

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № 5**

на тему «Система аутентификации авторизации и учета событий ААА»

Выполнил обучающийся гр. ВКБ42

Михайлов А.С.

Проверил:

Доцент Болдырихин Н.В.

Доцент Сосновский И.А.

Ростов-на-Дону

2024

Лабораторная работа №5

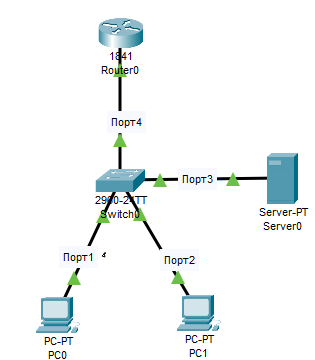


Рисунок 1 – Схема соединения сети

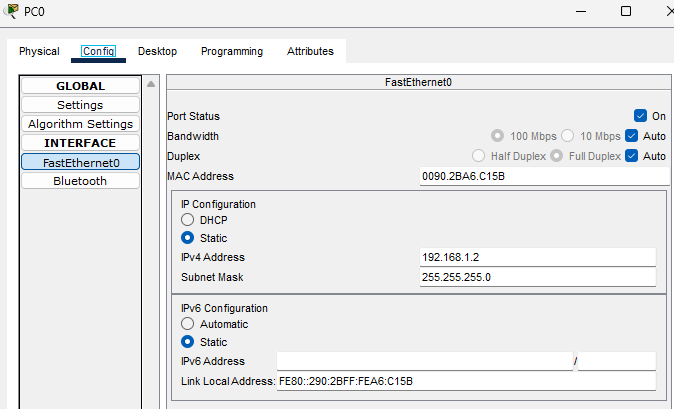


Рисунок 2 – Настройка ПК0

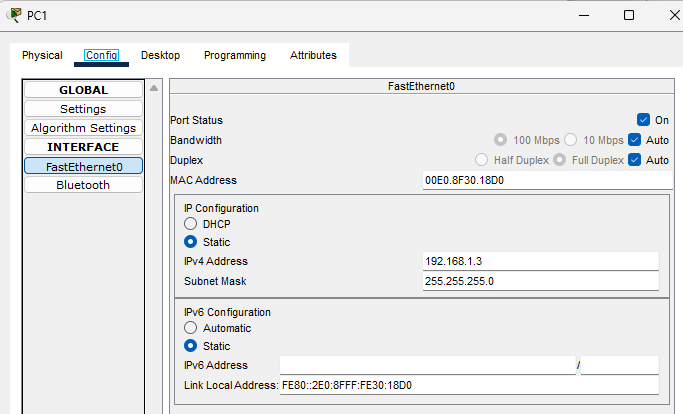


Рисунок 3 – Настройка ПК1

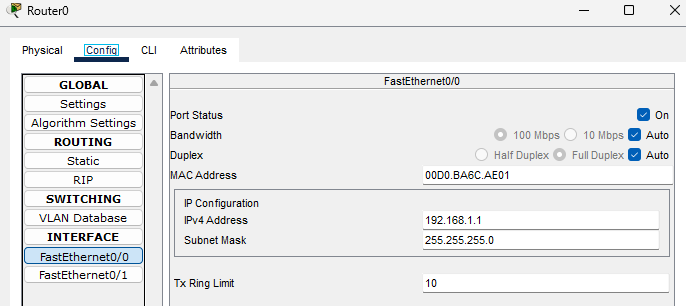


Рисунок 4 – Настройка маршрутизатора

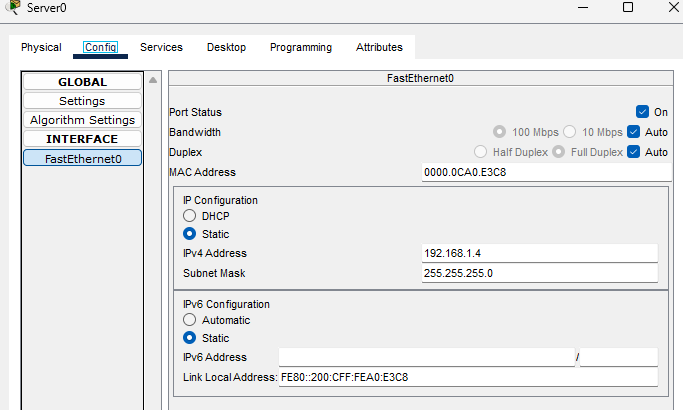


Рисунок 5 – Настройка сервера

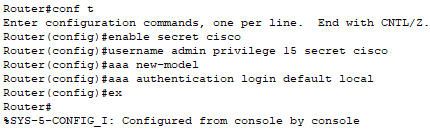


Рисунок 6 – Настройка роутера, Local Database

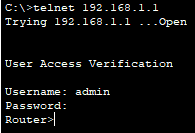


Рисунок 7 – Подключение к роутеру через telnet

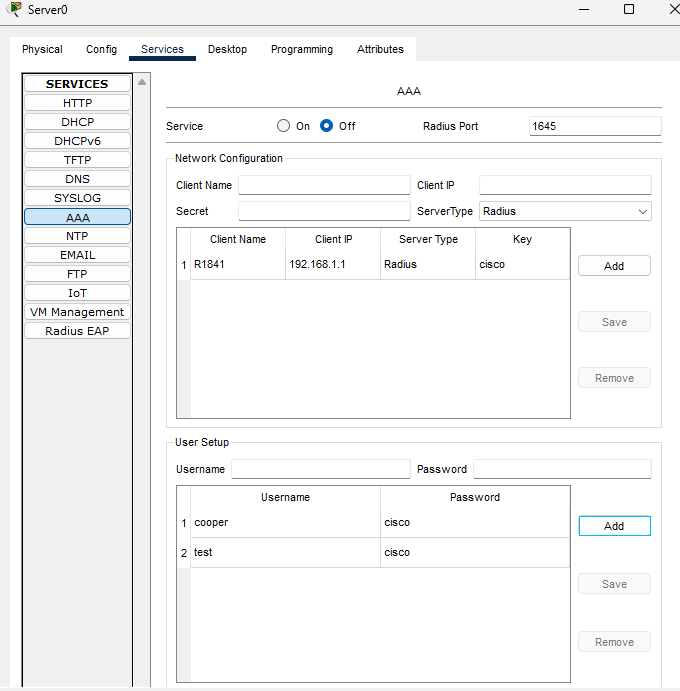
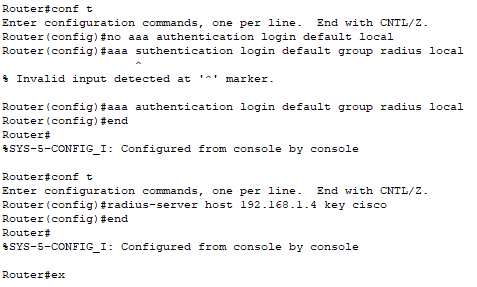


Рисунок 8 – Настройка ААА протокола на отдельном сервере



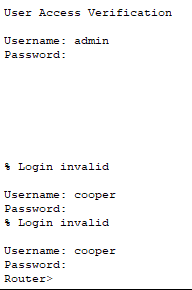


Рисунок 9 – Подключение ААА таблицы к роутеру, а также проверка аутентификации старого пользователя и через подключенный сервер

Вывод: в данной лабораторной работе мы успешно настроили аутентификации через AAA-сервер

1. **AAA-сервер** (Authentication, Authorization, Accounting) — это сервер, который обеспечивает централизованное управление доступом к сетевым ресурсам и устройствам. AAA-сервер выполняет три основные функции:

* **Аутентификация (Authentication)**: Проверка подлинности пользователя или устройства, пытающегося получить доступ к сетевым ресурсам. Это включает в себя проверку учетных данных (например, логина и пароля) для подтверждения личности.
* **Авторизация (Authorization)**: Определение прав доступа пользователя или устройства после успешной аутентификации. Авторизация определяет, какие ресурсы и действия доступны пользователю или устройству.
* **Учет (Accounting)**: Сбор и запись информации о действиях пользователя или устройства, таких как время доступа, использованные ресурсы и выполненные команды. Эта информация используется для мониторинга, аудита и биллинга.

2. **Аутентификация** — это процесс проверки подлинности личности пользователя или устройства, пытающегося получить доступ к системе или ресурсу. Цель аутентификации — убедиться, что пользователь или устройство действительно являются теми, за кого себя выдают.

**Основные методы аутентификации:**

1. **Пароль**: Пользователь предоставляет секретный пароль, который соответствует заранее заданному.
2. **Биометрия**: Использование уникальных физических характеристик, таких как отпечатки пальцев, распознавание лица или сетчатки глаза.
3. **Токены**: Устройства, генерирующие одноразовые пароли или коды, которые пользователь должен ввести для аутентификации.
4. **Многофакторная аутентификация (MFA)**: Комбинация нескольких методов аутентификации, например, пароль + SMS-код.
5. **Сертификаты**: Использование цифровых сертификатов, подтверждающих подлинность пользователя или устройства.

**Авторизация (Authorization)**

**Авторизация** — это процесс определения прав доступа пользователя или устройства к определенным ресурсам или действиям после успешной аутентификации. Авторизация определяет, какие действия и ресурсы доступны пользователю или устройству.

**Основные аспекты авторизации:**

1. **Роли**: Пользователи могут быть сгруппированы в роли (например, администратор, пользователь), каждая из которых имеет определенные права доступа.
2. **Политики доступа**: Определяют, какие ресурсы и действия доступны для каждой роли или пользователя.
3. **Разрешения**: Явное предоставление или ограничение прав доступа к определенным ресурсам или функциям.
4. **Контроль доступа на основе атрибутов (ABAC)**: Авторизация основана на атрибутах пользователя, ресурса и контекста доступа.

3. Telnet (Телетайп-сеть) в системе Cisco и других сетевых устройствах — это протокол удаленного доступа, который позволяет администраторам управлять сетевыми устройствами через сеть. Он используется для удаленного подключения к устройству и выполнения команд, настройки и мониторинга.

4. В контексте AAA (Authentication, Authorization, Accounting), аутентификация — это первый этап, на котором проверяется подлинность пользователя или устройства, пытающегося получить доступ к сетевым ресурсам. Существует несколько методов аутентификации, которые могут использоваться в AAA-системах. Вот основные из них:

### 1. ****Парольная аутентификация (Password Authentication)****

* **Описание**: Пользователь предоставляет секретный пароль, который соответствует заранее заданному.
* **Пример**: Ввод логина и пароля при входе в систему.

### 2. ****Биометрическая аутентификация (Biometric Authentication)****

* **Описание**: Использование уникальных физических характеристик, таких как отпечатки пальцев, распознавание лица или сетчатки глаза.
* **Пример**: Считывание отпечатка пальца для доступа к устройству.

### 3. ****Аутентификация с использованием токенов (Token-Based Authentication)****

* **Описание**: Устройства, генерирующие одноразовые пароли или коды, которые пользователь должен ввести для аутентификации.
* **Пример**: Использование аппаратного или программного токена для генерации OTP (одноразового пароля).

### 4. ****Многофакторная аутентификация (Multi-Factor Authentication, MFA)****

* **Описание**: Комбинация нескольких методов аутентификации, например, пароль + SMS-код.
* **Пример**: Ввод пароля и получение SMS-кода на мобильный телефон для дополнительной проверки.

### 5. ****Аутентификация на основе сертификатов (Certificate-Based Authentication)****

* **Описание**: Использование цифровых сертификатов, подтверждающих подлинность пользователя или устройства.
* **Пример**: Использование сертификата клиента для аутентификации в VPN.

### 6. ****Аутентификация на основе Kerberos (Kerberos Authentication)****

* **Описание**: Протокол аутентификации, который использует билеты для проверки подлинности пользователя.
* **Пример**: Использование Kerberos для аутентификации в среде Windows Active Directory.

### 7. ****Аутентификация на основе RADIUS (RADIUS Authentication)****

* **Описание**: Использование протокола RADIUS для централизованной аутентификации пользователей.
* **Пример**: Аутентификация пользователей, подключающихся к беспроводной сети через RADIUS-сервер.

### 8. ****Аутентификация на основе TACACS+ (TACACS+ Authentication)****

* **Описание**: Использование протокола TACACS+ для централизованной аутентификации пользователей на сетевых устройствах.
* **Пример**: Аутентификация администраторов, подключающихся к маршрутизаторам и коммутаторам Cisco.

### 9. ****Аутентификация на основе LDAP (LDAP Authentication)****

* **Описание**: Использование протокола LDAP для аутентификации пользователей на основе данных в каталоге.
* **Пример**: Аутентификация пользователей в веб-приложении с использованием LDAP-сервера.

### 10. ****Аутентификация на основе OAuth (OAuth Authentication)****

* **Описание**: Использование протокола OAuth для делегирования доступа к ресурсам без передачи учетных данных.
* **Пример**: Вход в веб-приложение через учетную запись Google или Facebook.