостью и упрощает централизованное управление пользовательской информацией. Реализовать AAA можно с помощью нескольких протоколов. В реальных условиях чаще всего используется протокол RADIUS.

В этой лабораторной работе вам предлагается настроить локальный механизм AAA для управления и контроля ресурсов, используемых удаленными пользователями Telnet.

#### Цели

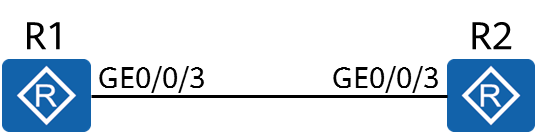
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

* Настройка локального механизма AAA
* Процедура создания домена
* Процедура создания локального пользователя
* Управление пользователями на основе домена

#### Топология сети

Маршрутизатор R1 выполняет функции клиента, а R2 — функции сетевого устройства. Необходим контроль доступа к ресурсам на R2. Следовательно, нужно настроить локальную аутентификацию AAA на маршрутизаторах R1 и R2 и управлять пользователями на основе доменов, а также настроить уровни полномочий для аутентифицированных пользователей.

Топология сети для конфигурирования локального механизма AAA, используемая в данной лабораторной работе



### Лабораторная работа

#### План работы

Настройка схемы AAA.

Создание домена и применение к нему схемы AAA.

Настройка локальных пользователей.

#### Процедура конфигурирования

Настройте основные параметры устройств.

# Присвойте имена маршрутизаторам R1 и R2.

Подробности данной операции здесь не приводятся.

# Настройте IP-адреса для маршрутизаторов R1 и R2.

[R1]interface GigabitEthernet 0/0/3

[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24

[R2]interface GigabitEthernet 0/0/3

[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24

Настройте схему AAA.

# Настройте схемы аутентификации и авторизации.

[R2-aaa]aaa

*Перейдите в режим AAA.*

[R2-aaa]authentication-scheme datacom

Info: Create a new authentication scheme.

*Создайте схему аутентификации с названием datacom.*

[R2-aaa-authen-datacom]authentication-mode local

*Задайте в качестве режима аутентификации локальную аутентификацию.*

[R2-aaa-authen-datacom]quit

[R2-aaa]authorization-scheme datacom

Info: Create a new authorization scheme.

*Создайте схему авторизации с названием datacom.*

[R2-aaa-author-datacom]authorization-mode local

*Задайте в качестве режима авторизации локальную авторизацию.*

[R2-aaa-author-datacom]quit

Устройство, выполняющее функции сервера AAA, называется локальным сервером AAA, который может выполнять аутентификацию и авторизацию, но не учет.

Локальному серверу AAA требуется база данных локальных пользователей, содержащая имя пользователя, пароль и информацию об авторизации локальных пользователей. Локальный сервер AAA быстрее и дешевле, чем удаленный сервер AAA, но имеет меньшую емкость хранилища.

Создайте домен и примените к нему схему AAA.

[R2]aaa

[R2-aaa]domain datacom

Устройства управляют пользователями на основе доменов. Домен — это группа пользователей. Каждый пользователь принадлежит к домену. Конфигурация AAA для домена применяется к пользователям в домене. Создайте домен с именем datacom.

[R2-aaa-domain-datacom]authentication-scheme datacom

*Схема аутентификации с названием datacom используется для пользователей в домене.*

[R2-aaa-domain-datacom]authorization-scheme datacom

*Схема авторизации с названием datacom используется для пользователей в домене.*

Настройте локальных пользователей.

# Создайте локального пользователя и настройте для него пароль.

[R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom

Info: Add a new user.

Если в имени пользователя содержится разделитель в виде символа @, то строка символов перед символом @ — это имя пользователя, а строка символов после символа @ — имя домена. Если в имени пользователя нет разделителя в виде символа @, вся символьная строка представляет собой имя пользователя, а для домена используется имя по умолчанию.

# Настройте параметры для локального пользователя, такие как тип доступа и уровень полномочий.

[R2-aaa]local-user hcia@datacom service-type telnet

Команда **local-user service-type** позволяет настроить тип доступа для локального пользователя. После настройки типа доступа пользователь сможет успешно войти в систему, только применив настроенный тип доступа. Если в качестве типа доступа было указано telnet, пользователь не сможет получить доступ к устройству через веб-страницу. Для одного пользователя можно настроить несколько типов доступа.

[R2-aaa]local-user hcia@datacom privilege level 3

Для локального пользователя настроен уровень полномочий. Этому пользователю будут доступны только команды, предоставляемые указанным уровнем полномочий, и команды более низкого уровня полномочий.

Включите функцию telnet на R2.

[R2]telnet server enable

*На устройстве включена функция сервера Telnet. На некоторых устройствах эта функция включена по умолчанию.*

[R2]user-interface vty 0 4

[R2-ui-vty0-4]authentication-mode aaa

Команда **authentication-mode** позволяет настроить режим аутентификации для доступа к пользовательскому интерфейсу. По умолчанию режим аутентификации на пользовательском интерфейсе VTY не настроен. Для интерфейса входа в систему необходимо настроить режим аутентификации. В противном случае пользователи не смогут выполнять вход в устройство.

Проверьте конфигурацию.

# Выполните вход с R1 на R2 через Telnet.

<R1>telnet 10.0.12.2

Press CTRL\_] to quit telnet mode

Trying 10.0.12.2 ...

Connected to 10.0.12.2 ...

Login authentication

Username:hcia@datacom

Password:

<R2>

*С маршрутизатора R1 можно выполнить вход в систему R2.*

# Выведите на экран список пользователей, подключенных к R2.

[R2]display users

User-Intf Delay Type Network Address AuthenStatus AuthorcmdFlag

129 VTY 0 00:02:43 **TEL** **10.0.12.1**  pass

Username : hcia@datacom

----Конец

### Проверка

Подробности данной операции здесь не приводятся.

### Справочные конфигурации

Конфигурация на R1

#

sysname R1

#

interface GigabitEthernet0/0/3

ip address 10.0.12.1 255.255.255.0

#

return

Конфигурация на R2

#

sysname R2

#

aaa

uthentication-scheme datacom

authorization-scheme datacom

domain datacom

authentication-scheme datacom

authorization-scheme datacom

local-user hcia@datacom password irreversible-cipher %^%#.}hB'1"=&=:FWx!Ust(3s^\_<.[Z}kEc/>==P56gUVU\*cE^|]5@|8/O5FC$9A%^%#

local-user hcia@datacom privilege level 3

local-user hcia@datacom service-type telnet

#

interface GigabitEthernet0/0/3

ip address 10.0.12.2 255.255.255.0

#

telnet server enable

#

user-interface vty 0 4

authentication-mode aaa

user privilege level 15

#

return

### Вопросы

Вопросы по этой теме не предоставляются.