**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №2**

*дисциплина: Администрирование локальных сетей*

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

**МОСКВА**

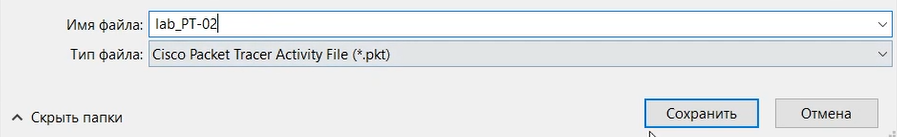
2024 г.

# Цель работы:

# Получить основные навыки по начальному конфигурированию оборудования Cisco.

**Выполнение работы:**

Создадим новый проект с названием lab\_PT-02.pkt (Рис. 1.1):

****

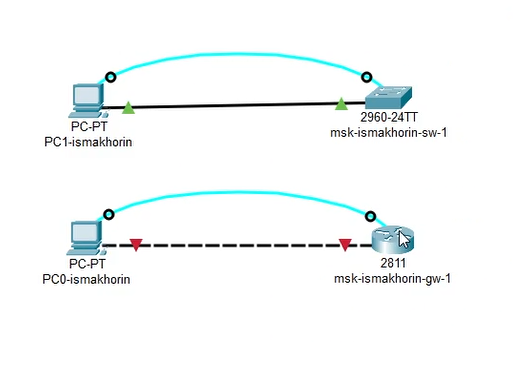
**Рис. 1.1.** Создание нового проекта.

В логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соединим один PC с маршрутизатором, другой PC — с коммутатором (Рис. 1.2). После чего, щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса (Рис. 1.3):

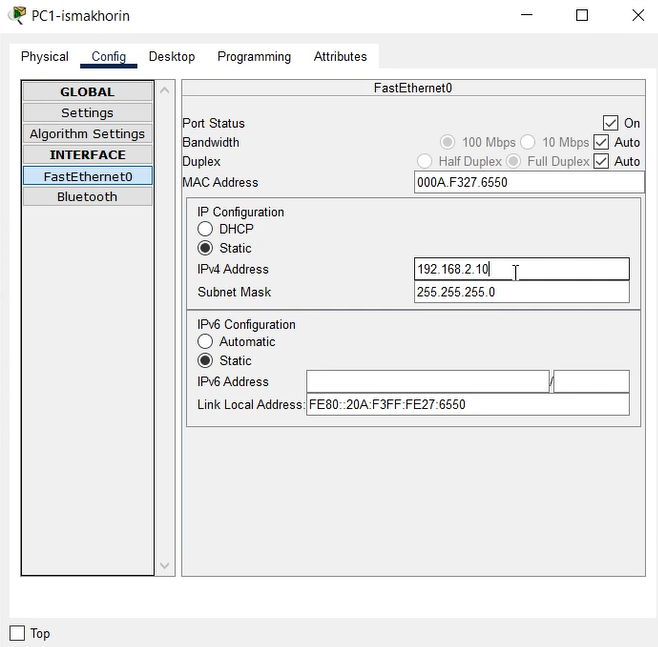
192.168.1.10

192.168.2.10

с маской подсети 255.255.255.0

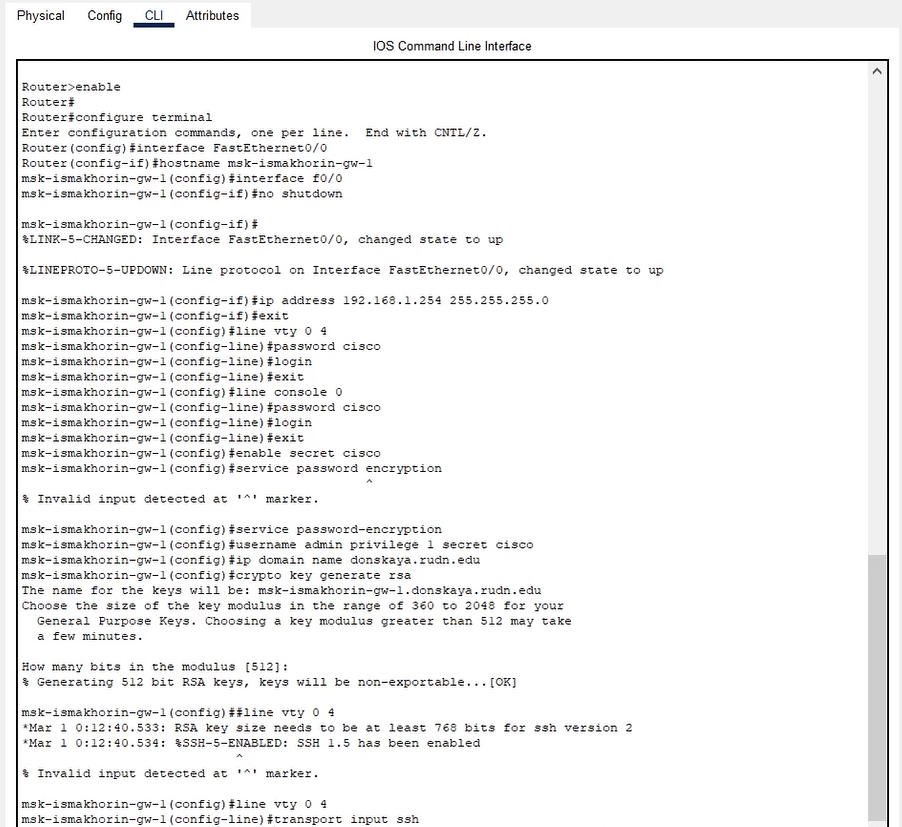
****

**Рис. 1.2.** Размещение коммутатора, маршрутизатора и двух оконечных устройств. Последующие соединение.

****

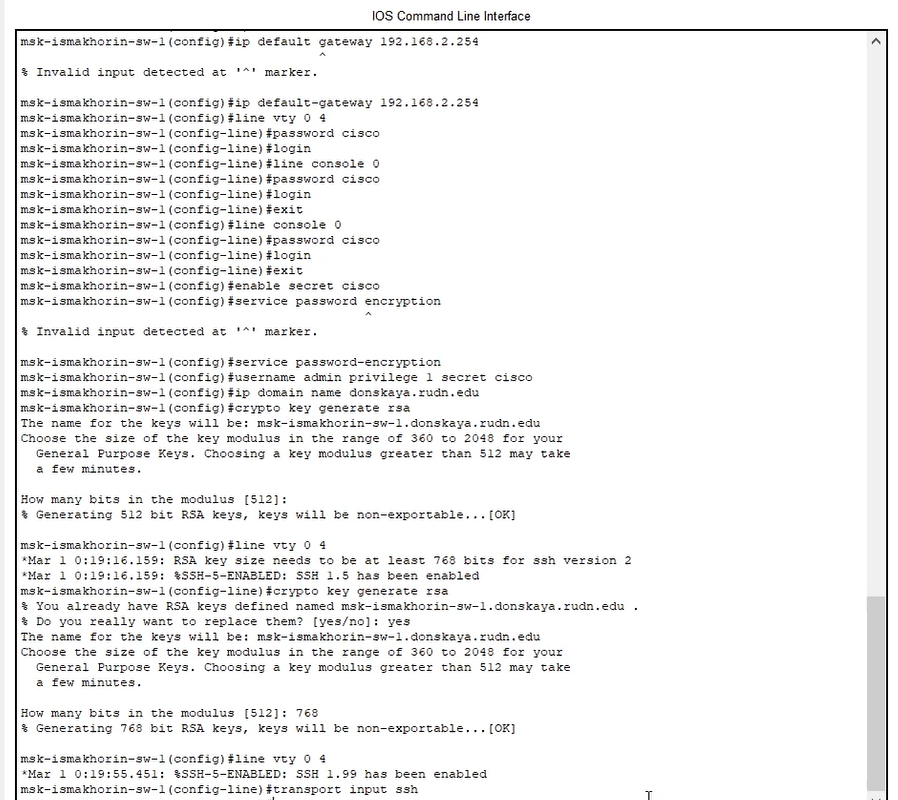
**Рис. 1.3.** Присвоение статического IP-адреса и маски подсети.

Проведём настройку маршрутизатора в соответствии с заданием (Рис. 1.4):

****

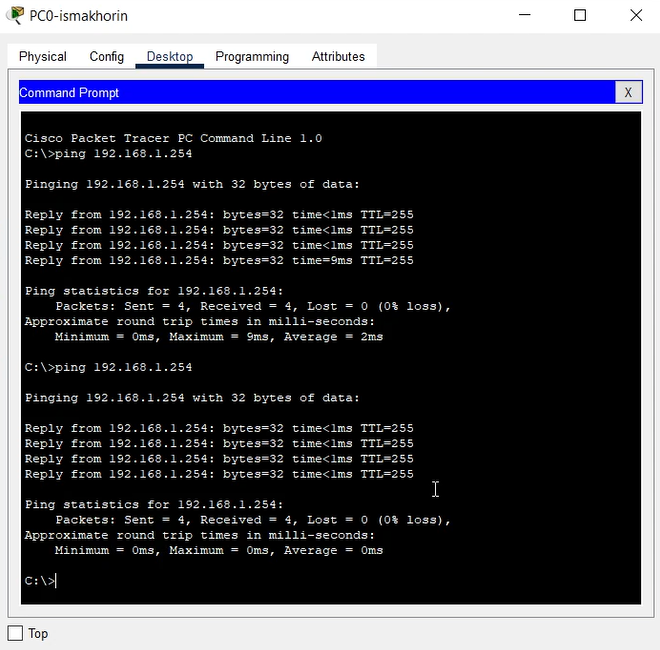
**Рис. 1.4.** Проведение настройки маршрутизатора.

Теперь проведём настройку коммутатора в соответствии с заданием (Рис. 1.5):

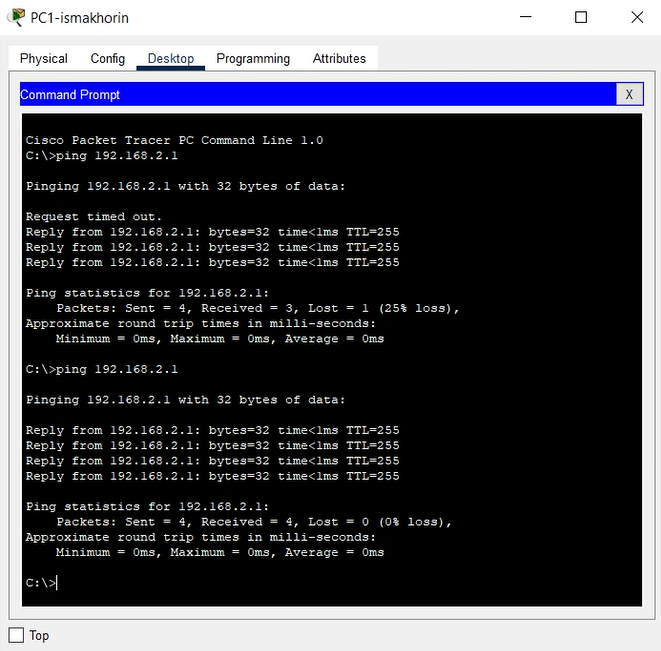
****

**Рис. 1.5.** Проведение настройки коммутатора.

Далее проверим работоспособность соединений с помощью команды ping (Рис. 1.6 – 1.7).

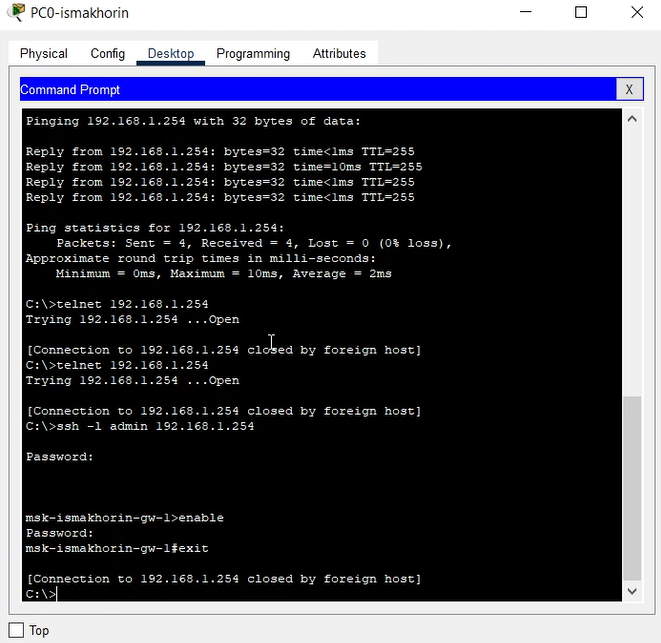
****

**Рис. 1.6.** Проверка работоспособности соединения PC0-ismakhorin -> msk-ismakhorin-gw-1.

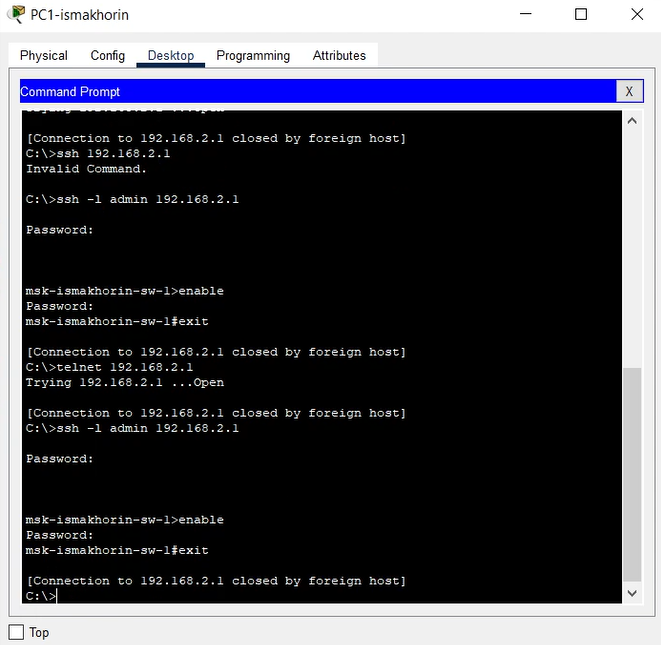
****

**Рис. 1.7.** Проверка работоспособности соединения PC1-ismakhorin -> msk-ismakhorin-sw-1.

Попробуем подключиться к коммутатору и маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh) (Рис. 1.8 – 1.9):

****

**Рис. 1.8.** Попытка подключения к маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

****

**Рис. 1.9.** Попытка подключения к коммутатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

**Вывод:**

# В ходе выполнения лабораторной работы были получены основные навыки по начальному конфигурированию оборудования Cisco.

**Ответы на контрольные вопросы:**

1. Укажите возможные способы подключения к сетевому оборудованию. - **Проводное подключение (Ethernet): наиболее распространенный метод подключения, который использует сетевой кабель (обычно категории Ethernet) для соединения компьютера, маршрутизатора, коммутатора или другого сетевого устройства.**

**Беспроводное подключение (Wi-Fi): используют радиоволновые соединения для передачи данных между устройствами. Wi-Fi обычно используется для подключения мобильных устройств, но также может использоваться для подключения компьютеров и другого сетевого оборудования.**

1. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему? - **Для подключения оконечного оборудования пользователя к маршрутизатору обычно используется кабель Ethernet. Существует несколько видов Ethernet-кабелей, но наиболее распространенным и рекомендуемым для этой цели является кабель категории 5e (Cat5e) или категории 6 (Cat6).**

**Кабели Cat5e и Cat6 имеют несколько преимуществ, делающих их предпочтительными для подключения оконечного оборудования к маршрутизатору:**

* **Скорость и пропускная способность.**
* **Поддержка Gigabit Ethernet.**
* **Устойчивость к помехам.**
* **Будущая совместимость.**

1. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему? - **Для подключения оконечного оборудования пользователя к коммутатору также рекомендуется использовать кабель Ethernet. В зависимости от требований сети и возможностей коммутатора, можно использовать кабели различных категорий, но обычно предпочтительными являются кабели категории 5e (Cat5e) или категории 6 (Cat6) по тем же причинам, что и при подключении к маршрутизатору:**

* **Скорость и пропускная способность.**
* **Поддержка Gigabit Ethernet.**
* **Устойчивость к помехам.**
* **Будущая совместимость.**

1. Каким типом сетевого кабеля следует подключать коммутатор к коммутатору и почему? - **Для подключения коммутатора к коммутатору также используются сетевые кабели Ethernet. Однако здесь обычно используются кабели определенной категории в зависимости от требований к сети и пропускной способности, а также от расстояния между коммутаторами. Наиболее распространенными кабелями для соединения коммутаторов являются кабели категории 5e (Cat5e), категории 6 (Cat6) и категории 6a (Cat6a).**

**Выбор кабеля зависит от нескольких факторов:**

* **Пропускная способность и расстояние.**
* **Будущие потребности.**
* **Бюджет.**
* **Совместимость с имеющейся инфраструктурой.**

**Таким образом, для подключения коммутатора к коммутатору наиболее подходящими кабелями являются Cat5e, Cat6 или Cat6a, в зависимости от требований к пропускной способности, расстоянию и бюджету.**

1. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю. –

* **Пароли на уровне устройства.**
* **AAA (Authentication, Authorization, Accounting.**
* **SSH (Secure Shell) или Telnet: SSH и Telnet - это протоколы удаленного управления, которые позволяют администраторам подключаться к сетевому оборудованию через сеть и вводить команды для настройки и управления устройством. Часто они могут быть защищены паролем для обеспечения безопасного доступа.**
* **Web-based интерфейс управления.**
* **Локальные аккаунты.**
* **Протокол SNMP (Simple Network Management Protocol).**
* **Все эти методы позволяют администраторам обеспечить безопасный доступ к сетевому оборудованию по паролю, минимизируя риски несанкционированного доступа и обеспечивая конфиденциальность и целостность сетевых данных.**

1. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему? –

* **SSH (Secure Shell): SSH предоставляет защищенное соединение с удаленным сетевым оборудованием через шифрование данных. Этот метод обеспечивает безопасность и конфиденциальность при передаче команд и данных по сети.**
* **Telnet: Telnet также предоставляет удаленный доступ к сетевому оборудованию, но не обеспечивает защиту данных, так как информация передается в открытом виде. Использование Telnet не рекомендуется из-за небезопасности этого протокола.**
* **VPN (Virtual Private Network): VPN создает защищенное соединение через общую сеть, такую как интернет, что позволяет удаленным пользователям безопасно подключаться к сетевому оборудованию, как если бы они были внутри локальной сети.**
* **SSL VPN (Secure Socket Layer Virtual Private Network): SSL VPN предоставляет удаленным пользователям защищенный доступ к сетевому оборудованию через веб-браузер, используя SSL-шифрование для защиты данных.**
* **Модемный доступ: Многие сетевые устройства могут быть настроены для доступа через модемы, обеспечивая резервное подключение в случае проблем с основной сетью.**
* **Удаленное управление через веб-интерфейс: Некоторые сетевые устройства предоставляют веб-интерфейс для удаленного управления, который позволяет администраторам настроить и управлять устройством через веб-браузер.**

**Предпочтительным методом для настройки удаленного доступа к сетевому оборудованию является использование SSH или VPN. Оба эти метода обеспечивают защищенное соединение и шифрование данных, что обеспечивает конфиденциальность и безопасность при удаленном доступе. SSH особенно удобен для доступа к командной строке устройства, в то время как VPN обеспечивает более универсальный и общий доступ к сети. Таким образом, использование SSH или VPN является предпочтительным для обеспечения безопасного удаленного доступа к сетевому оборудованию.**