Packet Tracer. Настройка аутентификации AAA на маршрутизаторах Cisco. Топология

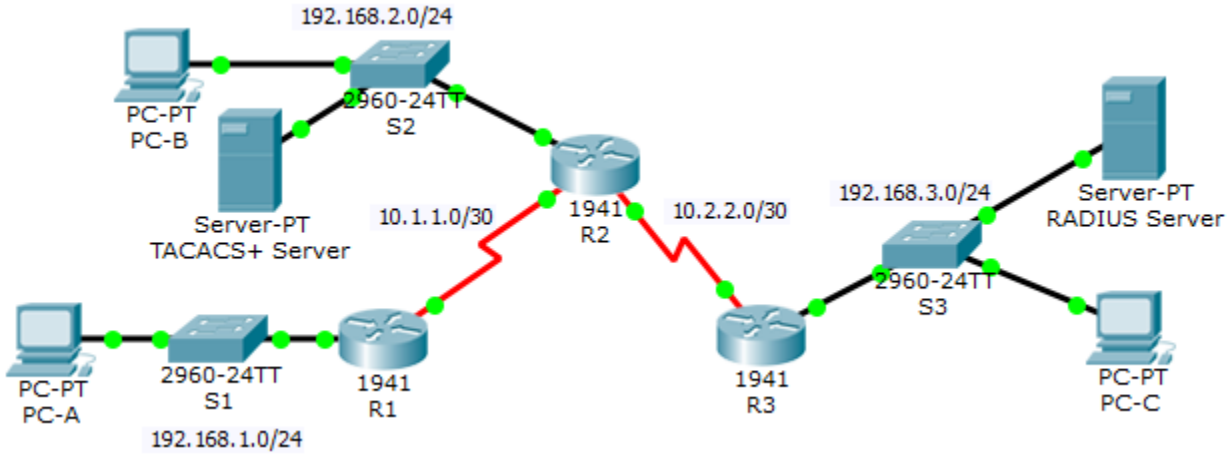

Таблица адресации

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 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	Н/П	Н/П
R2	G0/0	192.168.2.1	255.255.255.0	Н/П	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.1	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	10.2.2.2	255.255.255.252	Н/П	Н/П
Сервер TACACS+	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
Сервер RADIUS	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

- Настройка учетной записи локального пользователя на маршрутизаторе R1 и настройка аутентификации на линиях консоли и VTY с использованием локального решения AAA.
- Проверка локальной аутентификации AAA с консоли R1 и клиента PC-A.
- Настройка серверной аутентификации AAA по протоколу TACACS+.
- Проверка серверной аутентификации AAA с клиента PC-B.
- Настройка серверной аутентификации AAA по протоколу RADIUS.
- Проверка серверной аутентификации AAA с клиента PC-C.

Исходные данные/сценарий

Топология сети включает маршрутизаторы R1, R2 и R3. В настоящее время все административные меры безопасности основаны на знании секретного пароля. Ваша задача – настроить и проверить решения AAA на базе сервера.

Вы создадите учетную запись локального пользователя и настроите локальную аутентификацию AAA на маршрутизаторе R1 для проверки входа в консоль и VTY.

- Учетная запись пользователя: **Admin1** и пароль **admin1pa55**

Затем на маршрутизаторе R2 вы настроите поддержку серверной аутентификации по протоколу TACACS+. Сервер TACACS+ был предварительно настроен следующим образом.

- Клиент: **R2** с ключевым словом **tacacspa55**
- Учетная запись пользователя: **Admin2** и пароль **admin2pa55**

Наконец, на маршрутизаторе R3 вы настроите поддержку серверной аутентификации по протоколу RADIUS. Сервер RADIUS был предварительно настроен следующим образом.

- Клиент: **R3** с ключевым словом **radiuspa55**
- Учетная запись пользователя: **Admin3** и пароль **admin3pa55**

На маршрутизаторах также были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: **ciscoenpa55**
- Протокол маршрутизации OSPF с аутентификацией MD5, пароль: **MD5pa55**

Примечание. Линии консоли и линии vty не были предварительно настроены.

Примечание. IOS версии 15.3 использует SCRYPT в качестве алгоритма хеширования для надежного шифрования, но текущая версия IOS, поддерживаемая в Packet Tracer, использует алгоритм MD5. Используйте всегда наиболее надежный вариант, доступный на вашем оборудовании.

Часть 1: Настройка локальной аутентификации AAA для консольного доступа на маршрутизаторе R1

Шаг 1: Проверьте связь.

- Отправьте эхо-запрос с компьютера **PC-A** на компьютер **PC-B**.
- Отправьте эхо-запрос с компьютера **PC-A** на компьютер **PC-C**.
- Отправьте эхо-запрос с компьютера **PC-B** на компьютер **PC-C**.

Шаг 2: Настройте имя локального пользователя на маршрутизаторе R1.

Настройте имя пользователя **Admin1** с секретным паролем **admin1pa55.**

Шаг 3: Настройте локальную аутентификацию AAA для консольного доступа на маршрутизаторе R1.

Включите AAA на маршрутизаторе R1 и настройте аутентификацию AAA так, чтобы для входа в консоль использовалась локальная база данных.

Шаг 4: Настройте консоль для использования определенного метода аутентификации AAA.

Включите AAA на маршрутизаторе R1 и настройте аутентификацию AAA так, чтобы для входа в консоль использовался список методов по умолчанию.

Шаг 5: Проверьте метод аутентификации AAA.

Проверьте вход пользователя в режиме EXEC с помощью локальной базы данных.

Часть 2: Настройка локальной аутентификации AAA для линий VTY на маршрутизаторе R1

Шаг 1: Настройте доменное имя и криптографический ключ для использования с протоколом SSH.

a. Используйте ccnasecurity.com в качестве доменного имени на маршрутизаторе R1.

b. Создайте криптографический ключ RSA из 1024 бит.

Шаг 2: Настройте метод аутентификации AAA с использованием именованного списка для линий VTY на маршрутизаторе R1.

Создайте именованный список **SSH-LOGIN** для аутентификации входа в систему с использованием локального метода AAA.

Шаг 3: Настройте линии VTY для использования определенного метода аутентификации AAA.

Настройте линии VTY для использования именованного метода AAA и разрешения удаленного доступа только по протоколу SSH.

Шаг 4: Проверьте метод аутентификации AAA.

Проверьте конфигурацию SSH для маршрутизатора **R1** из командной строки компьютера **PC-A**.

Часть 3: Настройка серверной аутентификации AAA по протоколу TACACS+ на маршрутизаторе R2

Шаг 1: Настройте резервную запись в локальной базе данных с именем Admin.

Для целей резервирования создайте имя локального пользователя **Admin2** и секретный пароль **admin2pa55**.

Шаг 2: Проверьте конфигурацию сервера TACACS+.

Выберите TACACS+ Server (Сервер TACACS+). На вкладке Services выберите **AAA**. Обратите внимание на наличие записи сетевой конфигурации для маршрутизатора **R2** и записи User Setup (Настройка пользователя) для **Admin2.**

Шаг 3: Настройте параметры сервера TACACS+ на маршрутизаторе R2.

Настройте IP-адрес и секретный ключ сервера TACACS для AAA на маршрутизаторе **R2.**

Примечание. Команды **tacacs-server host** и **tacacs-server key** использовать не рекомендуется. В настоящее время Packet Tracer не поддерживает новую команду **tacacs server.**

```
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
```

Шаг 4: Настройка аутентификации AAA для консольного доступа на маршрутизаторе R2.

Включите AAA на маршрутизаторе **R2** и настройте аутентификацию всех попыток входа в систему с использованием сервера TACACS+ для AAA. Если он недоступен, используйте локальную базу данных.

Шаг 5: Настройте консоль для использования определенного метода аутентификации AAA.

Настройте аутентификацию AAA так, чтобы для входа в консоль использовался метод аутентификации AAA по умолчанию.

Шаг 6: Проверьте метод аутентификации AAA.

Проверьте вход пользователя в режиме EXEC с помощью сервера TACACS+ для AAA.

Часть 4: Настройка серверной аутентификации AAA по протоколу RADIUS на маршрутизаторе R3

Шаг 1: Настройте резервную запись в локальной базе данных с именем Admin.

Для целей резервирования создайте имя локального пользователя **Admin3** и секретный пароль **admin3pa55.**

Шаг 2: Проверьте конфигурацию сервера RADIUS.

Выберите RADIUS Server (Сервер RADIUS). На вкладке Services выберите **AAA**. Обратите внимание на наличие записи сетевой конфигурации для маршрутизатора **R3** и записи User Setup (Настройка пользователя) для **Admin3.**

Шаг 3: Настройте параметры сервера RADIUS на маршрутизаторе R3.

Настройте IP-адрес и секретный ключ сервера RADIUS для AAA на маршрутизаторе **R3.**

Примечание. Команды **radius-server host** и **radius-server** использовать не рекомендуется. В настоящее время Packet Tracer не поддерживает новую команду **radius server**.

```
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55
```

Шаг 4: Настройка аутентификации AAA для консольного доступа на маршрутизаторе R3.

Включите AAA на маршрутизаторе **R3** и настройте аутентификацию всех попыток входа в систему с использованием сервера RADIUS для AAA. Если он недоступен, используйте локальную базу данных.

Шаг 5: Настройте консоль для использования определенного метода аутентификации AAA.

Настройте аутентификацию AAA так, чтобы для входа в консоль использовался метод аутентификации AAA по умолчанию.

Шаг 6: Проверьте метод аутентификации AAA.

Проверьте вход пользователя в режиме EXEC с помощью сервера RADIUS для AAA.

Шаг 7: Проверьте результаты.

Вы полностью выполнили задание. Нажмите **Check Results (Проверить результаты)** для просмотра отзыва и проверки завершенных обязательных компонентов.

