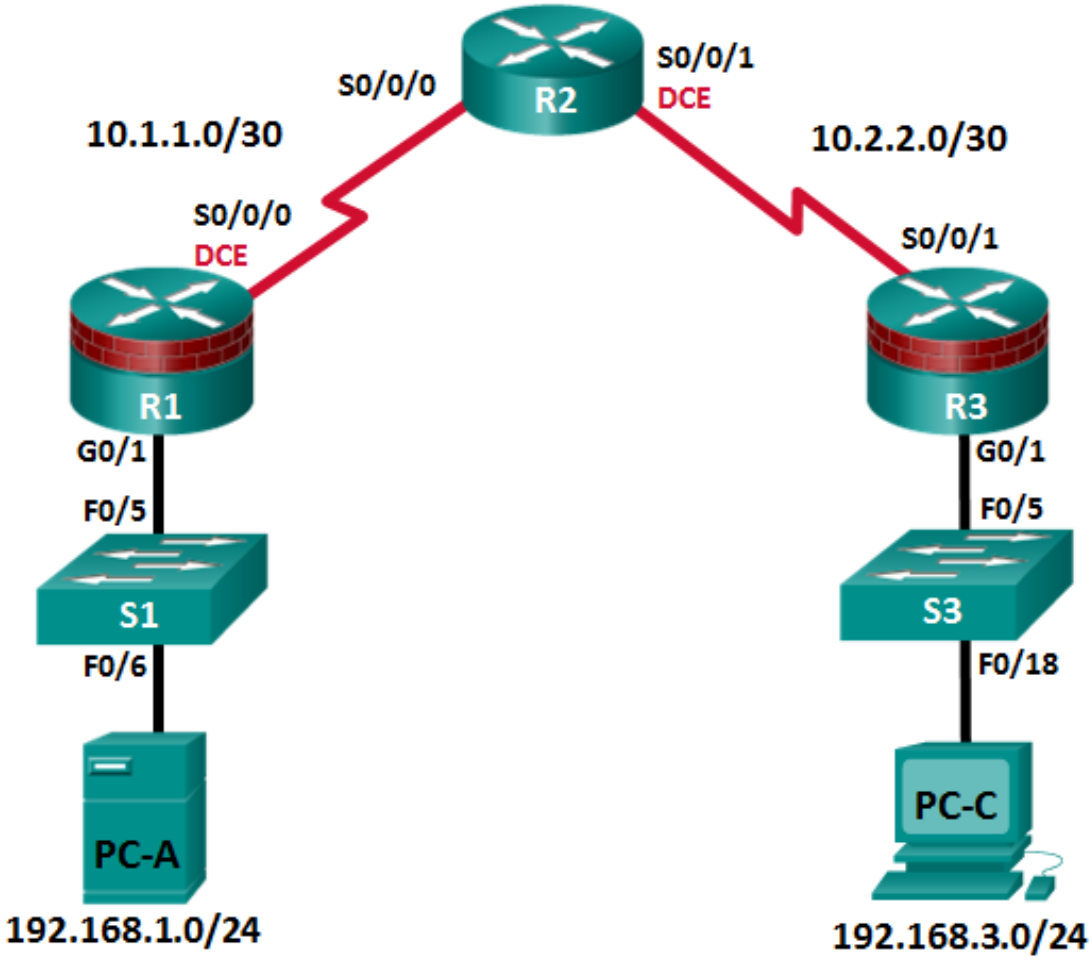
CCNA Security

Лабораторная работа. Защита административного доступа с помощью AAA и RADIUS

Топология



Примечание. В устройствах ISR G1 используются интерфейсы FastEthernet вместо GigabitEthernet.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

Часть 1. Настройка основных параметров устройства

- Настройте основные параметры, такие как имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте статическую маршрутизацию.

Часть 2. Настройка локальной аутентификации

- Настройте локального пользователя базы данных и локальный доступ для линий консоли, vty и aux.
- Проверьте конфигурацию.

Часть 3. Настройка локальной аутентификации с помощью AAA

- Настройте локальную базу данных пользователей с помощью Cisco IOS.
- Настройте локальную аутентификацию AAA с помощью Cisco IOS.
- Проверьте конфигурацию.

Часть 4. Настройка централизованной аутентификации с помощью AAA и RADIUS

- Установите на компьютер сервер RADIUS.
- Настройте пользователей на сервере RADIUS.
- На маршрутизаторе настройте сервисы AAA с помощью Cisco IOS, чтобы получить доступ к серверу RADIUS для аутентификации.
- Проверьте конфигурацию AAA и RADIUS.

Исходные данные/сценарий

Самым распространенным способом обеспечения безопасного доступа к маршрутизатору является создание паролей для линий консоли, vty и aux. При попытке доступа к маршрутизатору у пользователя будет запрашиваться только пароль. Настройка секретного пароля в привилегированном режиме повышает уровень безопасности, но в любом случае для каждого уровня доступа требуется только основной пароль.

Помимо основных паролей, в локальной базе данных маршрутизатора можно настроить отдельные имена или учетные записи пользователей с разными уровнями привилегий, которые могут применяться ко всему маршрутизатору. Когда для линий консоли, vty или aux настроено обращение к этой локальной базе данных, то при использовании любой из этих линий для доступа к маршрутизатору пользователю предлагается ввести имя и пароль.

Для дополнительного контроля над процессом входа может применяться метод аутентификации, авторизации и учета (AAA). Для обеспечения базовой аутентификации функцию AAA можно настроить на доступ к локальной базе данных при вводе имен пользователей. Кроме того, могут быть определены запасные процедуры. Однако данный подход не обладает хорошей масштабируемостью, так как его нужно настраивать на каждом маршрутизаторе. Для обеспечения максимальной масштабируемости и максимально эффективного применения AAA, данную функцию нужно использовать совместно с базой данных внешнего сервера TACACS+ или RADIUS. При попытке пользователя войти в систему маршрутизатор обращается к внешнему серверу базы данных для проверки действительности имени пользователя и пароля.

В данной лабораторной работе вы построите сеть из нескольких маршрутизаторов и настроите маршрутизаторы и хосты. Затем вам будет необходимо использовать команды CLI для настройки на маршрутизаторах базовой локальной аутентификации с помощью AAA. Вы установите на внешнем компьютере программное обеспечение RADIUS и будете использовать AAA для аутентификации пользователей с помощью сервера RADIUS.

Примечание. В данной лабораторной работе используются команды и выходные данные для маршрутизатора Cisco 1941 с ПО Cisco IOS Release 15.4(3)M2 (с лицензией Security Technology Package). Допускается использование других маршрутизаторов и версий Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы для определения идентификаторов интерфейсов с учетом оборудования в лаборатории. В зависимости от модели маршрутизатора и версии Cisco IOS, доступные команды и выходные данные могут отличаться от указанных в данной лабораторной работе.

Примечание. Перед началом работы убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 2 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 2 ПК (Windows 7 или 8.1, с установленным SSH-клиентом и WinRadius)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка основных параметров устройства

В части 1 этой лабораторной работы вы создадите топологию сети и настроите основные параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Все операции должны быть выполнены на маршрутизаторах R1 и R3. На маршрутизаторе R2 необходимо выполнить только шаги 1, 2, 3 и 6. В качестве примера здесь показана процедура для маршрутизатора R1.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

a. Задайте имена хостов согласно топологической схеме.

b. Настройте IP-адреса, как показано в таблице IP-адресов.

c. Настройте тактовую частоту маршрутизаторов с помощью DCE-кабеля, подключенного к последовательному интерфейсу каждого из них.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. Чтобы маршрутизатор не пытался неправильно интерпретировать введенные команды как имена хостов, отключите функцию DNS-поиска.

```
R1(config)# no ip domain-lookup
```


Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.

a. Настройте статический маршрут по умолчанию из маршрутизатора R1 в R2 и из маршрутизатора R3 в R2.

b. Настройте статический маршрут из маршрутизатора R2 к LAN маршрутизатора R1 и статический маршрут из маршрутизатора R2 к LAN маршрутизатора R3.

Шаг 4: Настройте параметры IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-C, как показано в таблице IP-адресов.

Шаг 5: Проверьте связь между компьютером PC-A и маршрутизатором R3.

a. Отправьте эхо-запрос с маршрутизатора R1 на маршрутизатор R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, то это означает, что статическая маршрутизация настроена верно и работает исправно. Если эхо-запрос был выполнен с ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командами **show run** и **show ip route**, чтобы определить проблемы, связанные с протоколом маршрутизации.

Шаг 6: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Шаг 7: Сконфигурируйте и зашифруйте пароли на маршрутизаторах R1 и R3.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегчения процесса выполнения лабораторной работы пароли были относительно упрощены. В производственной сети рекомендуется использовать более сложные пароли.

На данном шаге настройте параметры одинаковым образом на маршрутизаторах R1 и R3. В качестве примера здесь показан маршрутизатор R1.

a. Задайте минимальную длину пароля.

Используйте команду **security passwords**, чтобы задать минимальную длину пароля в 10 символов.

```
R1(config)# security passwords min-length 10
```

b. Настройте пароль **enable secret** на обоих маршрутизаторах. Используйте алгоритм хеширования type 9 (SCRYPT).

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

Шаг 8: Настройте основную консоль, вспомогательный порт и линии vty.

a. Настройте пароль консоли и активируйте вход в систему для маршрутизатора 1. Для дополнительной безопасности команда **exec-timeout** обеспечивает выход из системы линии, если в течение **5** минут отсутствует активность. Команда **logging synchronous** предотвращает прерывание ввода команд сообщениями консоли.

Примечание. Чтобы исключить необходимость постоянного повторного входа в систему во время лабораторной работы, вы можете ввести команду **exec-timeout** с параметрами 0 0, чтобы отключить проверку истечения времени ожидания. Однако такой подход не считается безопасным.

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```


b. Настройте пароль для порта AUX для маршрутизатора R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

c. Настройте пароль на линиях vty для маршрутизатора R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Зашифруйте пароли для консоли, aux и vty.

```
R1(config)# service password-encryption
```

e. Введите команду **show run**. Можете ли вы прочитать пароли для консоли, aux и vty? Поясните ответ.

_____

_____

Шаг 9: Настройте предупреждающий баннер при входе в систему на маршрутизаторах R1 и R3.

a. Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневным сообщением (MOTD) с помощью команды **banner motd**. При подключении пользователя к маршрутизатору до запроса на ввод авторизационных данных отображается баннер MOTD. В данном примере в начале и конце сообщения используется знак доллара ($).

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Выйдите из привилегированного режима с помощью команды **disable** или **exit**, а затем нажмите **Enter** для начала работы.

Если баннер отображается некорректно, создайте его заново с помощью команды **banner motd.**

Шаг 10: Сохраните базовые конфигурации на всех маршрутизаторах.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

```
R1# copy running-config startup-config
```

Часть 2: Настройка локальной аутентификации

В части 2 данной лабораторной работы необходимо создать локальное имя пользователя и пароль, а также настроить способ доступа к линиям консоли, aux и vty через локальную базу данных маршрутизатора, где находятся действительные имена пользователей и пароли. Выполните все шаги на маршрутизаторах R1 и R3. Ниже показана процедура для маршрутизатора R1.

Шаг 1: Настройте локальную базу данных пользователей.

a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хеширования MD5. Используйте алгоритм хеширования type 9 (SCRYPT).

```
R1(config)# username user01 algorithm-type scrypt secret user01pass
```

b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать пароль пользователя?

_____

_____

Шаг 2: Настройте локальную аутентификацию для линии консоли и входа в систему.

a. Настройте линию консоли на использование локально определенных имен пользователей и паролей.

```
R1(config)# line console 0
R1(config-line)# login local
```

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

```
R1 con0 is now available. Press RETURN to get started.
```

c. Войдите в систему с помощью ранее настроенной учетной записи **user01** и пароля.

Чем сейчас отличается вход через консоль от того, что было раньше?

_____

_____

d. После входа введите команду **show run.** Вам удалось отправить команду? Поясните ответ.

_____

_____

Войдите в привилегированный режим, используя команду **enable**. У вас был запрошен пароль? Поясните ответ.

_____

_____

Шаг 3: Проверьте новую учетную запись путем входа в рамках сеанса Telnet.

a. Установите сеанс Telnet с маршрутизатором R1 с компьютера PC-A.

```
PC-A> telnet 192.168.1.1
```

b. Система запросила у вас учетные данные? Поясните ответ.

_____

_____

c. Настройте линию vty на использование ранее локально определенных учетных записей и паролей и сконфигурируйте команду **transport input**, чтобы разрешить Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# exit
```

d. Повторно свяжитесь с маршрутизатором R1 с компьютера PC-A с помощью Telnet.

```
PC-A> telnet 192.168.1.1
```

Система запросила у вас учетные данные? Поясните ответ.

_____

e. Войдите в систему как пользователь **user01** с паролем **user01pass**.

f. Во время сеанса Telnet с маршрутизатором R1 войдите в привилегированный режим с помощью команды **enable**.

Какой пароль вы использовали?

_____

g. Для дополнительной безопасности настройте порт AUX на использование локально определенных учетных записей для входа.

```
R1(config)# line aux 0
R1(config-line)# login local
```

h. Завершите сеанс Telnet с помощью команды **exit**.

Шаг 4: Сохраните конфигурацию на маршрутизаторе R1.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

```
R1# copy running-config startup-config
```

Шаг 5: Выполните шаги 1–4 на маршрутизаторе R3 и сохраните конфигурацию.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

Часть 3: Настройка локальной аутентификации на маршрутизаторе R3 с помощью AAA

Задача 1: Настройка локальной базы данных пользователей с помощью Cisco IOS.

Шаг 1: Настройте локальную базу данных пользователей.

a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хеширования SCRYPT.

```
R3(config)# username Admin01 privilege 15 algorithm-type scrypt secret Admin01pass
```

b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать пароль пользователя?

_____

_____

Задача 2: Настройка локальной аутентификации AAA с помощью Cisco IOS.

Включите сервисы на маршрутизаторе R3 с помощью команды **aaa new-model** в режиме глобальной настройки. Так как вы устанавливаете локальную аутентификацию, используйте ее в качестве первичного метода и метод без аутентификации – в качестве вторичного.

Если вы использовали метод аутентификации через удаленный сервер, например TACACS+ или RADIUS, вы должны были настроить вторичный метод аутентификации в качестве запасного, если сервер недоступен. Обычно вторичным методом является аутентификация по локальной базе данных. В нашем случае, если в локальной базе данных не настроены имена пользователей, маршрутизатор будет предоставлять доступ к устройству всем пользователям.

Шаг 1: Включите сервисы AAA.

```
R3(config)# aaa new-model
```

Шаг 2: Разверните сервисы AAA с помощью локальной базы данных.

a. Настройте список аутентификации для входа в систему по умолчанию с помощью команды **aaa authentication login default** *method1[method2][method3];* укажите список методов с помощью ключевых слов **local** и **none.**

```
R3(config)# aaa authentication login default local-case none
```

Примечание. Если вы не укажете список методов аутентификации по умолчанию, маршрутизатор может быть заблокирован, и вам будет нужно выполнить процедуру восстановления пароля для конкретного маршрутизатора.

Примечание. Параметр **local-case** используется для того, чтобы сделать имена пользователей зависимыми от регистра.

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

```
R3 con0 is now available

Press RETURN to get started.
```

Войдите в консоль как **Admin01** с паролем **Admin01pass.** Помните, что сейчас и имена пользователей, и пароли чувствительны к регистру. Вам удалось войти? Поясните ответ.

_____

_____

Примечание. Если ваш сеанс через порт консоли маршрутизатора истекает по времени, вам может потребоваться войти в систему с помощью списка методов аутентификации по умолчанию.

c. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

```
R3 con0 is now available

Press RETURN to get started.
```

d. Попытайтесь войти в консоль как пользователь **baduser** с любым паролем. Вам удалось войти? Поясните ответ.

_____

_____

e. Если в локальной базе данных учетные записи пользователей не настроены, каким пользователям будет предоставлен доступ к устройству?

_____

_____

Шаг 3: Создайте профиль аутентификации AAA для Telnet с помощью локальной базы данных.

a. Создайте отдельный список методов аутентификации для доступа к маршрутизатору по Telnet. В нем не должно быть запасного метода без аутентификации, поэтому если в локальной базе данных не будет имен пользователей, доступ по Telnet будет отключен. Для создания профиля аутентификации, который не является профилем по умолчанию, укажите имя списка TELNET_LINES и примените его к линиям vty.

```
R3(config)# aaa authentication login TELNET_LINES local
R3(config)# line vty 0 4
R3(config-line)# login authentication TELNET_LINES
```

b. Убедитесь, что профиль аутентификации используется при открытии сеанса Telnet с компьютера PC-C на маршрутизатор R3.

```
PC-C> telnet 192.168.3.1
Trying 192.168.3.1 ... Open
```

c. Войдите как **Admin01** с паролем **Admin01pass.** Вам удалось войти? Поясните ответ.

_____

_____

d. Завершите сеанс Telnet с помощью команды **exit**, затем снова подключитесь к маршрутизатору R3 по Telnet.

e. Попытайтесь войти как **baduser** с любым паролем. Вам удалось войти? Поясните ответ.

_____

_____

Задача 3: Изучение отладки аутентификации AAA с помощью Cisco IOS.

В этом задании с помощью команды **debug** вы рассмотрите успешные и неуспешные попытки аутентификации.

Шаг 1: Убедитесь, что системное время и временные метки для отладки правильно настроены.

a. От имени пользователя маршрутизатора R3 или в привилегированном режиме введите команду **show clock,** чтобы определить, какое текущее время установлено на маршрутизаторе. Если время и дата установлены неправильно, установите их в привилегированном режиме по команде **clock set HH:MM:SS DD month YYYY.** Ниже приведен пример для маршрутизатора R3.

```
R3# clock set 14:15:00 13 September 2019
```

b. Убедитесь, что подробная информация о временных метках доступна в выходных данных отладки, с помощью команды **show run.** Эта команда отобразит все строки текущей конфигурации, в которых есть текст timestamps (временные метки).

```
R3# show run | include timestamps
service timestamps debug datetime msec
service timestamps log datetime msec
```

c. Если команда **service timestamps debug** отсутствует, введите ее в режиме глобальной настройки.

```
R3(config)# service timestamps debug datetime msec
R3(config)# exit
```

d. Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

```
R3# copy running-config startup-config
```

Шаг 2: Используйте отладку для проверки доступа пользователя.

a. Включите отладку для аутентификации AAA.

```
R3# debug aaa authentication
AAA Authentication debugging is on
```

b. Запустите на маршрутизаторе R2 сеанс Telnet с маршрутизатором R3.

c. Войдите под именем пользователя **Admin01** и паролем **Admin01pass**. Просмотрите события аутентификации AAA в окне сеанса консоли. Там должны отображаться сообщения об отладке, похожие на следующие.

```
R3#
Feb 20 08:45:49.383: AAA/BIND(0000000F): Bind i/f
Feb 20 08:45:49.383: AAA/AUTHEN/LOGIN (0000000F): Pick method list 'TELNET_LINES'
```

d. Из окна Telnet перейдите в привилегированный режим. Используйте пароль привилегированного доступа **cisco12345**. Там должны отображаться сообщения об отладке, похожие на следующие. Обратите внимание на имя пользователя в третьей строке (Admin01), номер виртуального порта (tty132) и адрес удаленного клиента Telnet (10.2.2.2). Также обратите внимание, что последняя строка о состоянии – PASS.

```
R3#
Feb 20 08:46:43.223: AAA: parse name=tty132 idb type=-1 tty=-1
Feb 20 08:46:43.223: AAA: name=tty132 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=132
channel=0
Feb 20 08:46:43.223: AAA/MEMORY: create user (0x32716AC8) user='Admin01' ruser='NULL' ds0=0
port='tty132' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 initial_task_id='0',
vrf= (id=0)
Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): port='tty132' list='' action=LOGIN
service=ENABLE
Feb 20 08:46:43.223: AAA/AUTHEN/START (2
R3#655524682): non-console enable - default to enable password
Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): Method=ENABLE
```



```
Feb 20 08:46:43.223: AAA/AUTHEN (2655524682): status = GETPASS
R3#
Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): continue_login (user='(undef)')
Feb 20 08:46:46.315: AAA/AUTHEN (2655524682): status = GETPASS
Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): Method=ENABLE
Feb 20 08:46:46.543: AAA/AUTHEN (2655524682): status = PASS
```

e. В окне Telnet выйдите из привилегированного режима с помощью команды **disable.** Попытайтесь перейти в привилегированный режим снова, но на этот раз используйте неправильный пароль. Просмотрите выходные данные отладчика на маршрутизаторе R3. Обратите внимание, что сейчас состояние – FAIL.

```
Feb 20 08:47:36.127: AAA/AUTHEN (4254493175): status = GETPASS
Feb 20 08:47:36.127: AAA/AUTHEN/CONT (4254493175): Method=ENABLE
Feb 20 08:47:36.355: AAA/AUTHEN(4254493175): password incorrect
Feb 20 08:47:36.355: AAA/AUTHEN (4254493175): status = FAIL
Feb 20 08:47:36.355: AAA/MEMORY: free_user (0x32148CE4) user='NULL' ruser='NULL' port='tty132'
rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
R3#
```

f. В окне Telnet выйдите из сеанса Telnet с маршрутизатором. Попытайтесь снова открыть сеанс Telnet с маршрутизатором, но на этот раз попытайтесь войти в систему как **Admin01** с неправильным паролем. Выходные данные отладчика в окне консоли должны быть похожи на следующее.

```
Feb 20 08:48:17.887: AAA/AUTHEN/LOGIN (00000010): Pick method list 'TELNET_LINES'
```

Какое сообщение было показано на экране клиента Telnet?

_____

_____

g. Выключите полностью процесс отладки с помощью команды привилегированного режима **undebug all.**

Часть 4: Настройка централизованной аутентификации с помощью AAA и RADIUS

В части 4 данной лабораторной работы необходимо установить программное обеспечение RADIUS на компьютере PC-A. Затем необходимо настроить доступ на маршрутизаторе R1 к внешнему серверу RADIUS для аутентификации пользователей. В этой части лабораторной работы используется бесплатный сервер WinRadius.

Задача 1: Восстановление базовой конфигурации маршрутизатора R1.

Чтобы избежать ошибок из-за созданной ранее конфигурации AAA RADIUS, начните с возврата базовых настроек на маршрутизаторе R1, как показано в частях 1 и 2 данной лабораторной работы.

Шаг 1: Повторно загрузите и восстановите сохраненную конфигурацию на маршрутизаторе R1.

На данном шаге верните базовые настройки на маршрутизаторе, сохраненные в частях 1 и 2.

a. Подключитесь к консоли маршрутизатора R1, войдите в систему как **user01** с паролем **user01pass.**

b. Войдите в привилегированный режим с паролем **cisco12345.**

c. Перезагрузите маршрутизатор и ответьте **no** на запрос о сохранении конфигурации.

```
R1# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```


Шаг 2: Проверьте связь.

a. Проверьте связь, отправив эхо-запрос с компьютера PC-A на PC-C. Если запрос выполнился с ошибкой, устраните неисправности в настройках маршрутизатора и ПК.

b. Если вы вышли из консоли, войдите снова как **user01** с паролем **user01pass**, затем войдите в привилегированный режим с паролем **cisco12345.**

Задача 2: Загрузка и установка на компьютере PC-A сервера RADIUS.

Существует несколько серверов RADIUS, как платных, так и бесплатных. В данной лабораторной работе используется WinRadius – стандартный бесплатный сервер RADIUS, работающий под управлением ОС Windows. Бесплатная версия этого ПО поддерживает лишь 5 имен пользователей.

Примечание. Zip-архив с программным обеспечением WinRadius можно запросить у своего инструктора.

Шаг 1: Загрузите программное обеспечение WinRadius.

a. Создайте папку с именем **WinRadius** на рабочем столе или в другом месте, куда будете сохранять файлы.

b. Распакуйте архив с WinRadius в папку, созданную на шаге 1a. Среди них не будет файла с установщиком. Распакованный файл WinRadius.exe является исполняемым.

c. На рабочем столе можно создать ярлык для файла WinRadius.exe.

Примечание. Если WinRadius используется на компьютере под управлением ОС Microsoft Windows Vista или Microsoft Windows 7, есть вероятность, что интерфейс ODBC (Open Database Connectivity) не будет создан, так как он не сможет записывать данные в реестр.

Возможные решения:

a. Настройки для Compatibility (совместимость)

1) Щелкните правой кнопкой мыши значок **WinRadius.exe** и выберите **Properties**.

2) В диалоговом окне **Properties** перейдите на вкладку **Compatibility.** На этой вкладке установите флажок **Run this program in compatibility mode for**. Затем в раскрывающемся меню снизу выберите установленную на вашем компьютере операционную систему (например, Windows 7).

3) Нажмите **ОК.**

b. Настройки для Run as Administrator

1) Щелкните правой кнопкой мыши значок **WinRadius.exe** и выберите **Properties**.

2) В диалоговом окне **Properties** перейдите на вкладку **Compatibility.** На этой вкладке установите флажок **Run this program as administrator** в разделе Privilege Level.

3) Нажмите **ОК.**

c. Выберите Run as Administration для каждого запуска

1) Щелкните правой кнопкой значок **WinRadius.exe** и выберите **Run as Administrator**.

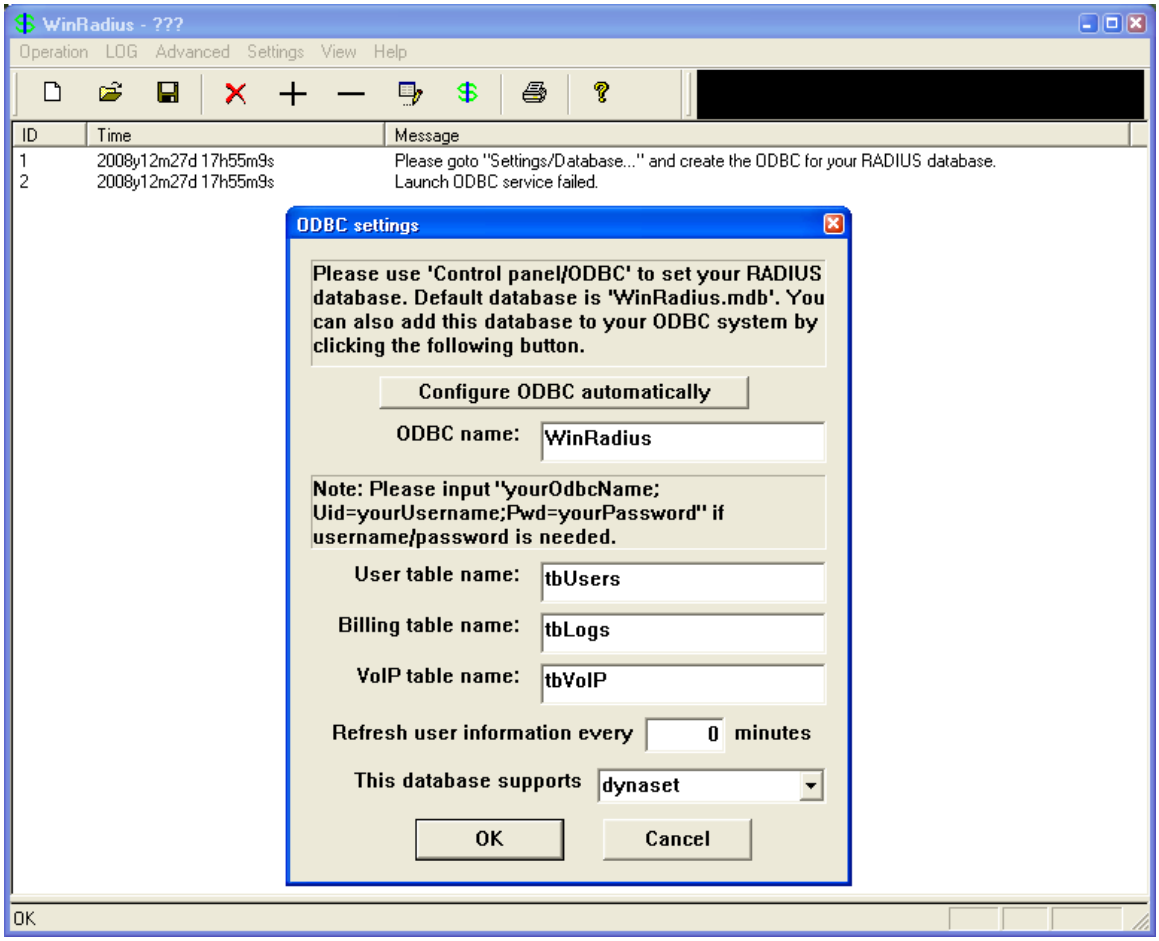
2) После запуска ПО WinRadius нажмите **Yes** в диалоговом окне User Account Control.

Шаг 2: Настройте базу данных сервера WinRadius.

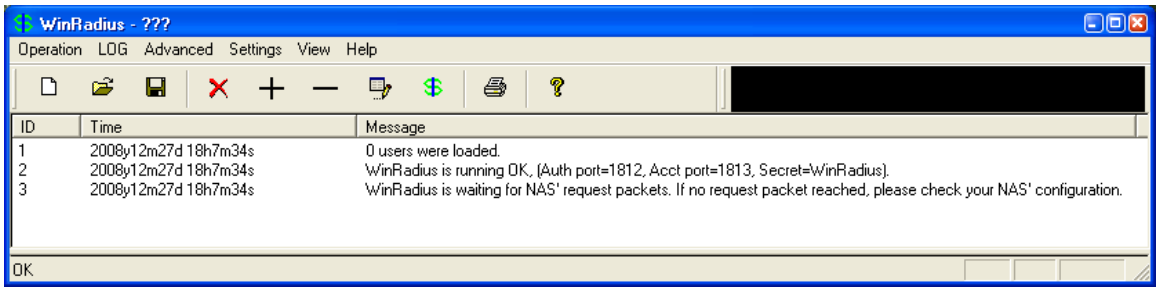
a. Запустите приложение WinRadius.exe**.** WinRadius использует локальную базу данных для хранения информации о пользователях. При первом запуске приложения появятся следующие сообщения:

```
Please go to "Settings/Database and create the ODBC for your RADIUS database.
Launch ODBC failed.
```


b. В главном меню выберите **Settings > Database.** Появится следующий экран. Нажмите кнопку **Configure ODBC Automatically,** затем нажмите **OK.** Вы должны получить сообщение, что ODBC был создан успешно. Выйдите из WinRadius и перезапустите приложение, чтобы применить изменения.



c. При повторном запуске WinRadius вы должны увидеть следующие сообщения.



Примечание по серверу WinRadius.

Бесплатная версия WinRadius поддерживает только пять имен пользователей. Если первое сообщение на указанном выше экране показывает, что загружено больше 0 пользователей, удалите ранее добавленных пользователей из базы данных WinRadius.

Чтобы определить существующие в базе данных имена пользователей, нажмите **Operation** > **Query**, затем нажмите **OK.** Список имен пользователей, находящихся в базе данных, будет отображен в нижней части окна WinRadius.

Чтобы удалить пользователя, нажмите **Operation** > **Delete User**, затем введите имя пользователя в точности так, как указано в списке. Имена пользователей чувствительны к регистру.

d. Какие порты слушает WinRadius для учета и аутентификации?

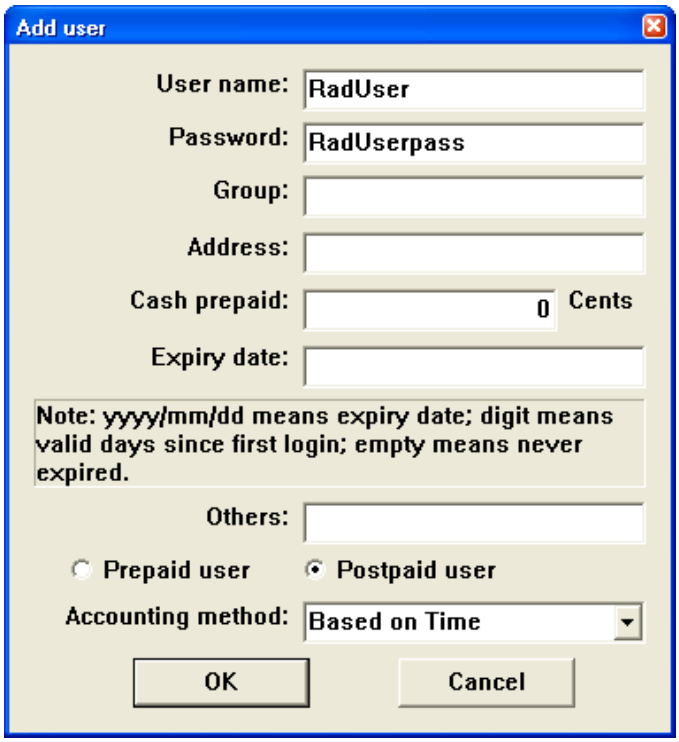
_____

_____

Шаг 3: Настройте пользователей и пароли на сервере WinRadius.

a. В главном меню выберите **Operation** > **Add User**.

b. Введите имя пользователя **RadUser** и пароль **RadUserpass.** Помните, что пароли чувствительны к регистру.



c. Нажмите **OK.** Вы должны получить сообщение в окне журнала о том, что пользователь успешно добавлен.

Шаг 4: Очистите окно журнала.

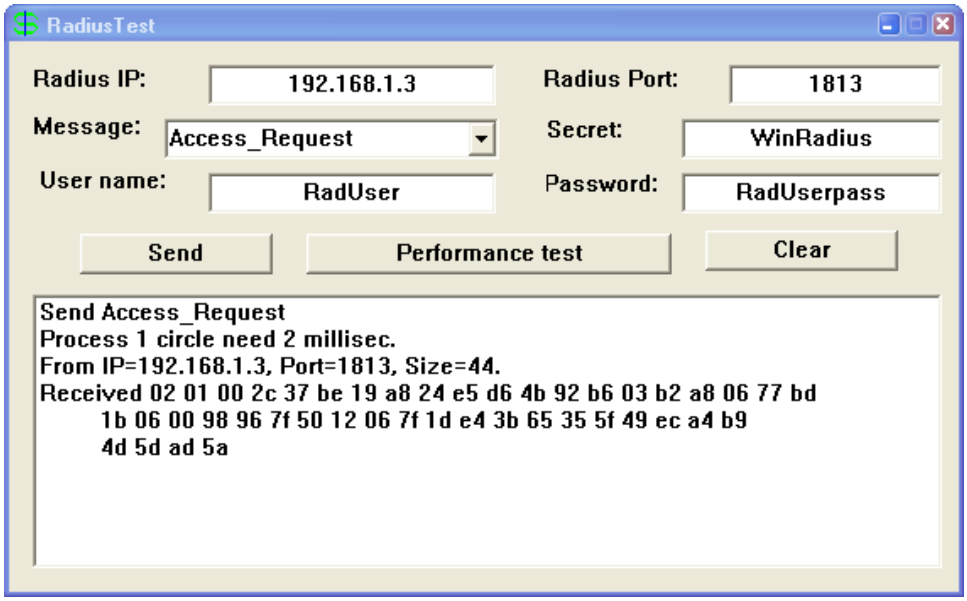
В главном меню выберите **Log** > **Clear**.

Шаг 5: Проверьте только что добавленного пользователя с помощью утилиты тестирования WinRadius.

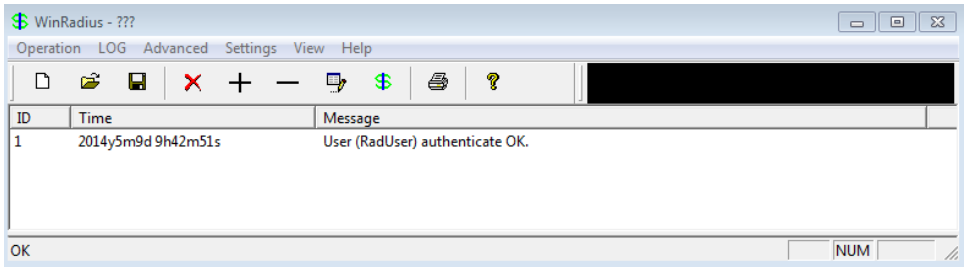
a. В скачанном архиве находится утилита тестирования WinRadius. Перейдите в папку, куда вы распаковали WinRadius.zip, и найдите файл RadiusTest.exe.

b. Запустите приложение RadiusTest, введите IP-адрес сервера RADIUS (**192.168.1.3),** имя пользователя **RadUser** и пароль **RadUserpass,** как показано ниже. Не изменяйте номер порта RADIUS по умолчанию 1813 и пароль RADIUS **WinRadius.**

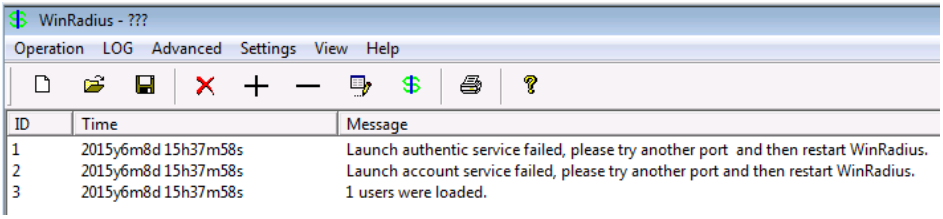
c. Нажмите **Send**, после чего вы должны увидеть сообщение Send Access_Request, в котором будет указано, что сервер по адресу 192.168.1.3 через порт 1813 получил 44 шестнадцатеричных символа.



d. Просмотрите журнал WinRadius и убедитесь, что пользователь RadUser был успешно аутентифицирован.



Примечание. Приложение WinRadius может быть свернуто в значок на панели задач. Оно продолжит работать во время запуска приложения RadiusTest и при попытке повторного запуска выведет сообщение об ошибке сервиса. Разверните окно WinRadius на экране, щелкнув значок на панели задач.



e. Закройте приложение RadiusTest.

Задача 3: Настройка на маршрутизаторе R1 сервисов AAA и получение доступа к серверу RADIUS с помощью Cisco IOS.

Шаг 1: Включите AAA на маршрутизаторе R1.

Воспользуйтесь командой **aaa new-model** в режиме глобальной настройки, чтобы включить AAA.

```
R1(config)# aaa new-model
```

Шаг 2: Настройте список методов аутентификации при входе в систему по умолчанию.

a. Настройте список на первоочередное использование RADIUS для сервиса аутентификации, а далее – без аутентификации. Если сервер RADIUS недоступен и аутентификация не может быть выполнена, маршрутизатор глобально разрешает доступ без аутентификации. Это необходимо для случая, если маршрутизатор начнет работу без связи с активным сервером RADIUS.

```
R1(config)# aaa authentication login default group radius none
```

b. В качестве альтернативы вы можете настроить локальную аутентификацию в качестве запасного метода.

Примечание. Если вы не укажете список методов аутентификации по умолчанию, маршрутизатор может быть заблокирован, и вам будет нужно выполнить процедуру восстановления пароля для конкретного маршрутизатора.

Шаг 3: Укажите сервер RADIUS.

a. Используйте команду **radius server** для входа в режим настройки сервера RADIUS.

```
R1(config)# radius server CCNAS
```

b. Используйте символ ? для вывода списка команд подрежима для настройки сервера RADIUS.

```
R1(config-radius-server)# ?
RADIUS server sub-mode commands:
  address          Specify the radius server address
  automate-tester  Configure server automated testing.
  backoff          Retry backoff pattern(Default is retransmits with constant
                   delay)
  exit             Exit from RADIUS server configuration mode
  key              Per-server encryption key
  no               Negate a command or set its defaults
  non-standard     Attributes to be parsed that violate RADIUS standard
  pac              Protected Access Credential key
  retransmit       Number of retries to active server (overrides default)
  timeout          Time to wait (in seconds) for this radius server to reply
                   (overrides default)
```

c. Используйте команду **address** для настройки IP-адреса для компьютера PC-A.

```
R1(config-radius-server)# address ipv4 192.168.1.3
```

d. Команда **key** используется для установки секретного пароля, который является общим для сервера RADIUS и маршрутизатора (в данном случае R1) и применяется для аутентификации соединения между маршрутизатором и сервером прежде, чем начнется процесс аутентификации пользователя. Используйте секретный пароль NAS по умолчанию **WinRadius,** указанный на сервере RADIUS (см. задачу 2, шаг 5). Помните, что пароли чувствительны к регистру.

```
R1(config-radius-server)# key WinRadius
R1(config-redius-server)# end
```


Задача 4: Проверка конфигурации AAA RADIUS.

Шаг 1: Проверьте связь между маршрутизатором R1 и компьютером, на котором работает сервер RADIUS.

Отправьте эхо-запрос с маршрутизатора R1 на компьютер PC-A.

```
R1# ping 192.168.1.3
```

Если запрос выполнен с ошибкой, проведите диагностику основных настроек компьютера и маршрутизатора перед тем, как продолжить.

Шаг 2: Проверьте конфигурацию.

a. Если вы перезапускали сервер WinRadius, вам потребуется заново создать пользователя **RadUser** с паролем **RadUserpass** путем выбора **Operation** > **Add User**.

b. Очистите журнал на сервере WinRadius путем выбора **Log** > **Clear** в главном меню.

c. На маршрутизаторе R1 перейдите на начальный экран маршрутизатора, на котором отображается:

```
R1 con0 is now available


Press RETURN to get started.
```

d. Проверьте конфигурацию – войдите в консоль на маршрутизаторе R1, используя имя пользователя **RadUser** и пароль **RadUserpass.** Удалось ли вам получить доступ в привилегированный режим и если да, была ли задержка?

_____

e. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

```
R1 con0 is now available


Press RETURN to get started.
```

f. Проверьте конфигурацию – войдите в консоль на маршрутизаторе R1, используя несуществующее имя пользователя **Userxxx** и пароль **Userxxxpass.** Удалось ли вам получить доступ в привилегированный режим? Поясните ответ.

_____

_____

g. Были ли отображены какие-либо сообщения в журнале сервера RADIUS или при входе?

_____

h. Почему несуществующему пользователю удалось получить доступ к маршрутизатору и при этом не были выведены сообщения в журнале сервера RADIUS?

_____

_____

i. Когда сервер RADIUS недоступен, после попыток входа в систему могут появляться примерно следующие сообщения:

```
*Dec 26 16:46:54.039: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.3:1645,1646 is not
responding.
*Dec 26 15:46:54.039: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.3:1645,1646 is being marked
alive.
```


Шаг 3: Устраните неполадки при связи между маршрутизатором и сервером RADIUS.

a. Проверьте номера портов Cisco IOS RADIUS UDP по умолчанию, используемые на маршрутизаторе R1: снова войдите в режим настройки сервера RADIUS с помощью команды **radius server**, а затем используйте функцию Cisco IOS Help в команде подрежима **address.**

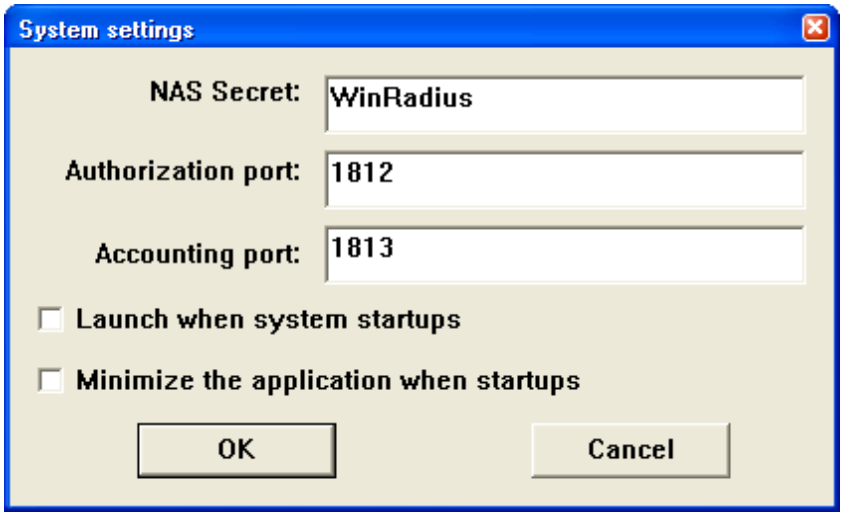
```
R1(config)# radius server CCNAS
R1(config-radius-server)# address ipv4 192.168.1.3 ?
  acct-port   UDP port for RADIUS acco/unting server (default is 1646)
  alias         1-8 aliases for this server (max. 8)
  auth-port   UDP port for RADIUS authentication server (default is 1645)
  <cr>
```

Каковы номера портов Cisco IOS UDP по умолчанию маршрутизатора R1 для сервера RADIUS?

_____

Шаг 4: Проверьте номера портов по умолчанию на сервере WinRadius на компьютере PC-A.

В главном меню WinRadius выберите **Settings > System.**



Каковы номера портов WinRadius UDP по умолчанию? _____

Примечание. В документе RFC 2865 официально назначены номера портов 1812 и 1813 для RADIUS.

Шаг 5: Поменяйте номера портов RADIUS на маршрутизаторе R1 для соответствия с сервером WinRadius.

Если не указано иное, конфигурация Cisco IOS RADIUS по умолчанию настроена на номера портов UDP 1645 и 1646. Либо номера портов Cisco IOS должны быть изменены в соответствии с номерами портов сервера RADIUS, либо номера портов сервера RADIUS должны быть изменены в соответствии с номерами портов маршрутизатора Cisco IOS.

Снова введите команду подрежима address. На этот раз укажите номера портов **1812** и **1813,** а также адрес IPv4.

```
R1(config-radius-server)# address ipv4 192.168.1.3 auth-port 1812 acct-port 1813
```


Шаг 6: Проверьте конфигурацию, войдя в консоль на маршрутизаторе R1.

a. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться: R1 con0 is now available, Press **RETURN** to get started.

b. Снова войдите под именем **RadUser** и паролем **RadUserpass.** Вам удалось войти? Была ли задержка на этот раз?

_____

_____

c. В журнале на сервере RADIUS должно появиться следующее сообщение.

```
User (RadUser) authenticate OK.
```

d. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

```
R1 con0 is now available, Press RETURN to get started.
```

e. Снова войдите с именем **Userxxx** и паролем **Userxxxpass.** Вам удалось войти?

_____

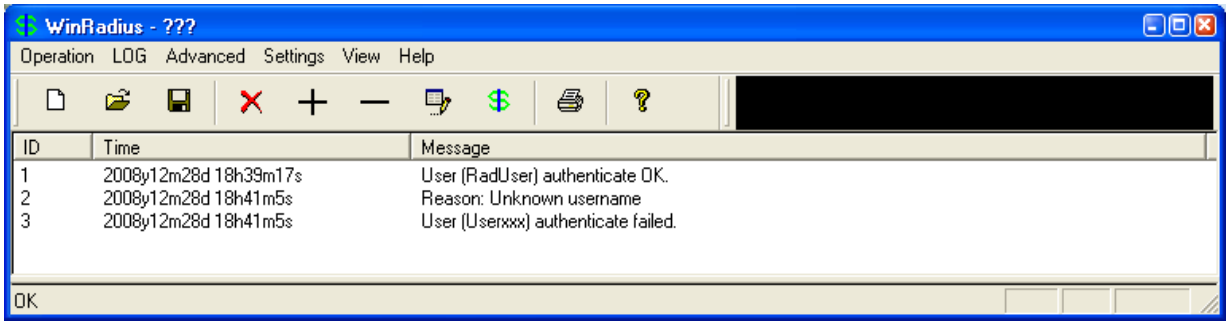
_____

Какое сообщение появилось на маршрутизаторе?

_____

В журнале на сервере RADIUS должны появиться следующие сообщения.

```
Reason: Unknown username
User (Userxxx) authenticate failed
```



Шаг 7: Создайте список методов аутентификации для Telnet и протестируйте его.

a. Создайте отдельный список методов аутентификации для доступа к маршрутизатору по Telnet. В нем не должно быть запасного режима «без аутентификации», поэтому если доступ к серверу RADIUS отсутствует, то доступ по Telnet будет отключен. Назовите данный список **TELNET_LINES**.

```
R1(config)# aaa authentication login TELNET_LINES group radius
```

b. Примените список к линиям vty на маршрутизаторе, используя команду login authentication.

```
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET_LINES
```

c. Подключитесь с компьютера PC-A к маршрутизатору R1 по Telnet и войдите с именем **RadUser** и паролем **RadUserpass.** Вам удалось получить доступ для входа? Поясните ответ.

_____

_____

d. Завершите сеанс Telnet, затем снова с компьютера PC-A подключитесь к маршрутизатору R1 по Telnet. Войдите с именем **Userxxx** и паролем **Userxxxpass.** Вам удалось войти? Поясните ответ.

_____

_____

Вопросы для повторения

1. Зачем организации может понадобиться использование централизованного сервера аутентификации вместо того, чтобы настраивать пользователей и пароли на каждом маршрутизаторе по отдельности?

_____

_____

_____

_____

_____

_____

_____

_____

2. Сравните локальную аутентификацию и локальную аутентификацию с использованием AAA.

_____

_____

_____

_____

_____

_____

_____

_____

3. На основе содержания онлайн-курса Академии, результатов поиска в Интернете, а также использования RADIUS в данной лабораторной работе сравните RADIUS и TACACS+.

_____

_____

_____

_____

_____

_____

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.

