

# **Отчёт по лабораторной работе №2**

**Дисциплина: Администрирование локальных сетей**

Исаев Булат Абубакарович НПИбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Вывод</b>	<b>15</b>
3.1	Контрольные вопросы . . . . .	15

# Список иллюстраций

2.1	Создание нового проекта. . . . .	6
2.2	AAAAAAAAAAAAРазмещение коммутатора, маршрутизатора и двух оконечных устройств. Последующие соединения.AAAAAAAAAA .	7
2.3	Присвоение статического IP-адреса и маски подсети. . . . .	8
2.4	Проведение настройки маршрутизатора. . . . .	9
2.5	Проведение настройки коммутатора. . . . .	10
2.6	Проверка работоспособности соединения PC0-baisaev -> msk-baisaev-gw-1. . . . .	11
2.7	Проверка работоспособности соединения PC1-baisaev -> msk-baisaev-sw-1. . . . .	12
2.8	Попытка подключения к маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh). . . . .	13
2.9	Попытка подключения к коммутатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh). . . . .	14

## Список таблиц

# 1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

## 2 Выполнение лабораторной работы

Создадим новый проект с названием lab\_PT-02.pkt (рис. 2.1)

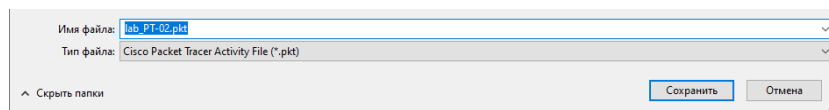


Рис. 2.1: Создание нового проекта.

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. 2.2). После чего, щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса (рис. 2.3) 192.168.1.10 192.168.2.10 с маской подсети 255.255.255.0

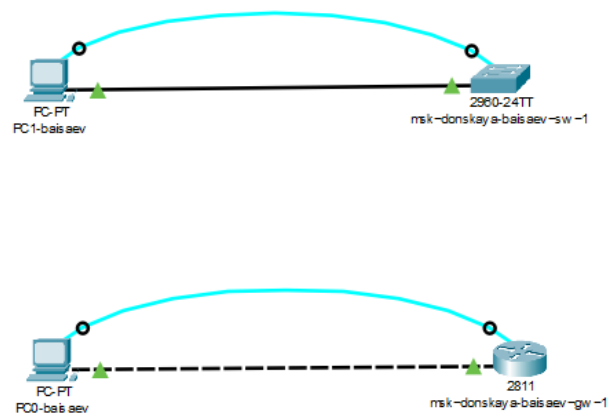


Рис. 2.2: АAAAAAAAAAAAAРазмещение коммутатора, маршрутизатора и двух оконечных устройств. Последующие соединения.AAAAAAAAAAAAA

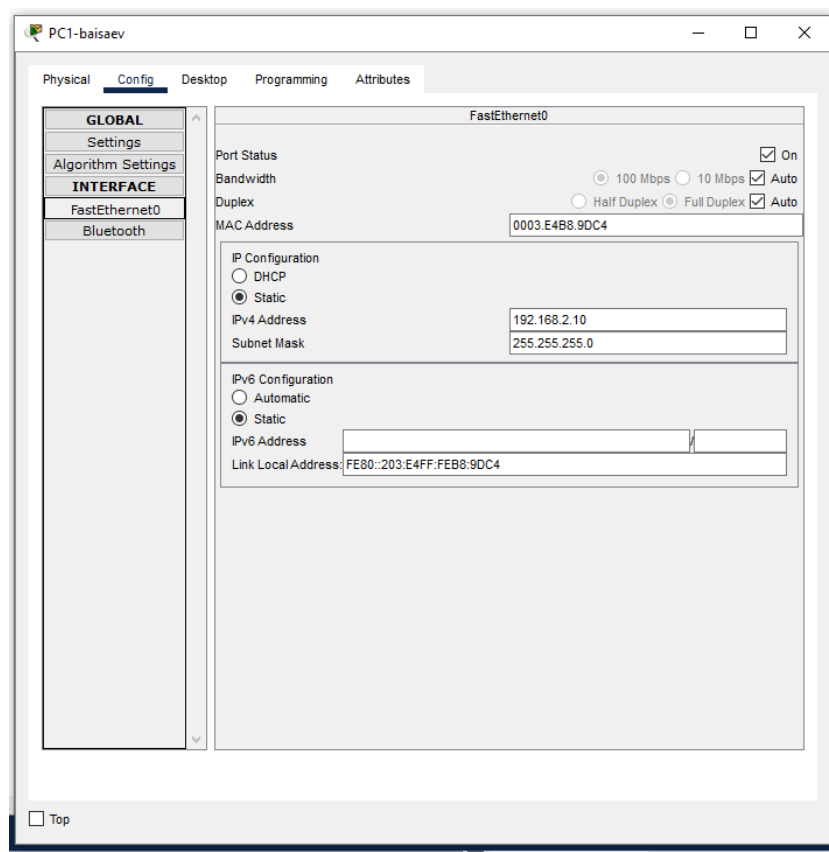


Рис. 2.3: Присвоение статического IP-адреса и маски подсети.

Проведём настройку маршрутизатора в соответствии с заданием (рис. 2.4)





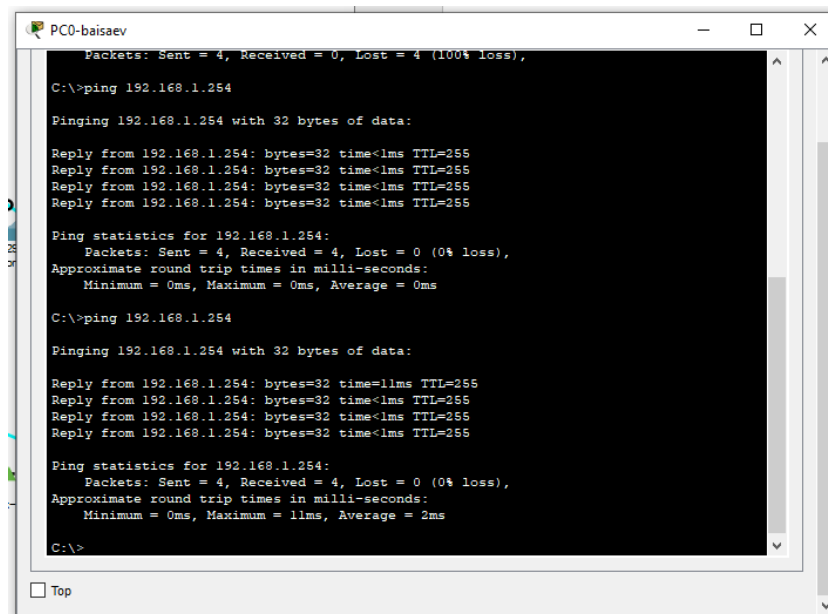
Рис. 2.4: Проведение настройки маршрутизатора.

Теперь проведём настройку коммутатора в соответствии с заданием (рис. 2.5)



Рис. 2.5: Проведение настройки коммутатора.

Далее проверим работоспособность соединений с помощью команды ping (рис. 2.6), (рис. 2.7)



```
PC0-baisaev
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=11ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>
```

Рис. 2.6: Проверка работоспособности соединения PC0-baisaev -> msk-baisaev-gw-1.

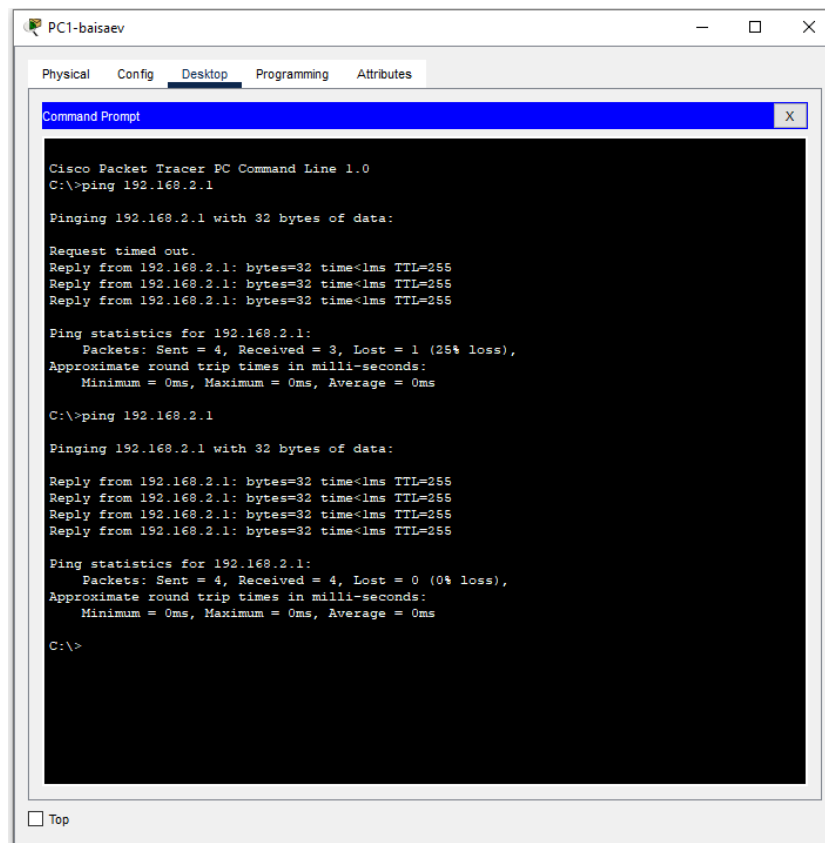


Рис. 2.7: Проверка работоспособности соединения PC1-baisaev -> msk-baisaev-sw-1.

Попробуем подключиться к коммутатору и маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh) (рис. 2.8), (рис. 2.9)

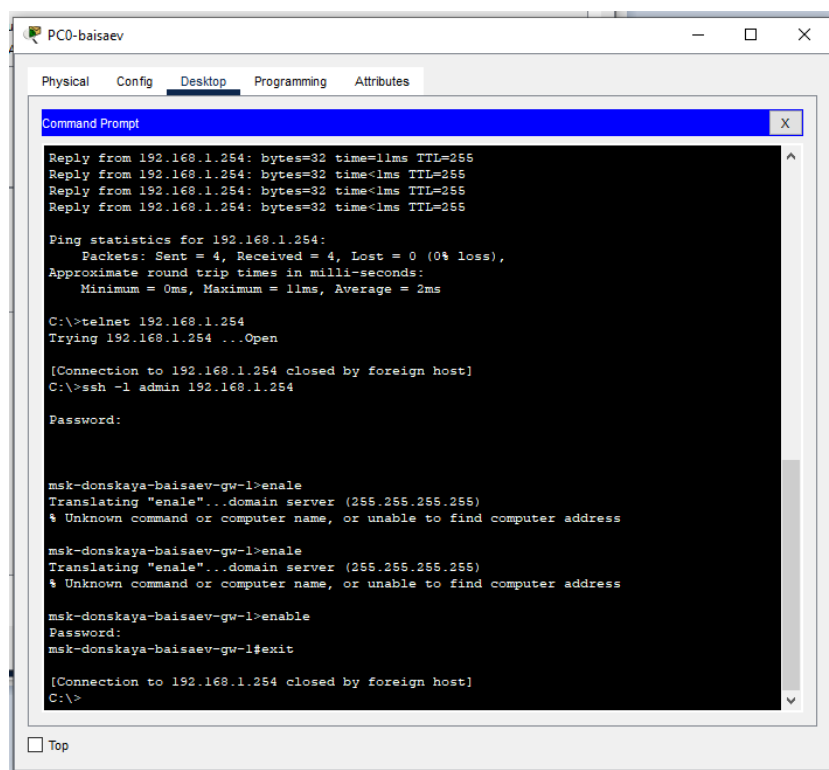


Рис. 2.8: Попытка подключения к маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

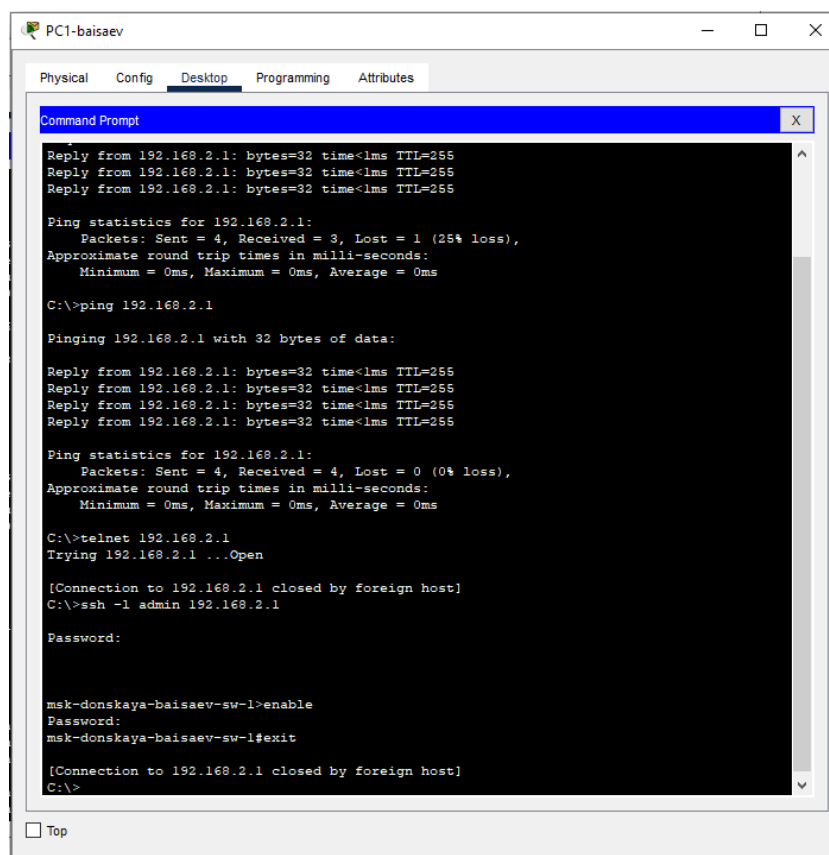


Рис. 2.9: Попытка подключения к коммутатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

## 3 Вывод

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

### 3.1 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.

2. 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 5е (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.**

3. 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 5е (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.**

4. 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 5е (Cat5e), категории 6 (Cat6) и категории 6а (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.**

5. 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.

6. 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.