


**Министерство науки и высшего образования Российской Федерации**  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«Владимирский государственный университет**  
**имени Александра Григорьевича и Николая Григорьевича Столетовых»**  
**(ВлГУ)**

УТВЕРЖДАЮ  
Заведующий кафедрой ИСПИ

  
И.Е. Жигалов  
«20» марта 2025 г.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
**К ЛАБОРАТОРНЫМ РАБОТАМ**  
**УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ**

«КОМПЬЮТЕРНЫЕ СЕТИ»

09.02.09 Веб-разработка  
Разработчик веб приложений

**Владимир, 2025**

Методические указания к лабораторным работам учебной дисциплины профессиональной подготовки «Компьютерные сети» разработали: преподаватель КИТП Ларин Е.С., преподаватель КИТП Нестеров Н.А.

Методические указания к лабораторным работам рассмотрены и одобрены на заседании УМК специальности 09.02.09 Веб-разработка протокол № 1 от «10» марта 2025 г.

Председатель УМК специальности  И.Е. Жигалов

Методические указания к лабораторным работам рассмотрены и одобрены на заседании кафедры ИСПИ протокол № 7а от «12» марта 2025 г.

<b>Оглавление</b>	
<b>Лабораторная работа № 1</b> .....	<b>3</b>
<b>Лабораторная работа № 2</b> .....	<b>21</b>
<b>Лабораторная работа №3</b> .....	<b>25</b>
<b>Лабораторная работа № 4</b> .....	<b>33</b>
<b>Лабораторная работа № 5</b> .....	<b>40</b>
<b>Лабораторная работа №6</b> .....	<b>47</b>
<b>Лабораторная работа №7</b> .....	<b>50</b>
<b>Лабораторная работа №8</b> .....	<b>56</b>
<b>СПИСОК ЛИТЕРАТУРЫ</b> .....	<b>61</b>

## Лабораторная работа № 1 НАЧАЛЬНАЯ КОНФИГУРАЦИЯ КОММУТАТОРА CISCO

**Цель работы:** Проверка конфигурации коммутатора по умолчанию. Настройка базовых параметров коммутатора. Настройка баннера MOTD. Сохранение файлов конфигурации в NVRAM. Настройка коммутатора S2.

**Используемые средства и оборудование:** IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

### Исходные данные.

В этом задании нам необходимо настроить основные параметры коммутатора. Необходимо обеспечить безопасность доступа к интерфейсу командной строки (CLI) и портам консоли с помощью зашифрованных и текстовых паролей. Изучить способы конфигурации сообщений, которые будут адресованы пользователям, выполняющим вход в систему коммутатора. Эти баннерные сообщения также предупреждают пользователей о том, что несанкционированный доступ запрещён.

### 1. КРАТКАЯ ТЕОРИЯ

Сетевой коммутатор (жарг. свитч, свич от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI).

В отличие от концентратора (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Принцип работы коммутатора. Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется.

Стоит отметить малую латентность (задержку) и высокую скорость пересылки на каждом порту интерфейса.

Режимы коммутации. Существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.

- С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.
- Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.
- Бесфрагментный (fragment-free) или гибридный. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).

Задержка, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него, и вместе с ним определяет общую задержку коммутатора.

Буфер памяти. Для временного хранения фреймов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные. Буфер памяти может использовать два метода хранения и отправки фреймов: буферизация по портам и буферизация с общей памятью. При буферизации по портам пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передаётся на выходной порт только тогда, когда все фреймы, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один фрейм задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные фреймы могут быть переданы на открытые порты их пунктов назначения.

При буферизации в общей памяти все фреймы хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого фреймы, находившиеся в буфере, динамически распределяются по выходным портам. Это позволяет получить фрейм на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить фреймы. Очистка этой карты происходит только после того, как фрейм успешно отправлен.

Поскольку память буфера является общей, размер фрейма ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные фреймы могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, то есть, когда порт с шириной полосы пропускания 100 Мб/с должен отправлять пакеты на порт 10 Мб/с.

Возможности и разновидности коммутаторов. Коммутаторы подразделяются на управляемые и неуправляемые (наиболее простые).

Более сложные коммутаторы позволяют управлять коммутацией на сетевом (третьем) уровне модели OSI. Обычно их именуют соответственно, например, «Layer 3 Switch» или

сокращенно «L3 Switch». Управление коммутатором может осуществляться посредством Web-интерфейса, интерфейса командной строки (CLI), протокола SNMP, RMON и т. п. Многие управляемые коммутаторы позволяют настраивать дополнительные функции: VLAN, QoS, агрегирование, зеркалирование.

Многие коммутаторы уровня доступа обладают такими расширенными возможностями, как сегментация трафика между портами, контроль трафика на предмет штормов, обнаружение петель, ограничение количества изучаемых mac адресов, ограничение входящей/исходящей скорости на портах, функции списков доступа и т.п.

Сложные коммутаторы можно объединять в одно логическое устройство — стек — с целью увеличения числа портов. Например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с 90  $((4*24)-6=90)$  портами либо с 96 портами (если для стекирования используются специальные порты).

## 2.ХОД РАБОТЫ

### 2.1. ПРОВЕРКА КОНФИГУРАЦИИ КОММУТАТОРА ПО УМОЛЧАНИЮ

#### Шаг 1: Вход в привилегированный режим.

В привилегированном режиме доступны все команды коммутатора. Но в связи с тем, что многими из привилегированных команд задаются рабочие параметры, привилегированный доступ должен быть защищён паролем во избежание несанкционированного использования.

Для выполнения лабораторной работы создаем топологию, представленную на рис. 1.1.

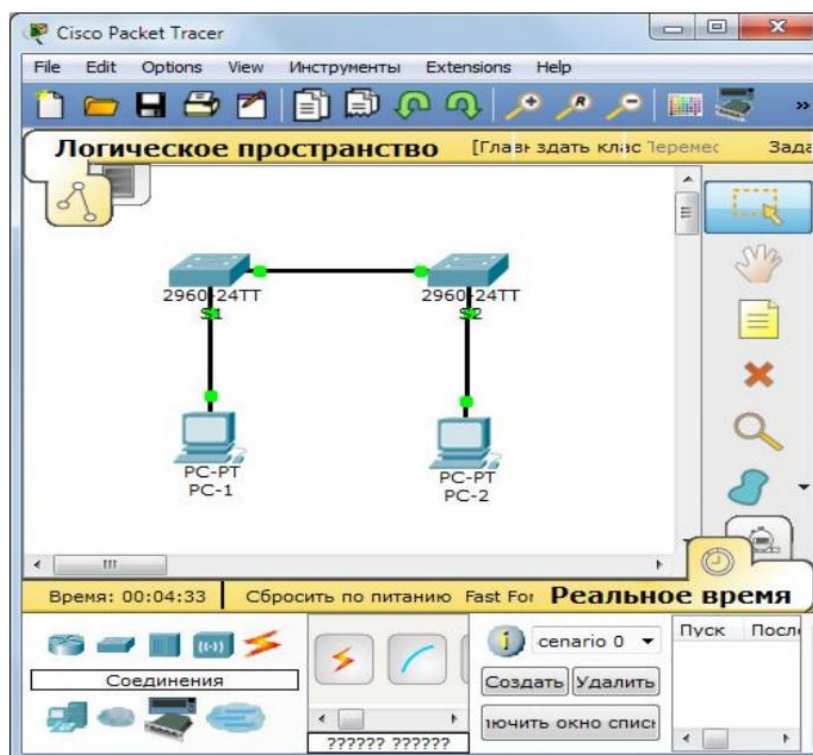


Рис. 1.1. Топология

К привилегированному набору команд относятся те, которые содержатся в пользовательском режиме, а также команда `configure`, при помощи которой выполняется доступ к остальным командным режимам.

- a. Щёлкаем S1 и открываем вкладку CLI. Нажимаем клавишу ВВОД.
- b. Переходим в привилегированный режим, выполнив команду enable (рис. 1.2).

Switch> enable

Switch#

Обращаем внимание на то, что изменённая в конфигурации строка будет отражать привилегированный режим.

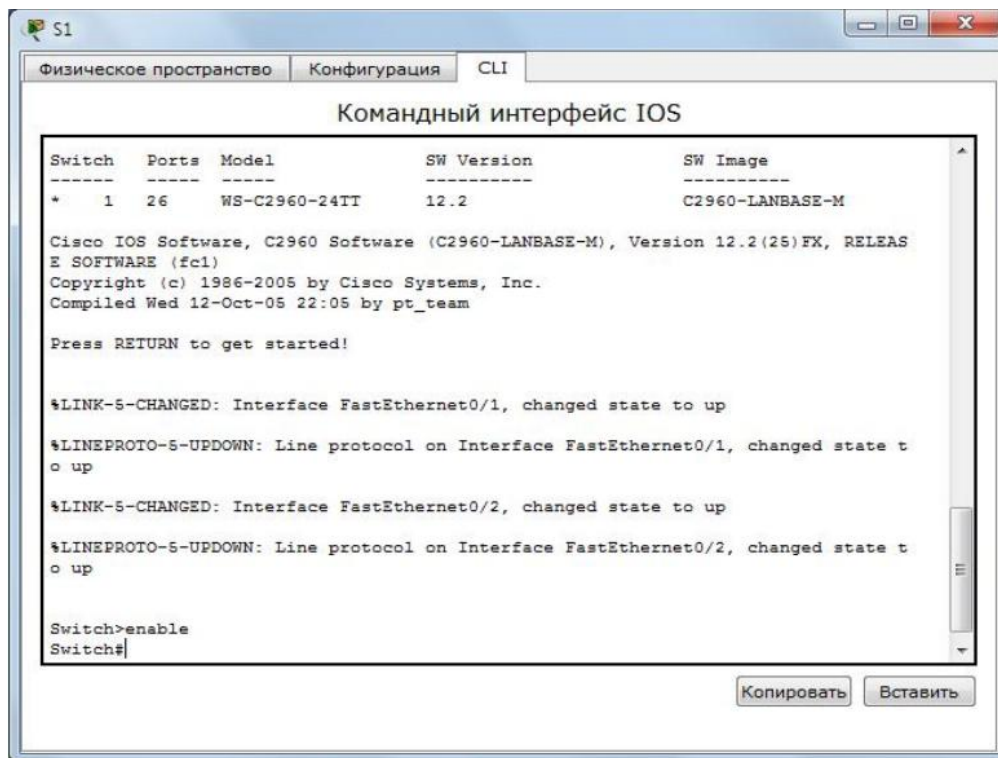


Рис. 1.2. Вход в привилегированный режим

## Шаг 2: Просматриваем текущую конфигурацию коммутатора.

- a. Выполняем команду show running-config (рис. 1.3).

Switch# show running-config

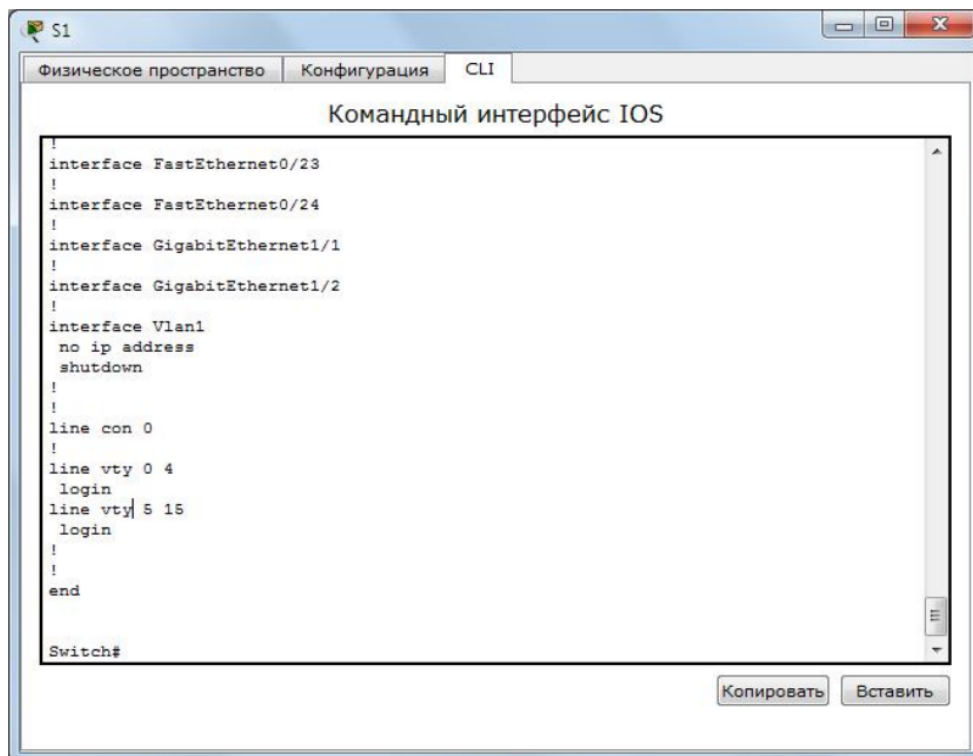


Рис. 1.3. Команда show running-config

б. Ответьте на следующие вопросы.

Сколько у маршрутизатора интерфейсов FastEthernet? 24

Сколько у маршрутизатора интерфейсов Gigabit Ethernet? 2

Каков диапазон значений, отображаемых в vty-линиях? 0-4, 5-15

Какая команда отображает текущее содержимое NVRAM? Switch# show startup-config  
startup-config is not present

Почему коммутатор отвечает сообщением startup-config is not present? Потому что файл конфигурации не сохранён в памяти

## 2.2. СОЗДАНИЕ БАЗОВОЙ КОНФИГУРАЦИИ КОММУТАТОРА

### Шаг 1: Назначение коммутатору имени.

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки. Обращаем внимание на то, как изменяется строка приглашения при переходе по разделам коммутатора (рис.1.4).

```
Switch# configure terminal
```

```
Switch(config)# hostname S1
```

```
S1(config)# exit
```

```
S1#
```



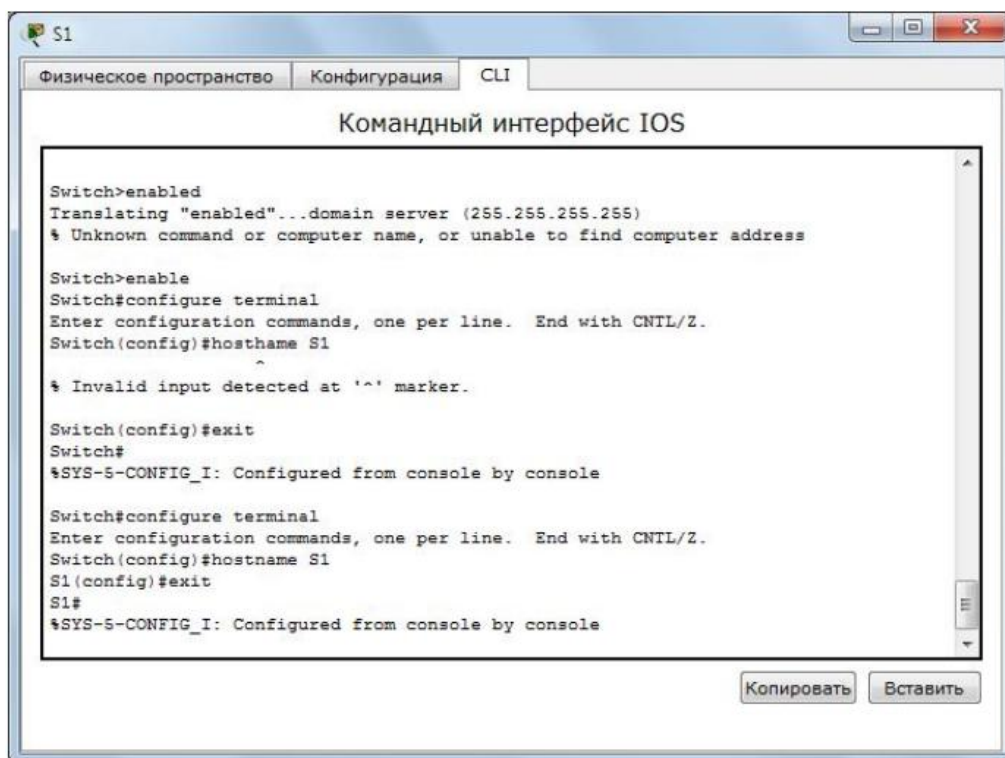


Рис. 1.4. Назначение коммутатору имени

## Шаг 2: Безопасный доступ к консоли.

Для обеспечения безопасного доступа к консоли переходим в режим config-line и устанавливаем для консоли пароль letmein (рис. 1.5).

```
S1# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S1(config)# line console 0
```

```
S1(config-line)# password letmein
```

```
S1(config-line)# login
```

```
S1(config-line)# exit
```

```
S1(config)# exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#
```

Для чего нужна команда login?

Чтобы при входе в консоль можно было установить запрос пароля и логина.

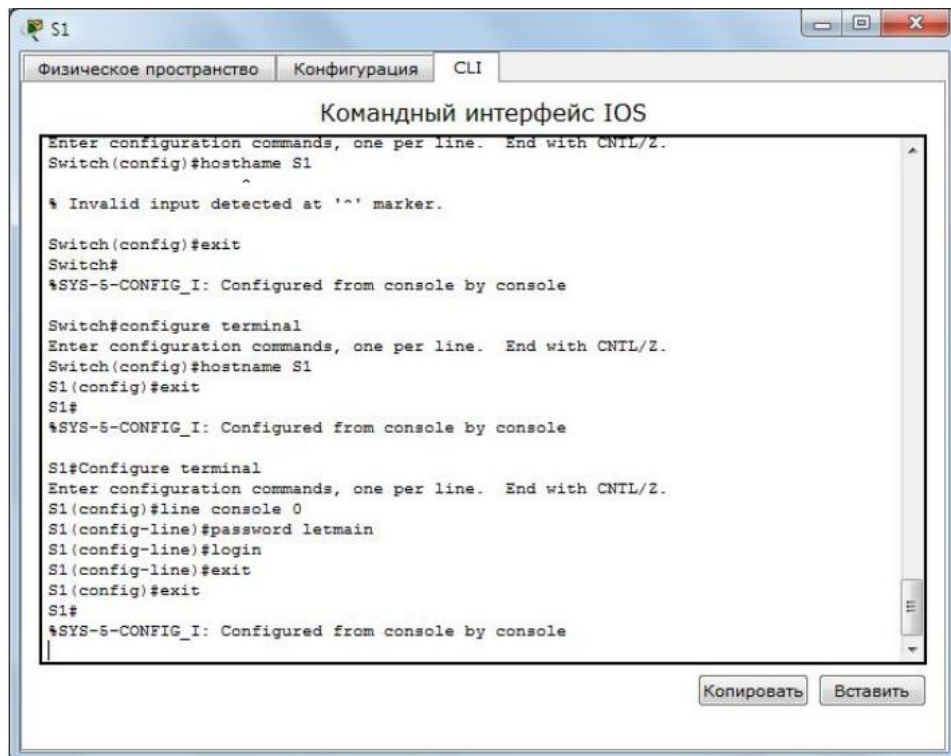


Рис. 1.5. Безопасный доступ к консоли

### Шаг 3: Убедимся, что доступ к консоли защищён паролем.

Выходим из привилегированного режима, чтобы убедиться, что для консольного порта установлен пароль (рис. 1.6).

```
S1# exit
```

```
Switch con0 is now available
```

```
Press RETURN to get started.
```

```
User Access Verification
```

```
Password:
```

```
S1>
```

Примечание. Если коммутатор не выводит запрос на ввод пароля, значит, вы не настроили параметр login в шаге 2.

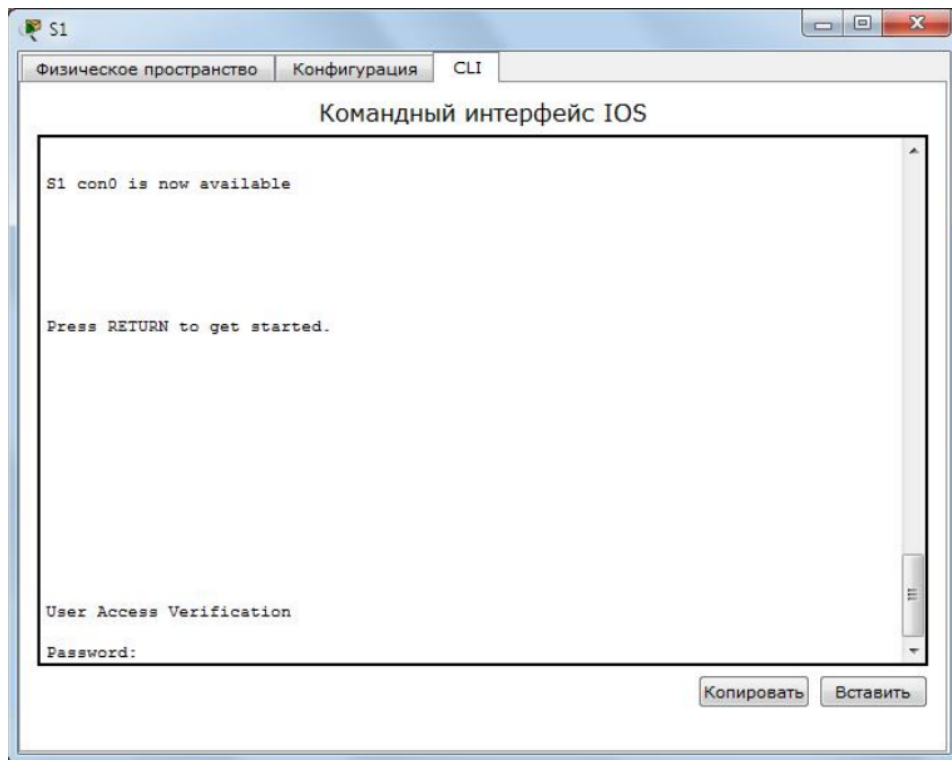


Рис. 1.6. Проверка доступа к консоли

#### **Шаг 4: Безопасный доступ в привилегированном режиме.**

Устанавливаем для enable пароль c1\$c0. Этот пароль ограничивает доступ к привилегированному режиму (рис. 1.7).

Примечание. Символ 0 в c1\$c0 – это цифра ноль, а не буква «О». Этот пароль не будет действительным, пока вы его не зашифруете в шаге 8.

```
S1> enable
```

```
S1# configure terminal
```

```
S1(config)# enable password c1$c0
```

```
S1(config)# exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#
```

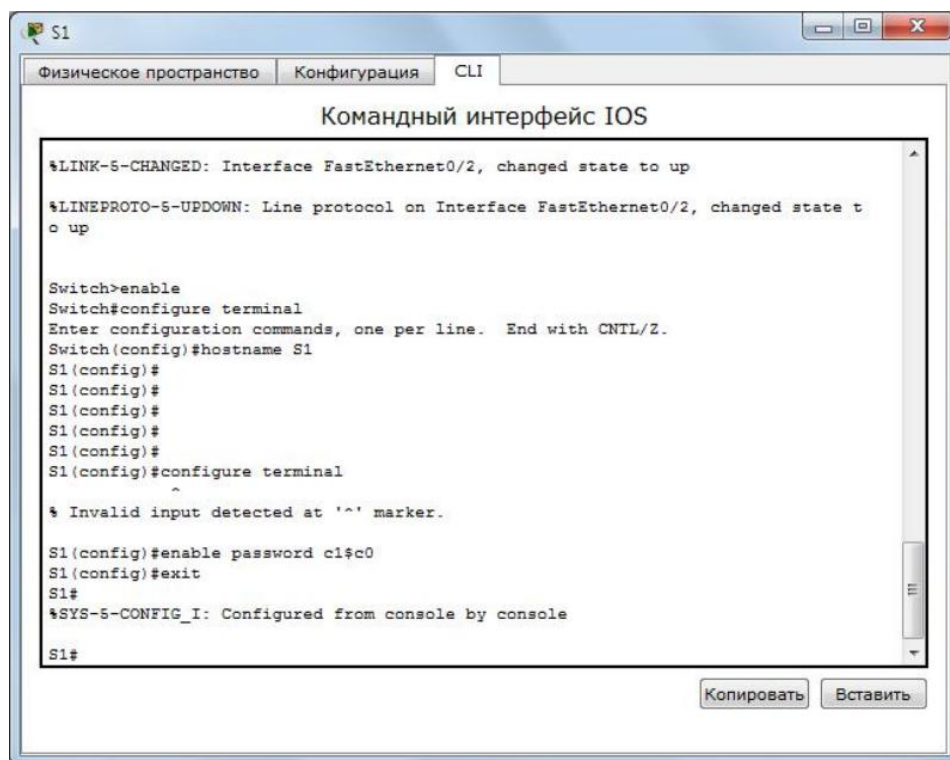


Рис. 1.7. Установка пароля для привилегированного режима

**Шаг 5: Убеждаемся, что доступ к привилегированному режиму защищён паролем.**

- a. Выполняем команду `exit` ещё раз, чтобы выйти из коммутатора.
- b. Нажимаем клавишу `^`, после чего будет предложено ввести пароль:

User Access Verification

Password:

- c. Первый пароль относится к консоли, который был задан для `line con 0`. Вводим этот пароль, чтобы вернуться в пользовательский режим.
- d. Вводим команду для доступа к привилегированному режиму.
- e. Вводим второй пароль, который был задан для ограничения доступа к привилегированному режиму (рис. 1.8).

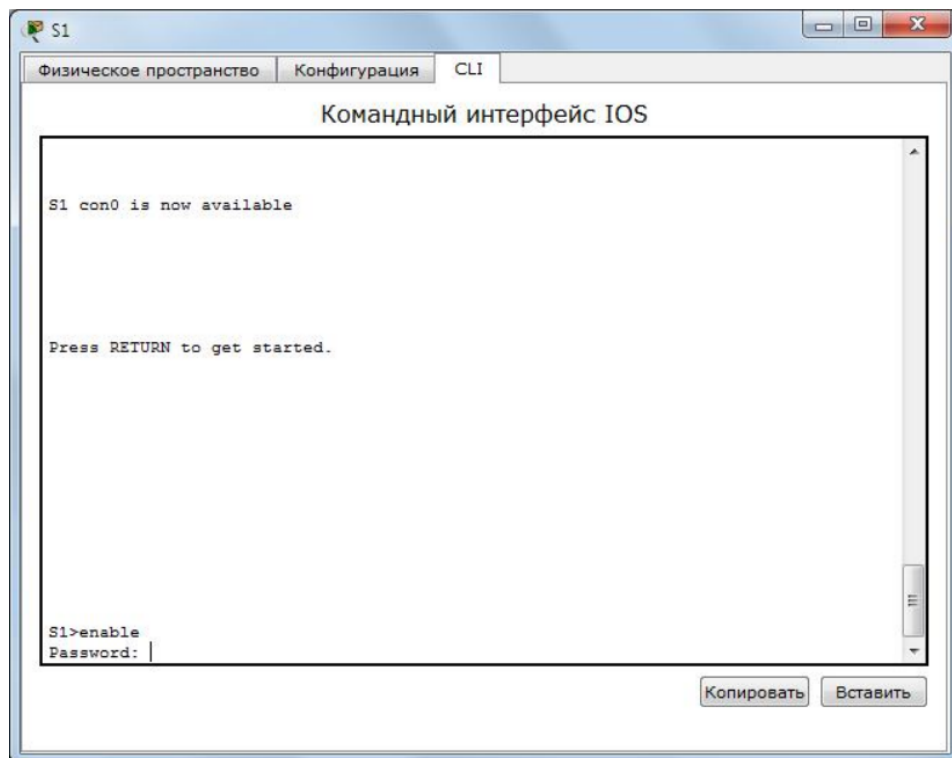


Рис. 1.8. Ввод пароля для входа в привилегированный режим

- f. Проверяем конфигурацию, изучив содержимое файла running-configuration (рис. 1.9):

S1# show running-config

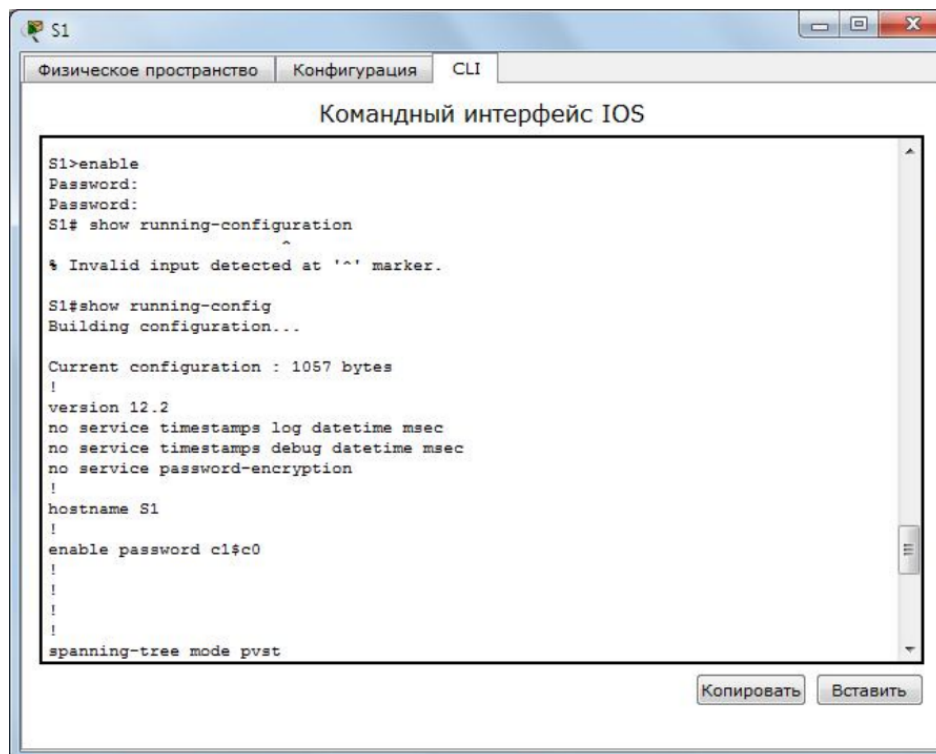


Рис. 1.9. Проверка конфигурации

Пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может представлять риск для системы безопасности, если за вашими действиями наблюдают из-за спины.

### Шаг 6: Настройка зашифрованного пароля для доступа к привилегированному режиму.

Пароль для enable нужно заменить на новый зашифрованный пароль с помощью команды enable secret. Устанавливаем для команды «enable» пароль itsasecret (рис. 1.10).

```
S1# config t
```

```
S1(config)# enable secret itsasecret
```

```
S1(config)# exit
```

```
S1#
```

Примечание. Пароль enable secret переопределяет пароль enable. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим нужно ввести пароль enable secret.

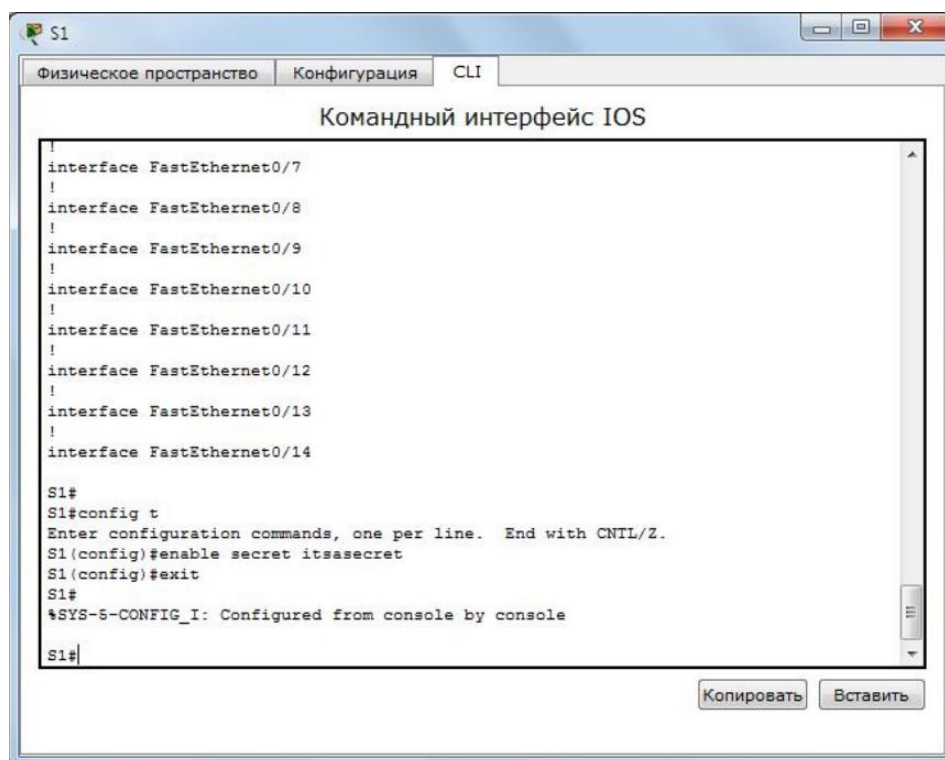


Рис. 1.10. Замена пароля на зашифрованный пароль

### Шаг 7: Убеждаемся в том, что пароль «enable secret» добавлен в файл конфигурации.

- a. Вводим команду show running-config ещё раз, чтобы проверить новый пароль enable secret (рис. 1.11).

Примечание. Команду show running-config можно сократить до S1# show run

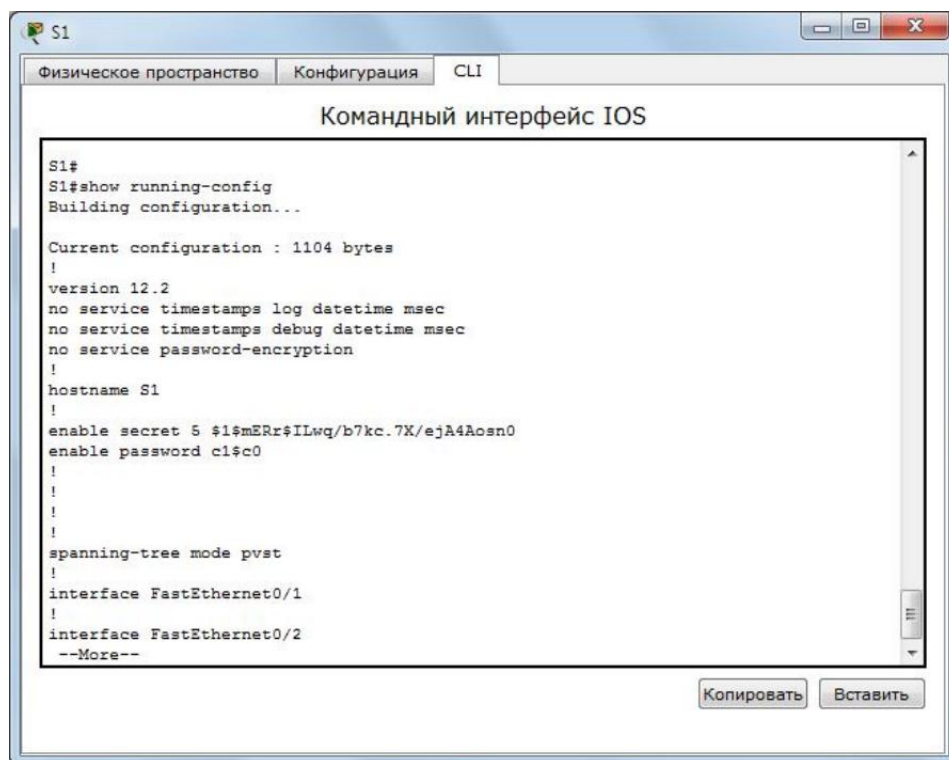


Рис. 1.11. Проверка зашифрованного пароля

б. Что отображается при выводе пароля enable secret?

```
$1$mERr$ILwq/b7kc.7X/ejA4Aosn0
```

с. Почему пароль enable secret отображается не так, как заданный пароль?

Потому что пароль enable secret зашифрован, а заданный пароль хранится в виде обычного текста

### **Шаг 8: Шифрование паролей для консоли и привилегированного режима.**

Как было видно в шаге 7, пароль enable secret зашифрован, а пароли enable и console хранятся в виде обычного текста. Сейчас мы зашифруем эти открытые пароли с помощью команды service password-encryption (рис. 1.12).

```
S1# config t
```

```
S1(config)# service password-encryption
```

```
S1(config)# exit
```

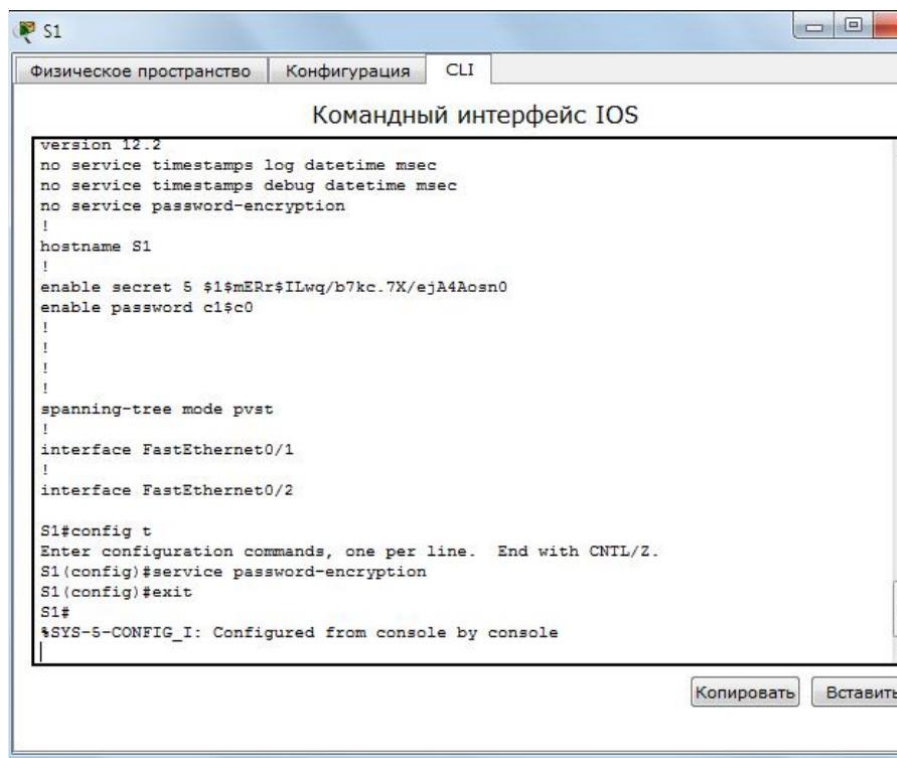


Рис. 1.12. Шифрование паролей

Если установить на коммутаторе другие пароли, они будут храниться в файле конфигурации в виде обычного текста или в зашифрованном виде?

Если на коммутаторе установить другие пароли, они будут храниться в файле конфигурации в зашифрованном виде.

## 2.3. НАСТРОЙКА БАННЕРА MOTD

### Шаг 1: Настройка сообщения ежедневного баннера (MOTD).

В набор команд Cisco IOS входит команда, которая позволяет настроить сообщение, которое будет показываться всем, кто входит в систему на коммутаторе. Это сообщение называется ежедневным баннером (MOTD). Текст баннера нужно заключить в двойные кавычки или использовать разделитель, отличный от любого символа в строке MOTD (рис. 1.13).

```
S1# config t
```

```
S1(config)# banner motd "Gruppa 3-7. NPI"
```

```
S1(config)# exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#
```



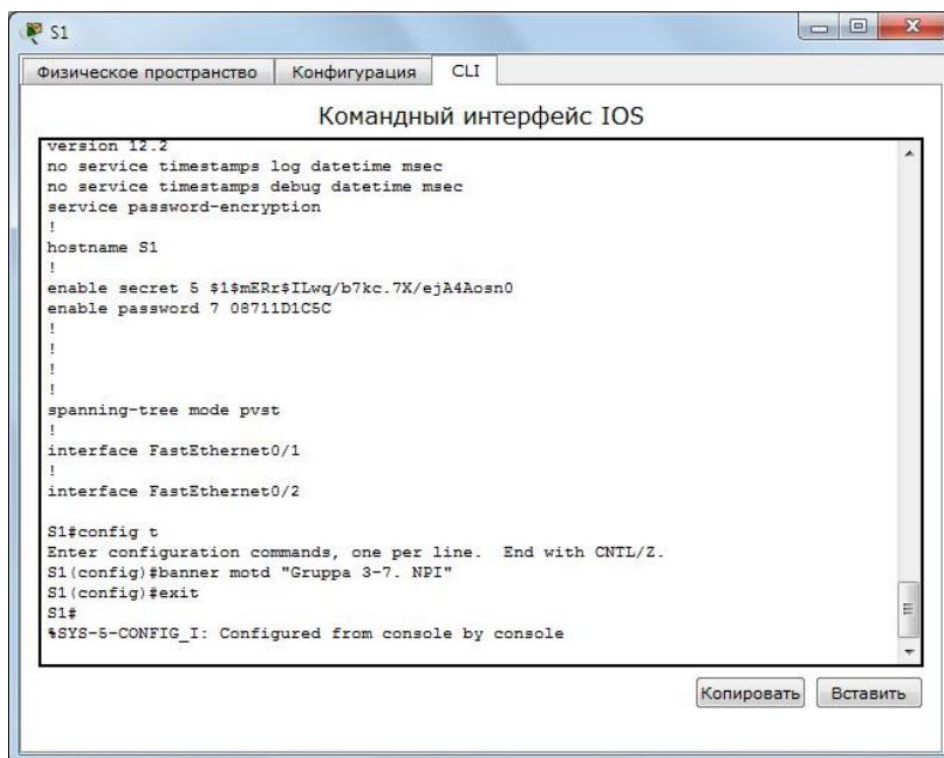


Рис. 1.13. Настройка сообщения ежедневного баннера MOTD

Когда будет отображаться этот баннер?

После ввода пароля и входа в консоль коммутатора (рис. 1.14).

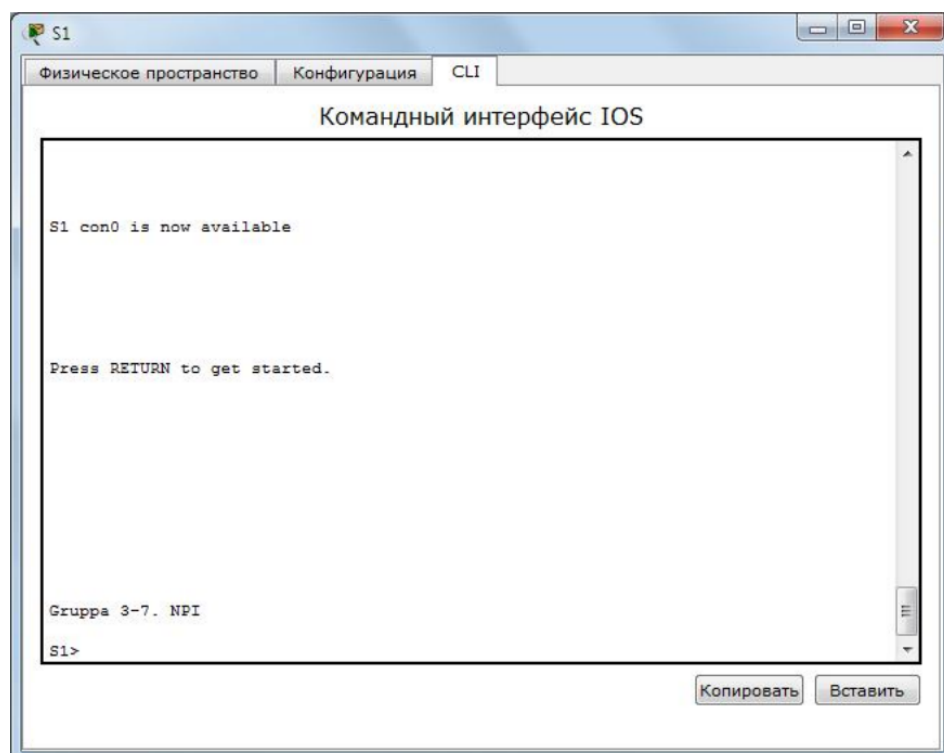


Рис. 1.14. Отображение ежедневного баннера MOTD

Зачем на всех коммутаторах должен быть баннер MOTD?

Чтобы при входе в коммутатор пользователю была доступна какая-либо полезная информация.

## 2.4. СОХРАНЕНИЕ ФАЙЛОВ КОНФИГУРАЦИИ В NVRAM

**Шаг 1: Проверяем правильность конфигурации с помощью команды «show run» (рис. 1.15).**

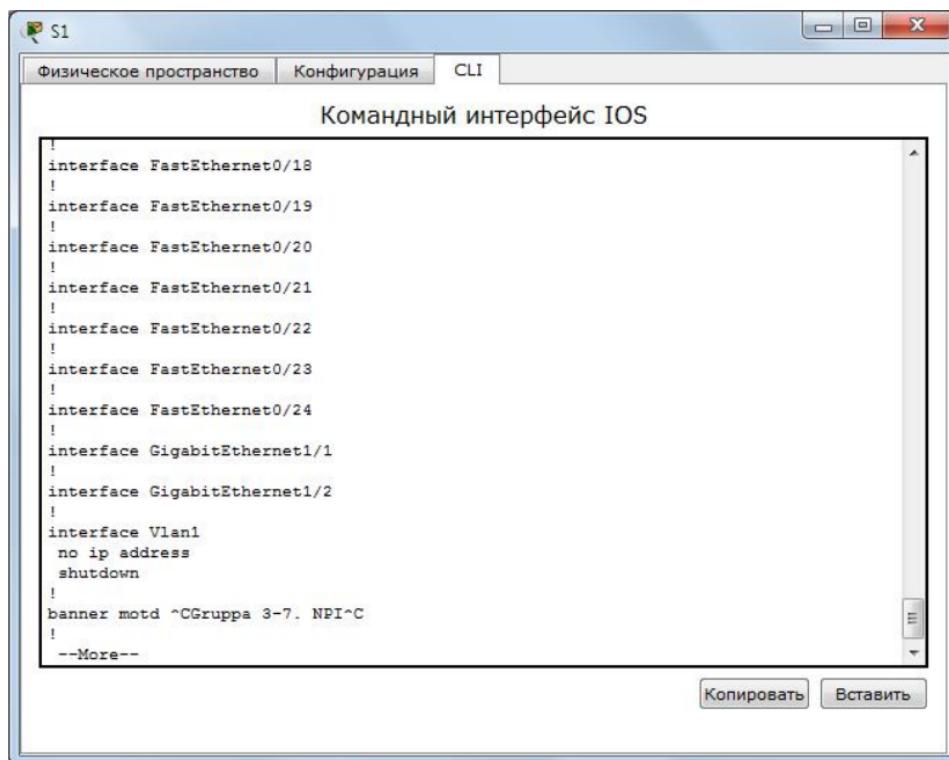


Рис. 1.15. Проверка правильности конфигурации

**Шаг 2: Сохраняем файл конфигурации.**

Мы завершили базовую настройку коммутатора. Теперь выполним резервное копирование файла конфигурации в NVRAM и проверим, чтобы внесённые изменения не потерялись после перезагрузки системы и отключения питания (рис. 1.16).

```
S1# copy running-config startup-config
```

```
Destination filename [startup-config]?[Enter]
```

```
Building configuration...
```

```
[OK]
```

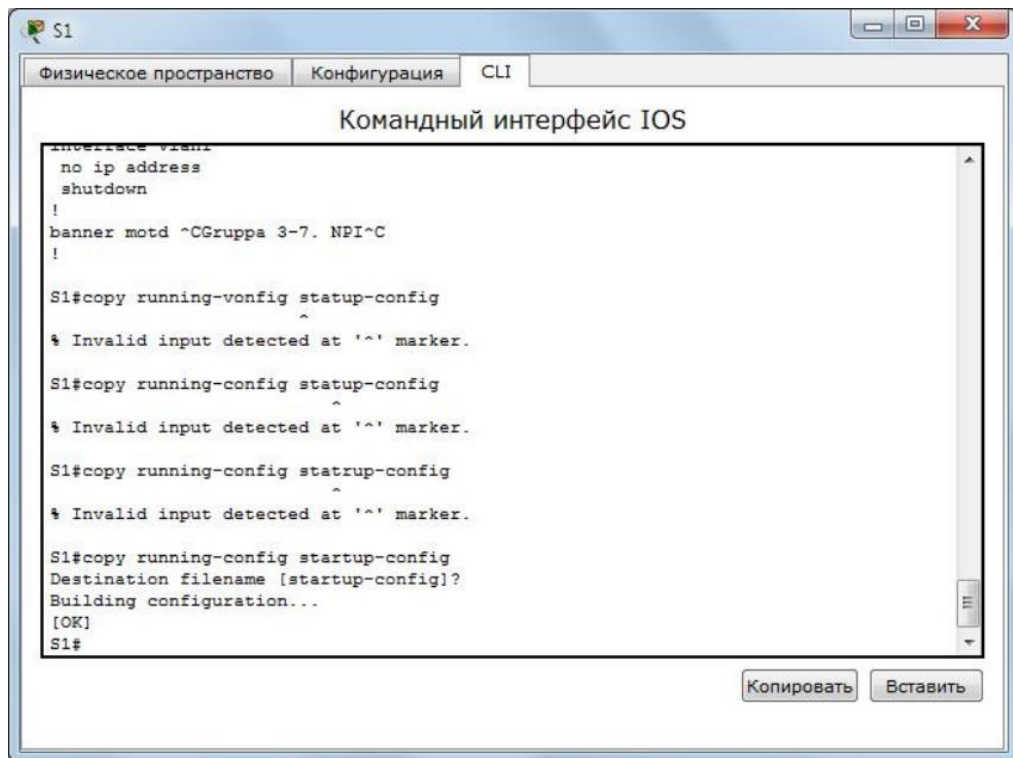


Рис. 1.16. Резервное копирование файла конфигурации в NVRAM

Какова самая короткая версия команды `copy running-config startup-config`? `copy running-config s` (рис. 1.17)

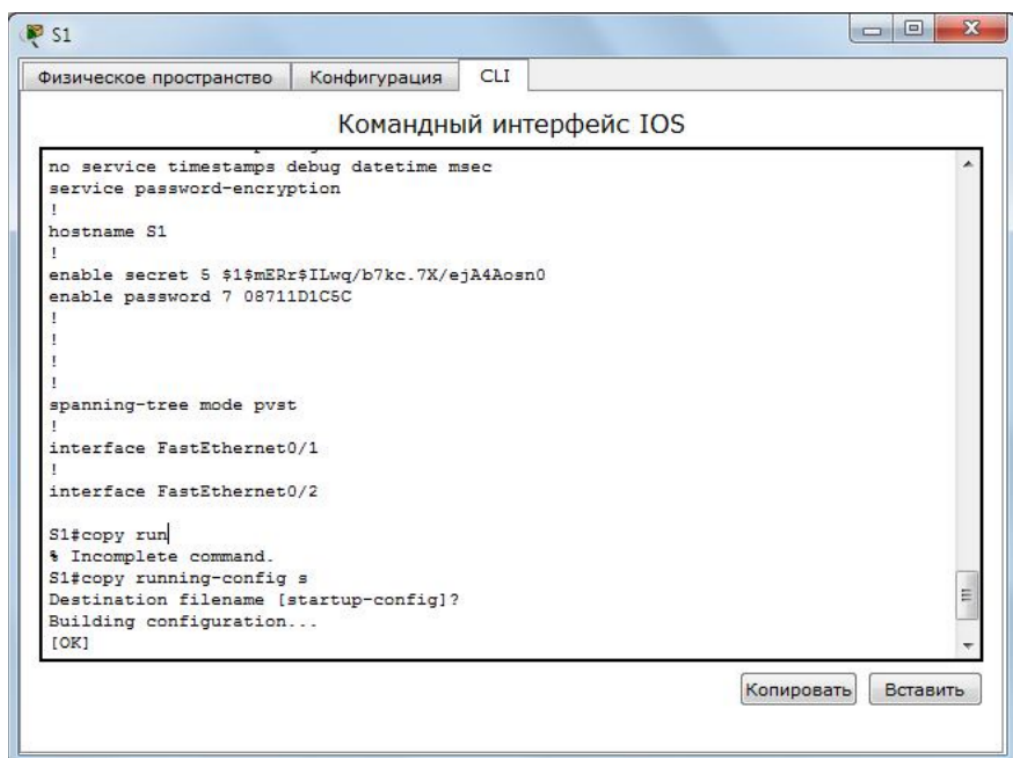


Рис. 1.17. Самая короткая версия команды `copy running-config startup-config`

### Шаг 3: Изучение начального файла конфигурации.

Какая команда отображает содержимое NVRAM?

S1# show run

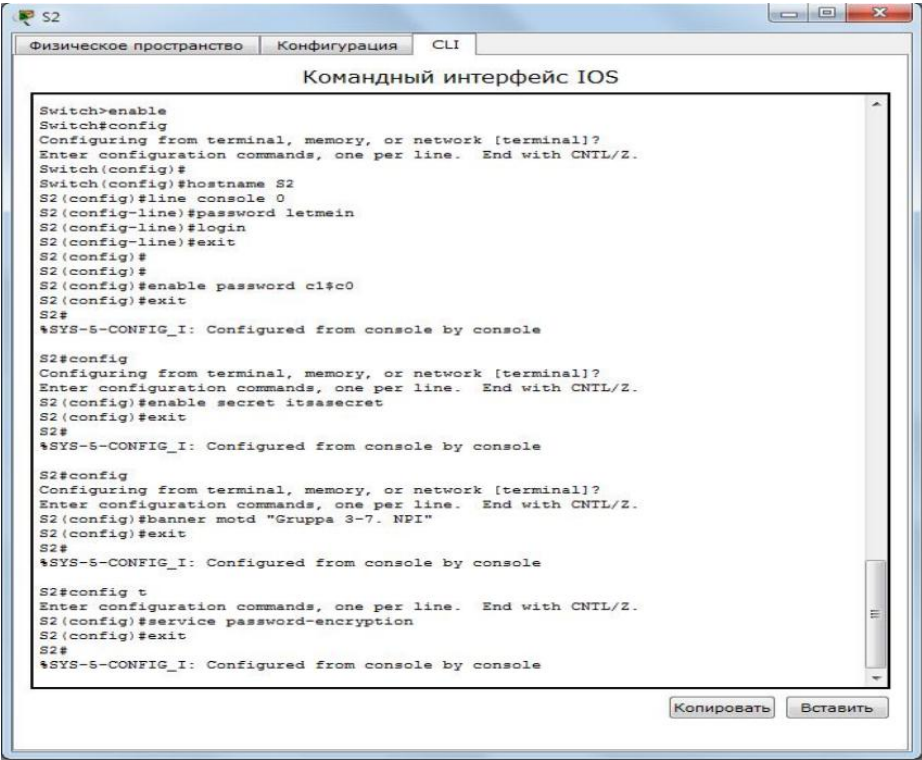
Все ли внесённые изменения были записаны в файл? Все внесённые изменения были записаны в файл.

## 2.5. КОНФИГУРАЦИЯ S2

Мы завершили настройку коммутатора S1. Теперь настроим коммутатор S2.

Настроим для коммутатора S2 следующие параметры.

- Имя устройства: S2 (рис. 1.18).
- Защищаем доступ к консоли паролем letmein (рис. 1.18).
- Устанавливаем для привилегированного режима пароль c1\$c0 и задаем пароль «enable secret» для itsasecret (рис. 1.18).
- Вводим следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе: «Gruppa 3-7. NPI» (рис. 1.18).
- Зашифровываем все открытые пароли (рис. 1.18).
- Проверяем правильность конфигурации (рис. 1.19).
- Сохраняем файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора (рис. 1.20).



```
Switch>enable
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#exit
S2(config)#
S2(config)#enable password c1$c0
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#enable secret itsasecret
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Gruppa 3-7. NPI"
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#service password-encryption
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Рис. 1.18. Конфигурирование коммутатора S2

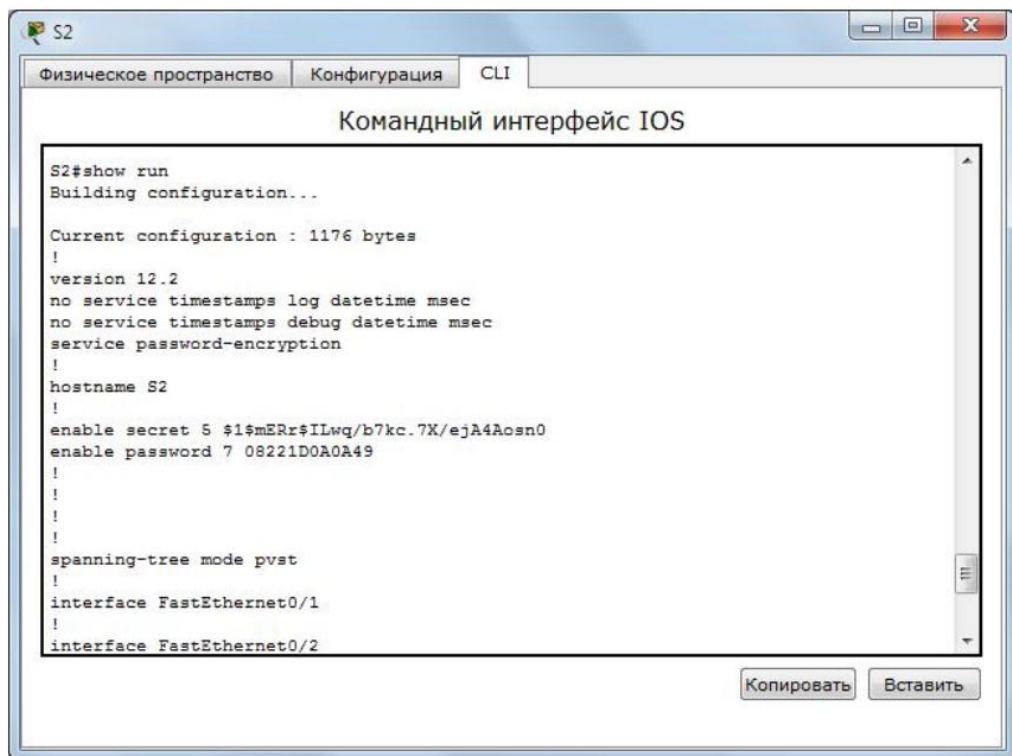


Рис. 1.19. Проверка правильности конфигурации

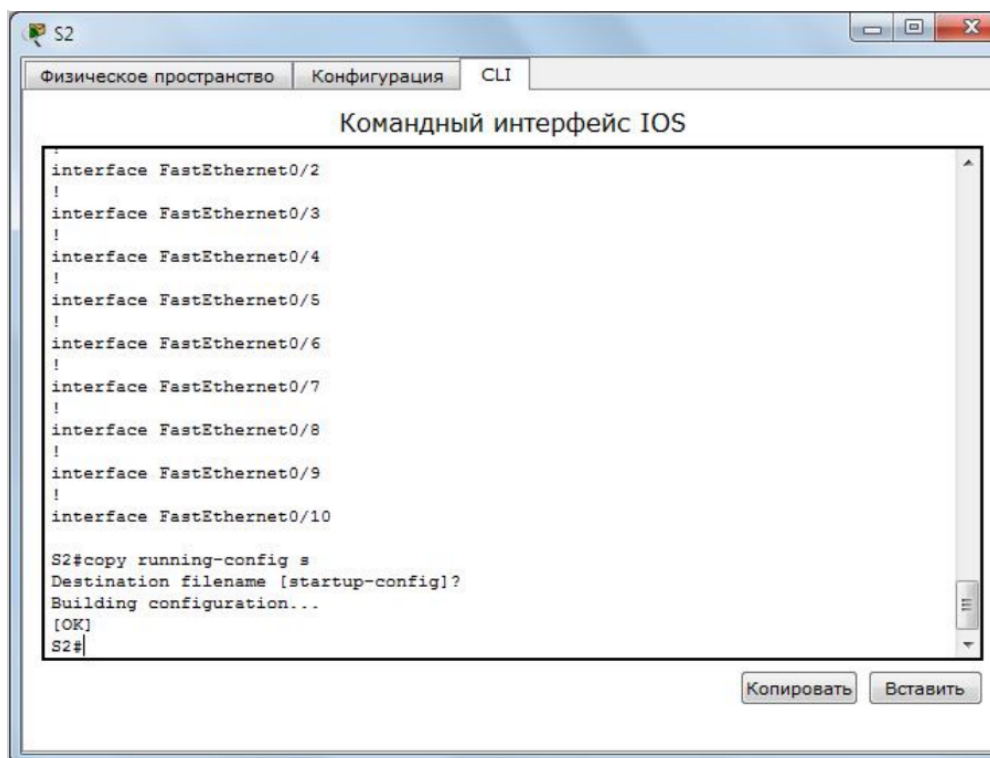


Рис. 1.20. Сохранение конфигурации 3.

## СОДЕРЖАНИЕ ОТЧЕТА

1. Тема работы.
2. Цель работы.
3. Индивидуальное задание.
4. Полное описание проделанной работы.

5. Выводы.

#### 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В привилегированном режиме доступны все команды коммутатора?
2. С помощью какой команды можно перейти в привилегированный режим?
3. С помощью какой команды можно просмотреть текущую конфигурацию коммутатора?
4. В какой режим нужно перейти, чтобы обеспечить безопасный доступ к консоли?
5. С помощью какой команды коммутатору можно назначить имя?
6. Какая команда осуществляет выход из коммутатора?
7. Для чего нужно шифрование паролей?
8. Как можно сократить команду `show running-config`?
9. С помощью какой команды можно зашифровать открытые пароли?
10. С помощью какой команды можно настроить зашифрованный пароль для доступа к привилегированному режиму?

#### Лабораторная работа № 2 НАСТРОЙКА СТАТИЧЕСКОЙ МАРШРУТИЗАЦИИ НА УСТРОЙСТВАХ CISCO

**Цель работы:** Создать (сконфигурировать) изображённую исходную сеть статической маршрутизации.

**Используемые средства и оборудование:** IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

#### 1. КРАТКАЯ ТЕОРИЯ

В маршрутизаторах используются три основных источника для добавления маршрутов в таблицы маршрутизации: подключенные маршруты, статические маршруты и динамические протоколы маршрутизации.

Маршрутизаторы всегда добавляют подключенные маршруты, если в конфигурациях интерфейсов заданы IP-адреса, а интерфейсы находятся в состоянии «up/np» и функционируют. Но в большинстве сетей инженеры сознательно прибегают к использованию динамических маршрутизирующих протоколов, чтобы вынудить каждый маршрутизатор накапливать информацию об остальных маршрутах в объединенной сети. Статические маршруты (маршруты, непосредственно добавляемые в таблицу маршрутизации при настройке конфигурации) используются наименее часто.

Статическая настройка конфигурации средств маршрутизации предусматривает добавление отдельных глобальных команд конфигурации `ip route`, которые задают маршрут к маршрутизатору. Эта команда конфигурации включает ссылку на подсеть (номер подсети и маску), а так же содержит указание, куда должны перенаправляться пакеты, предназначенные для данной подсети.

Статическая маршрутизация имеет собственные преимущества и недостатки.

Преимущества статической маршрутизации:

- нет нагрузки на процессор маршрутизатора;
- не используется полоса пропускания связей между маршрутизаторами;
- хорошая защита (поскольку только администратор устанавливает маршрутизацию к определенным сетям).

Недостатки статической маршрутизации:

- администратор должен хорошо понимать особенности объединенной сети и правильно настроить каждый маршрутизатор;
- если в объединенную сеть добавляется новая сеть, то администратору придется добавить новые пути во все маршрутизаторы;
- статическая маршрутизация неприменима в крупных сетях, поскольку требует большого объема работы.

## 2. ИСХОДНЫЕ ДАННЫЕ

В ходе выполнения лабораторной работы необходимо промоделировать сеть, представленную на рисунке 2.1

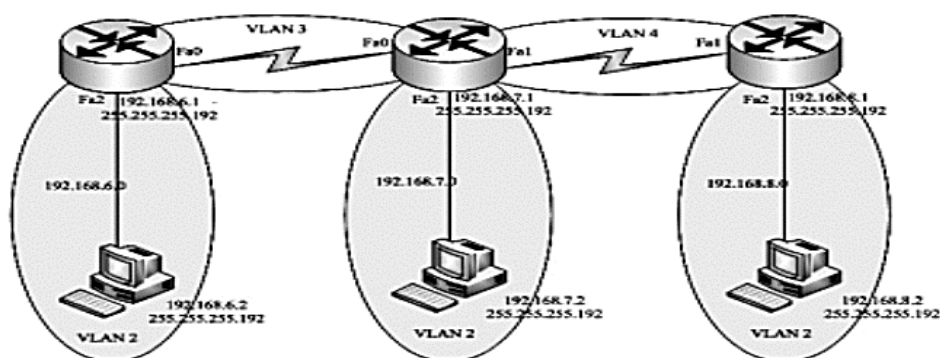


Рис. 2.1. Исходная сеть

### 2.1. Конфигурирование статической маршрутизации

После загрузки программы появился рабочее поле и различные «меню» в верхней и нижней части экрана (рис 2.2). Исходная топология сети уже собрана.

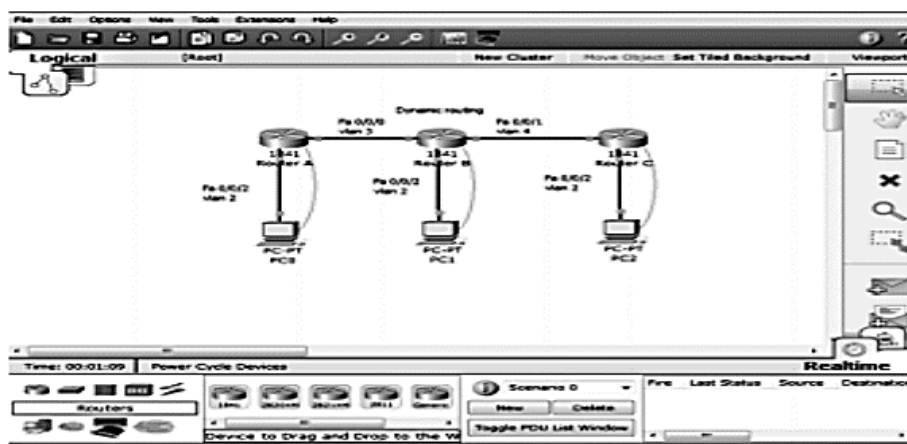


Рис. 2.2. Исходные данные

Также откроется окно с инструкциями (рис. 2.3). Листать страницы можно с помощью кнопки Check Results.



Рис.2.3. Инструкции к выполнению работы

## 2.2 Создание статической маршрутизации

Чтобы сконфигурировать статическую маршрутизацию администратор должен знать маршруты ко всем удаленным сетям назначения, которые непосредственно не присоединены к данному маршрутизатору.

Используйте команду `ip route`, чтобы сконфигурировать статическую маршрутизацию. Затем указываем адрес сети назначения, сетевую маску и адрес входного интерфейса следующего маршрутизатора на пути к адресату (шлюз).

1) Конфигурирование статической маршрутизации на маршрутизаторе Router\_A.

```
Router_A#conf t
Router_A(config)#ip route 192.168.7.0 255.255.255 192 192.168.4.2
Router_A(config)#ip route 192.168.5.0 255.255.255 192 192.168.4.2
Router_A(config)#ip route 192.168.8.0 255.255.255 192 192.168.4.2
```

2) Конфигурирование статической маршрутизации на маршрутизаторе Router\_B.

```
Router B#conf t Router_B(config)#ip route 192.168.6.0 255.255.255 192 192.168.4.1
Router_B(config)#ip route 192.168.8.0 255.255.255 192 192.168.5.2
```

3) Конфигурирование статической маршрутизации на маршрутизаторе Router\_C.

```
Router_C#conf t Router_C(config)#ip route 192.168.6.0 255.255.255 192 192.168.5.1
Router_C(config)#ip route 192.168.7.0 255.255.255 192 192.168.5.1
Router_C(config)#ip route 192.168.4.0 255.255.255 192 192.168.5.1
```

Проверим таблицу маршрутизации командами `show ip route` и `ping` (рис. 2.4).



```

Router_A>ena
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.4.0/26 is subnetted, 1 subnets
C       192.168.4.0 is directly connected, Vlan3
    192.168.5.0/26 is subnetted, 1 subnets
S       192.168.5.0 [1/0] via 192.168.4.2
    192.168.6.0/26 is subnetted, 1 subnets
C       192.168.6.0 is directly connected, Vlan2
    192.168.7.0/26 is subnetted, 1 subnets
S       192.168.7.0 [1/0] via 192.168.4.2
    192.168.8.0/26 is subnetted, 1 subnets
S       192.168.8.0 [1/0] via 192.168.4.2

```

Рис. 2.4. Проверка статической маршрутизации

4) Check Results! проверим правильность выполнения работы, нажав на кнопку в окне инструкции.

### 3. ВАРИАНТЫ ЗАДАНИЙ

Номер варианта		1	2	3
Router A	Vlan2	192.168.6.1/26	192.168.11.1/26	192.168.21.1/26
	Vlan3	192.168.4.1/26	192.168.14.1/26	192.168.24.1/26
Router B	Vlan2	192.168.7.1/26	192.168.12.1/26	192.168.22.1/26
	Vlan3	192.168.4.2/26	192.168.14.2/26	192.168.24.2/26
	Vlan4	192.168.5.1/26	192.168.15.1/26	192.168.25.1/26
Router C	Vlan2	192.168.8.1/26	192.168.13.1/26	192.168.23.1/26
	Vlan3	192.168.5.2/26	192.168.15.2/26	192.168.25.2/26
PC0		192.168.6.2/26	192.168.11.2/26	192.168.21.2/26
PC1		192.168.7.2/26	192.168.12.2/26	192.168.22.2/26
PC2		192.168.8.2/26	192.168.13.2/26	192.168.23.2/26

### 4. СОДЕРЖАНИЕ ОТЧЕТА

1. Тема работы.
2. Цель работы.
3. Домашнее задание.
4. Полное описание проделанной работы.
5. Выводы.

### 5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем преимущества статической маршрутизации?
2. Дайте характеристику параметрам статической таблицы маршрутизации?
3. Какие этапы при установке устройства присущи маршрутизаторам компании Cisco, но отсутствуют у коммутаторов?

4. Какую из указанных ниже команд можно встретить в интерфейсе командной строки маршрутизатора, но не коммутатора?
  - команда `clock rate`;
  - команда `ip address маска адрес`;
  - команда `ip address dhcp`;
  - команда `interface vlan 1`.
5. Чем отличаются интерфейсы командной строки маршрутизатора и коммутатора компании Cisco?
6. Какая из указанных ниже команд не покажет настройки IP адресов и масок в устройстве?
  - `show running-config`;
  - `show protocol` тип номер;
  - `show ip interface brief`;
  - `show version`.
7. Перечислите основные функции маршрутизатора в соответствии с уровнями модели OSI.
8. Приведите классификацию маршрутизаторов по областям применения.
9. Перечислите основные технические характеристики маршрутизаторов.
10. Дайте характеристику основным сериям маршрутизаторов компании Cisco.
11. Приведите перечень протоколов маршрутизации и дайте им краткие характеристики.
12. Приведите перечень поддерживаемых маршрутизаторами интерфейсов для локальных и глобальных сетей и определите их назначение.
13. Приведите перечень поддерживаемых маршрутизаторами сетевых протоколов и определите их назначение.
14. Для чего используются маршруты по умолчанию? Каким способом можно задать маршрут по умолчанию на роутере?
15. Какая команда используется для конфигурирования статической маршрутизации? Какие параметры она содержит? В каком командном режиме она вводится? В каких сетях лучше использовать статическую маршрутизацию?

### **Лабораторная работа №3 НАСТРОЙКА VLAN НА УСТРОЙСТВАХ CISCO**

**Цель работы:** научиться использовать технологию VLAN.

**Используемые средства и оборудование:** IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

#### **1.КРАТКАЯ ТЕОРИЯ**

VLAN — виртуальная локальная сеть. Группа устройств локальной сети, которые конфигурируются (с использованием программного обеспечения управления) таким образом, что могут участвовать в обмене данными так, словно подключены к одному кабелю, хотя на самом деле они находятся в различных сегментах сети. Поскольку

виртуальные сети основываются на виртуальных, а не физических соединениях, то они обладают чрезвычайно высокой гибкостью.

Как показано на рис. 3.1, виртуальная локальная сеть представляет собой логическое объединение устройств или пользователей. Объединение их в группу может производиться по выполняемым функциям, используемым приложениям, по отделам и т.д., независимо от их физического расположения в сегментах (segment). Конфигурирование виртуальной сети производится на коммутаторе программным путем. Виртуальные сети не стандартизированы и требуют использования программного обеспечения от производителя коммутатора.

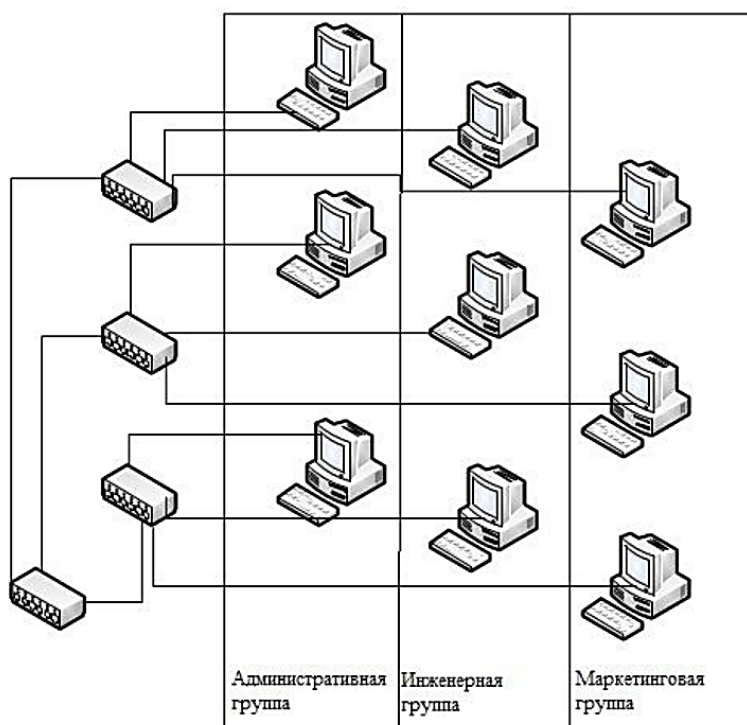


Рис. 3.1. Виртуальная сеть

Одной из важных функций, реализуемых в технологии Ethernet, являются виртуальные локальные сети (Virtual Local Area Networks – VLAN), в которых для объединения рабочих станций и серверов в логические группы используются коммутаторы. Связь устройств, принадлежащих к одной VLAN сети, возможна только с устройствами этой же сети, поэтому сеть с коммутацией функционирует как несколько индивидуальных, не соединенных друг с другом локальных сетей LAN. Трудно дать общее строгое определение сетей VLAN, поскольку разные производители используют различные подходы к созданию таких сетей.

Компании часто используют сети VLAN в качестве способа логической группировки пользователей. Это можно сравнить с традиционной организацией рабочих мест, в которой несколько отделов обычно группировались в локальный департамент, и локальная сеть естественным образом решала задачи связи для этого департамента. В настоящее время сотрудники часто не связаны с конкретным физическим рабочим местом, поэтому сети VLAN создают не физическую, а логическую группу пользователей. Например, сотрудники, работающие в отделе маркетинга, объединены VLAN-сетью маркетинга, а сотрудники инженерного подразделения – VLAN-сетью инженерных служб.

Сети VLAN решают задачи масштабирования сети, обеспечения безопасности и сетевого управления. В сетях с топологией VLAN маршрутизаторы обеспечивают фильтрацию широковещания, решают задачи защиты сети и управления потоками данных.

Сеть VLAN представляет собой группу сетевых устройств и служб, не ограниченную физическим сегментом или коммутатором.

## 2. ХОД РАБОТЫ

Схема с одним коммутатором:

1. Открываем Cisco Packet Tracer и перетаскиваем в рабочую область коммутатор 2960 и 4 компьютера Generic. Переходим во вкладку Connections и выбираем тип кабеля: Copper Straight-Through. Подключаем каждый компьютер к коммутатору (рис. 3.2).

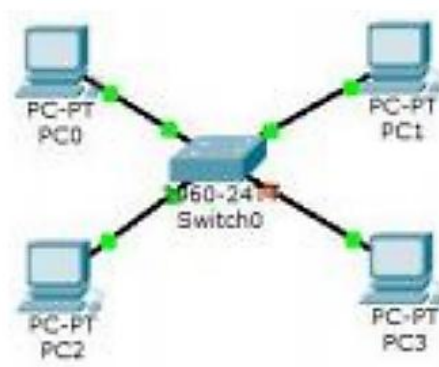


Рис. 3.2. Схема подключения к коммутатору

2. Предположим, что компьютеры PC0 и PC1 принадлежат одному сегменту бухгалтеров. Выберем фигуру прямоугольник и определяем сегмент. Далее аналогично определяем сегмент обычных пользователей (рис. 3.3).

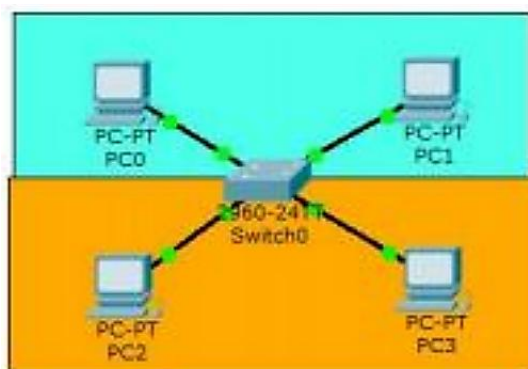


Рис. 3.3. Схема разбиения на сегменты

3. Разделим трафик сегментов. Открываем настройки коммутатора, входим в Console. С помощью команды `configure terminal` задаем режим глобального конфигурирования. Определяем `vlan`, в котором будут находиться пользователи. Затем создаем `vlan 2` и задаем имя `buh`. Выходим.

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name buh
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#

```

4. Переходим к настройке интерфейса. Наводим мышку на соединение и видим, что 1 компьютер подключается через FastEthernet0/1, а 2 - через FastEthernet0/2. Данные порты определяем в vlan 2. Заходим в настройки FastEthernet0/1 и видим, что порт функционирует в режиме access и определяем его в vlan 2. Настройка окончена. Аналогично настраиваем FastEthernet0/2.

```

Switch(config)#int
Switch(config)#interface Fa
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#

```

При помощи команды show vlan проверяем работу.

```

Switch#show vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/9, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig1/1, Gig1/2
2 buh	active	Fa0/1, Fa0/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100301	1500	-	-	-	-	-	0	0
2	enet	100302	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	learn	-	0	0

```

--More--

```

5. Аналогично настраиваем другой сегмент.

```

Switch#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#vlan 3
Switch(config-vlan)#name users
Switch(config-vlan)#exit
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#swi
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#swi
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch#
4898-9-CORRIG_1: Configured from console by console

```

При помощи команды show vlan проверяем работу.

6. Задаем IP-адреса 1 и 2 компьютерам (192.168.2.1 и 192.168.2.2), а 3 и 4 компьютерам (192.168.3.1 и 192.168.3.2). Проверяем командой ping соединение 1 компьютера со 2, а затем с 3.

```

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=0ms TTL=128
Reply from 192.168.3.2: bytes=32 time=0ms TTL=128
Reply from 192.168.3.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

```

7. Если посмотреть в коммутаторе таблицу mac-адресов, можно увидеть, что в ней стал указываться и vlan - адрес, с которого приходит mac-адрес.

```

Switch#show mac add
Switch#show mac address-table
-----
Mac Address Table
-----
Vlan    Mac Address      Type        Ports
-----
2       0001.c966.57a1   DYNAMIC     Fa0/2
2       0090.0c70.2b22   DYNAMIC     Fa0/1
3       0003.e44e.645d   DYNAMIC     Fa0/4
3       00e0.f774.b056   DYNAMIC     Fa0/3
Switch#

```

Схема с двумя коммутаторами:

1. Рассмотрим пример с использованием 2 коммутаторов. Для этого удаляем сегменты и дублируем оборудование. Соединяем коммутаторы типом кабеля: Copper Cross-Over GigabitEthernet 1/1 (рис. 3.4).

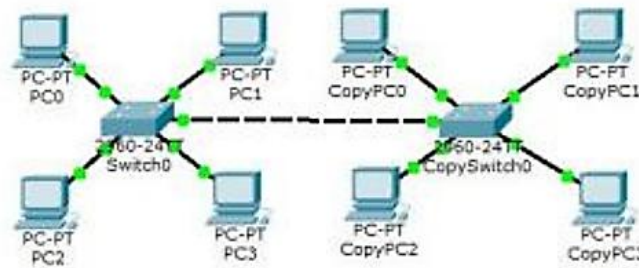


Рис. 3.4. Схема с двумя коммутаторами

2. Задаем IP-адреса компьютеров и объединяем их в сегменты (рис. 3.5).

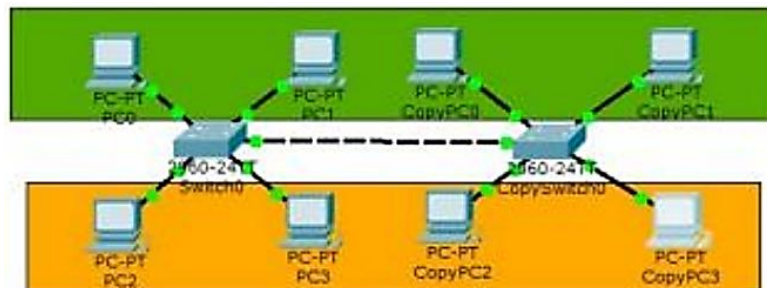


Рис. 3.5. Разбиение на сегменты схемы с двумя коммутаторами

3. Так, как коммутатор скопирован, он уже настроен. Проверяем с помощью команды show run.

```

!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!

```

4. Настраиваем trunk-port. Входим в режим конфигурирования, затем в interface GigabitEthernet 1/1 и указываем режим.

```

Switch(config)#int
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 1/1
Switch(config-if)#swi
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed stat
* to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed stat
* to up

```

Задаем нужные vlan.

```

Switch(config-if)#swi
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#exit
Switch(config)#

```

---

Аналогично настраиваем другой коммутатор.



```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 1/1
Switch(config-if)#swi
Switch(config-if)#switchport mode trunk
Switch(config-if)#swi
Switch(config-if)#switchport trunk allowed vlan 2?
WORD
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

```

5. Проверяем взаимодействие компьютеров командой ping.

```

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
~C
PC>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=1ms TTL=128

```

6. Исключаем из trunk-port vlan 3.

```

Switch(config)#interface gi1/1
Switch(config-if)#swi
Switch(config-if)#switchport trunk allowed vlan 2
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show run
Building configuration...

Current configuration : 1293 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
spanning-tree mode pvst
!

```

Проверяем взаимодействие компьютеров командой ping.

```

PC>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Ping statistics for 192.168.3.4:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Ping statistics for 192.168.3.3:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
PC>

```

### 3. СОДЕРЖАНИЕ ОТЧЕТА

1. Тема работы.
2. Цель работы.
3. Индивидуальное задание.
4. Полное описание проделанной работы.
5. Выводы.

### 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что собой представляет VLAN? Какими преимуществами и недостатками обладает VLAN?
2. Какие существуют способы организации VLAN?
3. Охарактеризуйте способы, позволяющие устанавливать членство в VLAN.
4. Охарактеризуйте протокол VTP. Какие преимущества и ограничения возникают при использовании протокола VTP?
5. Какие существуют режимы работы протокола VTP?

### Лабораторная работа № 4 ИСПОЛЬЗОВАНИЕ DHCP-ПРОТОКОЛА

**Цель работы:** изучить использование DHCP-протокола.

**Используемые средства и оборудование:** IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

#### 1. КРАТКАЯ ТЕОРИЯ

DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки хоста) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Данный протокол работает по модели «клиент-сервер». Передача данных производится при помощи протокола UDP. По умолчанию запросы от клиента делаются на 67 порт к серверу, сервер в свою очередь отвечает на порт 68 к клиенту, выдавая адрес IP и другую необходимую информацию, такую, как сетевую маску, шлюз по умолчанию и серверы DNS.

Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные

параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Стандарт протокола DHCP был принят в октябре 1993 года. Действующая версия протокола (март 1997 года) описана в RFC 2131. Новая версия DHCP, предназначенная для использования в среде IPv6, носит название DHCPv6 и определена в RFC 3315 (июль 2003 года).

Протокол DHCP предоставляет три способа распределения IP-адресов:

- Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес.

- Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определенного администратором диапазона.

- Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдается компьютеру не на постоянное пользование, а на определенный срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того клиент сам может отказаться от полученного адреса.

## 2.ХОД РАБОТЫ

### Пример №1.

1. Открываем Cisco Packet Tracer и приступаем к настройке схемы (рис. 4.1):



Рис.4.1. Исходная схема

2. Настраиваем Router0.

Настраиваем порт fa0/0, по которому подключен Switch0 и присваиваем порту ip-адрес.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#

```

### 3. Настраиваем DHCP.

```

Router(config)#
Router(config)#ip dhcp pool DHCP
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#

```

### 4. Исключаем определенные ip-адреса из выдачи DHCP. Это ip – адреса сервера и роутера.

```

Router(config)#ip dhcp ex
Router(config)#ip dhcp excluded-address 192.168.1.100
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#

```

### 5. Настраиваем ip – адреса на компьютерах (рис. 4.2).

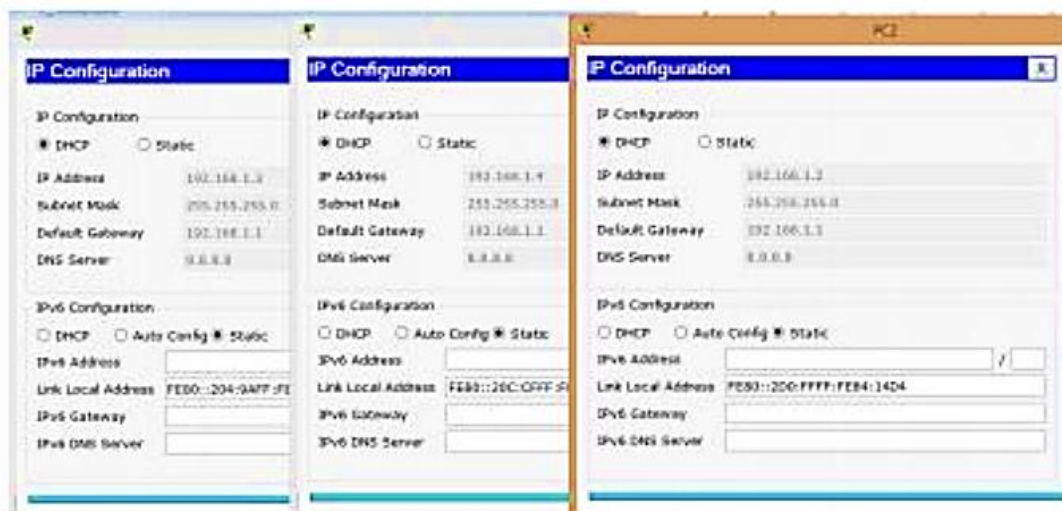


Рис.4.2. Настройка ip-адресов

### 6. Проверяем взаимодействие командой ping, пропинговав с PC0 шлюз, PC1, PC2. Ping успешен (рис. 4.3).

```

Packet Tracer: PC Command Line 1.2
Pinging 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Pinging 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=0ms TTL=255
Reply from 192.168.1.3: bytes=32 time=0ms TTL=255
Reply from 192.168.1.3: bytes=32 time=0ms TTL=255
Reply from 192.168.1.3: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Pinging 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=0ms TTL=255
Reply from 192.168.1.4: bytes=32 time=0ms TTL=255
Reply from 192.168.1.4: bytes=32 time=0ms TTL=255
Reply from 192.168.1.4: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Рис.4.3. Проверка взаимодействия

Таким образом, настроена раздача IP – адресов по DHCP.

**Пример №2.**

1. Открываем Cisco Packet Tracer и приступаем к настройке схемы (рис. 8.4).:

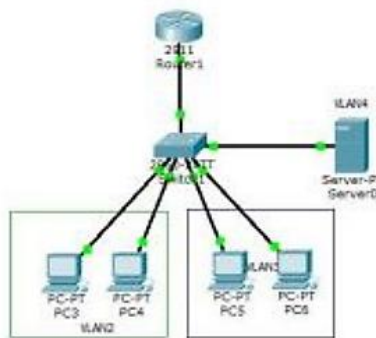


Рис. 4.4. Исследуемая схема сети

2. Настраиваем Switch1.

Создаем vlan.

```

Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit

Switch(config)#vlan 4
Switch(config-vlan)#name DHCP
Switch(config-vlan)#exit

```

Настраиваем порты.

```

Switch(config)#int range fa0/2-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#int range fa0/4-5
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#exit
Switch(config)#int fa0/6
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#

```

Ц

Прокидываем vlan на Router0.

```

Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr mem
Building configuration...
[OK]
Switch#

```

Просматриваем настройки с помощью команды show run.

```

!
interface FastEthernet0/1
 switchport trunk allowed vlan 2-4
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 4
 switchport mode access
!

```

3. Настраиваем Router1

Создаем сабинтерфейсы.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gi0/0.2
Router(config-subif)#enc
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int gi0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int gi0/0.4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

Просматриваем настройки с помощью команды show run.

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 192.168.4.2
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
 ip helper-address 192.168.4.2
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
```

4. Настраиваем DHCP сервер.

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IP Address	192.168.4.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.1
DNS Server	

5. Проверяем командой ping. Ping успешен (рис. 4.5).

```

Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time=1ms TTL=255
Reply from 192.168.4.1: bytes=32 time=0ms TTL=255
Reply from 192.168.4.1: bytes=32 time=0ms TTL=255
Reply from 192.168.4.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

SERVER>

```

Рис. 4.5. Проверка параметров

6. Заходим во вкладку Config, выбираем в меню DHCP и выполняем настройки (рис. 4.6.).

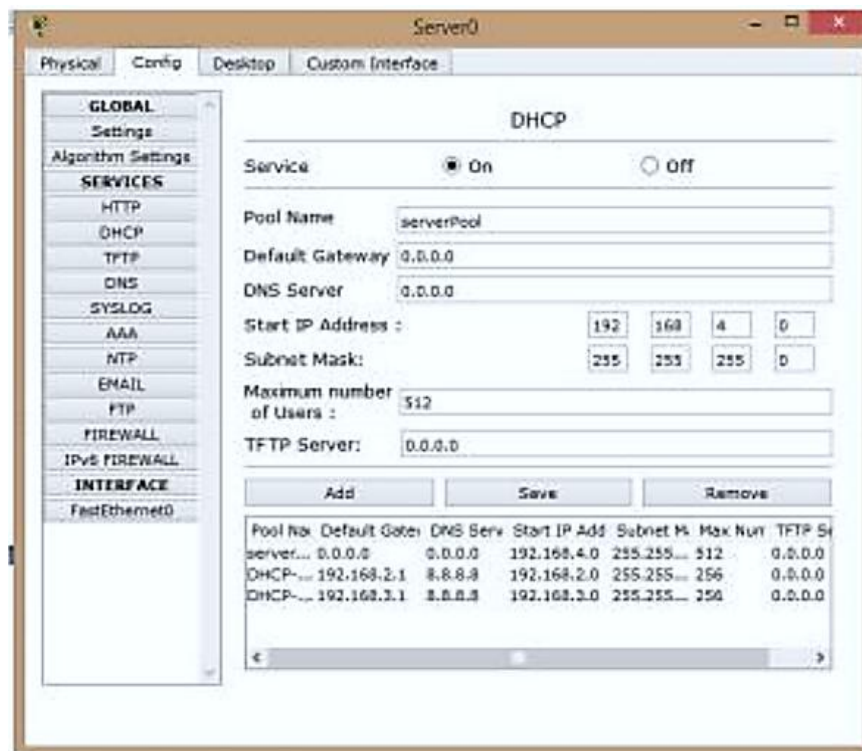


Рис. 4.6. Настройка параметров DHCP

7. Перенаправляем запросы DHCP на сервер.

```

Router(config)#int gi0/0.2
Router(config-subif)#ip-helper-address 192.168.4.2
% Invalid input detected at '^' marker.

Router(config-subif)#ip helper-address 192.168.4.2
Router(config-subif)#exit
Router(config)#int gi0/0.3
Router(config-subif)#ip helper-address 192.168.4.2
Router(config-subif)#exit
Router(config)#

```

8. Настраиваем IP – адреса на компьютерах (рис. 4.7).



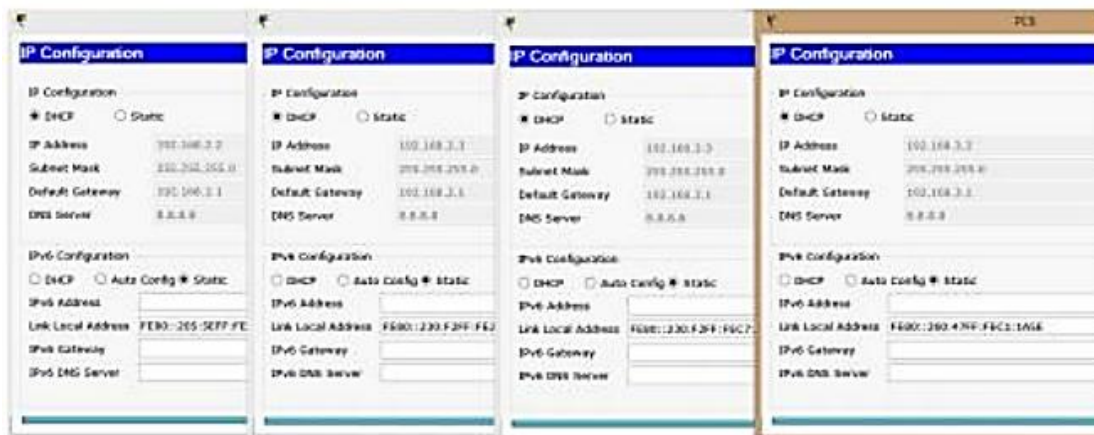


Рис. 4.7. Настройка IP – адреса на компьютерах

9. Проверям взаимодействие командой ping. Ping успешен (рис. 4.8.).

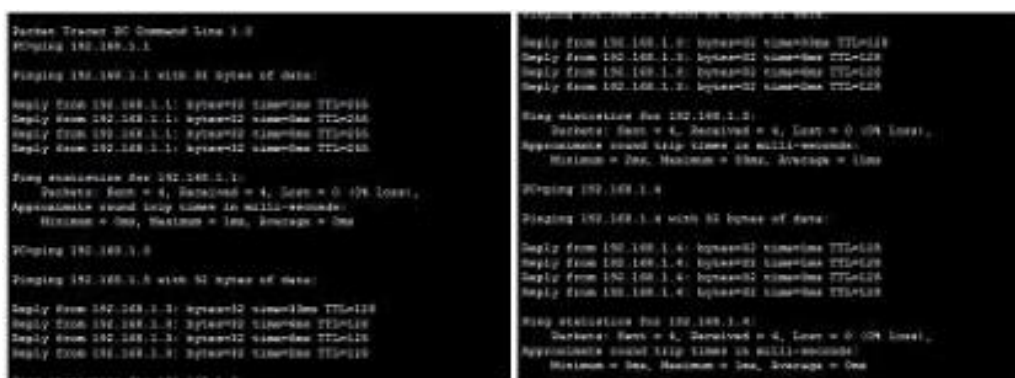


Рис. 4.8. Проверка взаимодействия посредством выделенного DHCP - сервера

Таким образом, настроена раздача IP – адресов для двух сегментов посредством выделенного DHCP - сервера.

### 3. СОДЕРЖАНИЕ ОТЧЕТА

1. Тема работы.
2. Цель работы.
3. Индивидуальное задание.
4. Полное описание проделанной работы.
5. Выводы.

### 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что из себя представляет протокол DHCP?
2. Охарактеризуйте способы распределение IP-адресов.
3. Охарактеризуйте опции DHCP
4. Опишите процедуру настройки пула DHCP.
5. Что собой представляют классы параметров DHCP? Каковы их разновидности?

### Лабораторная работа № 5 DNS – СЕРВЕР: УСТАНОВКА И УПРАВЛЕНИЕ

**Цель работы:** Изучение особенностей установки и управления DNS-сервером в сетях Windows

**Средства для выполнения работы:**

- аппаратные: ПК;
- программные: установленная ОС Windows 7, Windows 10;

1. Теоретические сведения В этом разделе теоретических сведений разберем подробности и особенности работы DNS-сервера. DNS-сервер, Domain name system — приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу. Также DNS-сервером могут называть хост, на котором запущено соответствующее приложение.

### 1.1. Типы DNS-серверов

По выполняемым функциям DNS-серверы делятся на несколько групп, при этом сервер определённой конфигурации может относиться сразу к нескольким типам:

- Авторитативный DNS-сервер - сервер, отвечающий за какую-либо зону.
  - Мастер, или первичный сервер (в терминологии BIND) — имеет право на внесение изменений в данные зоны. Обычно зоне соответствует только один мастер-сервер. В случае Microsoft DNS сервера и его интеграции с Active Directory мастер-серверов может быть несколько (так как репликация изменений осуществляется не средствами DNS-сервера, а средствами Active Directory, за счёт чего обеспечивается равноправность серверов и актуальность данных).
  - Слейв (англ. - Slave), или вторичный сервер, не имеющий права на внесение изменений в данные зоны и получающий сообщения об изменениях от мастер-сервера. В отличие от мастер-сервера, их может быть (практически) неограниченное количество. Слейв также является авторитативным сервером (и пользователь не может различить мастер и слейв, разница появляется только на этапе конфигурирования/внесения изменений в настройки зоны).
- Кэширующий DNS-сервер — обслуживает запросы клиентов (получает рекурсивный запрос, выполняет его с помощью нерекурсивных запросов к авторитативным серверам или передаёт рекурсивный запрос вышестоящему DNS-серверу).
- Перенаправляющий DNS-сервер (англ. forwarder, внутренний DNS-сервер) — перенаправляет полученные рекурсивные запросы вышестоящему кэширующему серверу в виде рекурсивных запросов. Используется преимущественно для снижения нагрузки на кэширующий DNS-сервер.
- Корневой DNS-сервер — сервер, являющийся авторитативным за корневую зону. Общеупотребительных корневых серверов в мире всего 13 штук, их доменные имена находятся в зоне root-servers.net и называются a.root-servers.net, b.root-servers.net, ..., m.root-servers.net. В определённых конфигурациях локальной сети возможна ситуация настройки локальных корневых серверов.
- Регистрирующий DNS-сервер. Сервер, принимающий динамические обновления от пользователей. Часто совмещается с DHCP-сервером. В Microsoft DNS-сервере при работе на контроллере домена сервер работает в режиме регистрирующего DNS-сервера, принимая от компьютеров домена информацию о соответствии имени и IP компьютера и обновляя в соответствии с ней данные зоны домена.
- DNSBL-сервер (сервер с чёрными списками адресов и имён). Формально не входит в иерархию DNS, однако использует те же механизм и протокол работы, что и DNS-серверы.

## 1.2. Особенности работы DNS-сервера

Некоторые серверы поддерживают возможность работать в разных режимах для разных сегментов сети. Например, сервер может для локальных адресов (например, 10.0.0.0/8) отдавать локальные адреса серверов, для пользователей внешней сети — внешние адреса. Так же сервер может быть авторитативным для заданной зоны только для указанного диапазона адресов (например, в сети 10.0.0.0/8 сервер объявляет себя авторитативным за зону internal, при этом для внешних адресов в ответ на запрос имени из зоны internal будет отдаваться ответ «неизвестен»).

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую наличие в имени произвольного количества составных частей.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- com - коммерческие организации (например, microsoft.com);
- edu - образовательные (например, mit.edu);
- gov - правительственные организации (например, nsf.gov);
- org - некоммерческие организации (например, fidonet.org);
- net - организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из

поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени: [www.eltech.ru](http://www.eltech.ru)

### 1.3. Виды DNS-запросов

Прямой запрос. Прямой (forward) запрос — запрос на преобразование имени (символьного адреса) хоста в его IP-адрес. Обратный запрос.

Обратный (reverse) запрос — запрос на преобразование IP-адреса хоста в его имя.

Рекурсивный запрос. Рекурсивный запрос предполагает получение окончательного ответа от сервера, к которому он направлен. Рекурсию выполняет сервер.

Итеративный запрос. Итеративный запрос предполагает (допускает) выполнение рекурсии клиентом.

## 2. Практическая часть. УСТАНОВКА DNS-СЕРВЕРА

2.1. В практической части необходимо выполнить настройку DNS-сервера, используя возможности и ресурсы операционной системы Windows 7.

2.2. В меню «Пуск» надо зайти в «Панель управления». Выберите «Панель управления»

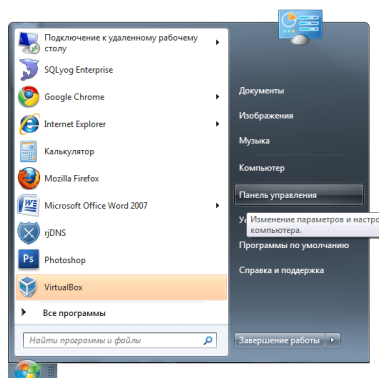


Рис. 5.1.

2.3. Если панель управления имеет сокращённый вид, то в пункте «Сеть и интернет» обратите внимание на «Просмотр состояния сети и задач». Если у вас по умолчанию отображаются все элементы панели управления единым списком, используйте «Центр управления сетями и общим доступом». Выберите «Просмотр состояния сети и задач»

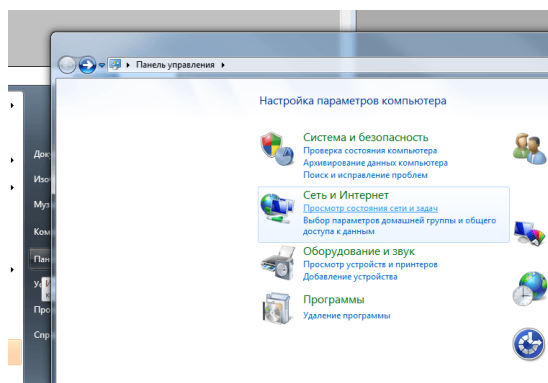


Рис. 5.2.

2.4. В разделе «Просмотр активных сетей» найдите то подключение, благодаря которому вы имеете доступ к интернету (то, что стоит после «Подключения»), и нажмите на него. Выберите подключение

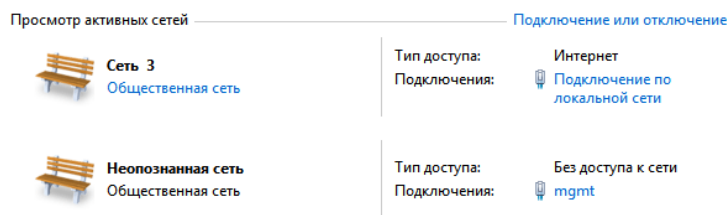


Рис. 5.3.

2.5. Перед вами откроется новое окно, в котором отображаются все настройки выбранного подключения. Нажмите кнопку «Свойства». Нажмите кнопку «Свойства»

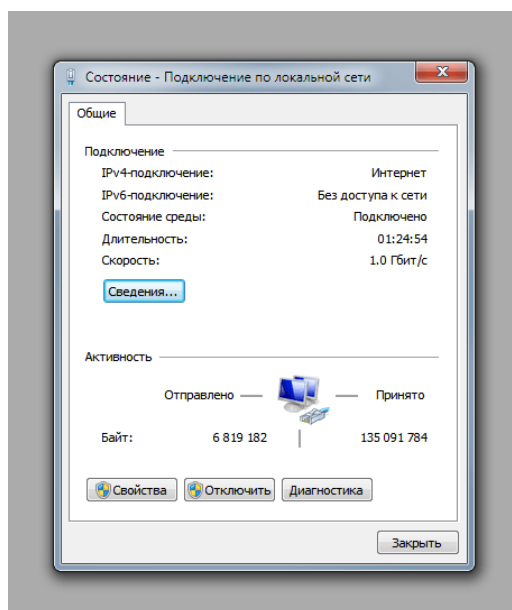


Рис. 5.4.

2.6. Среди отмеченных компонентов, которые используются подключением, найдите «Протокол Интернета версии 4 (TCP/IPv4)» или «Протокол Интернета версии 6 (TCP/IPv6)» и щёлкните по кнопке «Свойства». Выберите «Свойства» для подходящего протокола

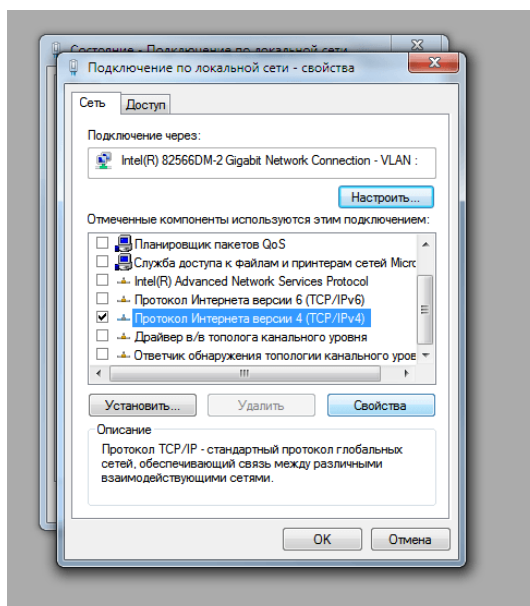


Рис. 5.5.

2.7. Активируйте пункт «Использовать следующие адреса DNS-серверов» и наберите в текстовом поле адрес вашего сервера и дополнительный, если первый окажется неактивным. Введите адрес вашего сервера и альтернативного

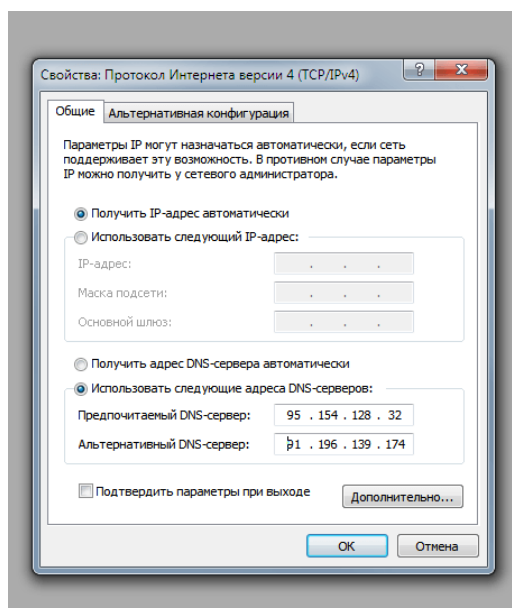


Рис. 5.6.

2.8. Нажмите «ОК», чтобы изменения сохранились.

### 3. Практическая часть. НАСТРОЙКА DNS-СЕРВЕРА

3.1. Прodelайте пункты 2.2 – 2.7 включения DNS.

3.2. Вместо ввода IP-адресов (которые уже есть) нажмите на кнопку «Дополнительно». Нажмите на кнопку «Дополнительно»

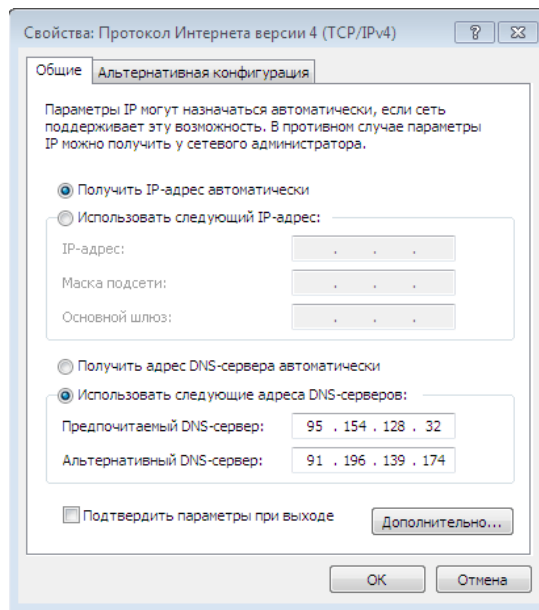


Рис. 5.7.

3.3. В новом открывшемся окне «Дополнительные параметры TCP/IP» перейдите на вкладку DNS. Перейдите на вкладку DNS и измените настройки сервера

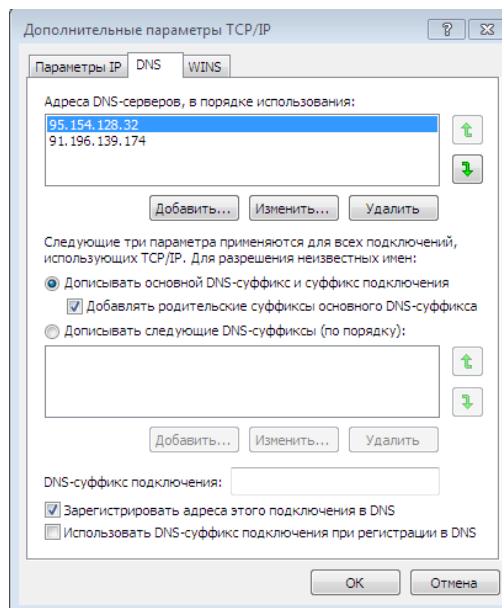


Рис. 5.8.

3.4. Измените настройки и нажмите «ОК», чтобы сохранить их.

#### Контрольные вопросы

1. Дайте определение DNS-сервера.
2. Перечислите типы DNS-серверов, дайте определение авторитативным DNS-серверам.
3. Перечислите особенности кэширующего и перенаправляющего DNS-серверов.
4. В чем заключаются особенности регистрирующего и DNSBL-серверов?
5. Перечислите виды DNS-запросов.

#### Содержание отчета

1. Наименование и цель лабораторной работы
2. Скриншоты выполнения лабораторной работы в соответствии с порядком выполнения практической части работы.
3. Выводы по лабораторной работе.
4. Ответы на контрольные вопросы

## **Лабораторная работа №6 МАРШРУТИЗАЦИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ**

**Цель работы:** Изучить теоретические положения, связанные с маршрутизацией в сетях передачи данных. Выполнить задание в соответствии с вариантом.

### **1.1 Основные теоретические положения**

В процессе организации межсетевого взаимодействия важное место занимает маршрутизация сообщений между отдельными подсетями. При этом под маршрутизацией понимается процесс доставки сообщения из одной подсети в другую. Данная задача может решаться различными способами. При этом, чем сложнее рассматриваемая система, чем больше подсетей ее образуют, тем более нетривиальным является решение задачи доставки сообщений. Сетевой компонент, выполняющий маршрутизацию пакетов, называется маршрутизатором (router). Маршрутизатор может быть реализован на базе компьютера с несколькими сетевыми интерфейсами, на котором установлено специальное программное обеспечение. В этом случае говорят о программном маршрутизаторе. В другом случае маршрутизатор может быть выполнен в виде отдельного сетевого устройства. Разумеется, наиболее эффективным решением является использование специальных аппаратных маршрутизаторов. В настоящее время лидером на рынке корпоративных маршрутизаторов является компания Cisco, предлагающая высокопроизводительные и надежные устройства. В небольших сетях (таких как сеть небольшого офиса или домашняя сеть), использование аппаратного маршрутизатора может быть экономически невыгодно.

В межсетевой среде каждая подсеть может быть соединена с произвольным количеством других подсетей посредством маршрутизаторов. Суть процесса маршрутизации сводится к тому, что два хоста, разделенных друг с другом любым произвольным количеством маршрутизаторов (другими словами, находящиеся в разных подсетях), могут взаимодействовать друг с другом. Всю организацию процесса доставки пакета от одного хоста другому берут на себя маршрутизаторы. Рассмотрим основные принципы, лежащие в основе процесса маршрутизации сообщений. Подавляющее большинство сетевых служб Windows функционирует на базе стека протоколов TCP/IP, получившего широкое распространение именно благодаря простоте организации межсетевого взаимодействия (как известно, самое большое объединение сетей — Интернет, тоже основывается на этом стеке протоколов). Тем не менее, заметим, что в своей основе принципы маршрутизации являются общими для большинства стеков протоколов.

В зависимости от количества вовлеченных получателей стек протоколов TCP/IP поддерживает два способа маршрутизации: одноадресная и многоадресная маршрутизация. Соответственно, мы рассмотрим принципы маршрутизации применительно к каждому из способов в отдельности.

Под одноадресной маршрутизацией понимается процесс передачи сообщений между подсетями, в котором сообщение адресовано только одному заданному получателю. Вся



задача маршрутизации в этом случае сводится к доставке пакета получателю и выбору оптимального маршрута из множества возможных.

Отправителя и получателя может разделять произвольное количество маршрутизаторов. При этом процесс передачи сообщения от одного маршрутизатора другому называется "прыжком" (hop). Каждый маршрутизатор обладает информацией о структуре сети на расстоянии одного прыжка. Другими словами, маршрутизатор не обладает информацией о точном местоположении требуемого хоста. В большой сети, да еще и с интенсивно меняющейся структурой (как, например, Интернет), это было бы невозможно. Вместо этого, маршрутизатор обладает информацией о соседних маршрутизаторах и о том, кому из них необходимо передать сообщение для последующей доставки в той или иной ситуации. Эта информация хранится в специальной таблице, которая носит название таблицы маршрутизации (routing table).

Таблицы маршрутизации используются для принятия решения о том, как именно будет доставлено то или иное сообщение. Наличие этих таблиц не является исключительным свойством маршрутизатора. В сети TCP/IP любой хост (даже не являющийся маршрутизатором) может также располагать таблицей маршрутизации, которая используется с целью определения оптимального маршрута передачи сообщений. Так, скажем, если в подсети имеется три маршрутизатора, хост использует таблицу маршрутизации для того, чтобы выбрать из них наиболее оптимальный для доставки сообщения.

Записи в таблице маршрутизации называются маршрутами. При этом существует три типа маршрутов.

Маршрут к хосту, или узловой маршрут (Host Route). Этот тип маршрута определяет путь доставки пакета, адресованного хосту с конкретным сетевым адресом. Маршруты к хостам обычно используются для создания настраиваемых маршрутов к определенным компьютерам, а также для управления или оптимизации сетевого трафика. Маршрут к сети, или сетевой маршрут (Network Route). Данный тип маршрута используется для определения способа доставки пакета в подсеть с определенным адресом. Большую часть содержимого таблицы маршрутизации представляют собой маршруты данного типа.

Маршрут по умолчанию (Default Route) используется, когда не найдены никакие другие маршруты в таблице маршрутизации. Маршрут по умолчанию используется в ситуации, когда в таблице маршрутизации отсутствует соответствующий маршрут по идентификатору сети или маршрут к хосту по адресу получателя. Маршрут по умолчанию упрощает конфигурацию компьютеров. Вместо конфигурирования компьютера и настройки маршрутов для всех идентификаторов сетей в межсетевой среде используется одиночный маршрут по умолчанию для пересылки всех пакетов в сеть получателя или по адресу в межсетевой среде, который не был найден в таблице маршрутизации.

Рассмотрим структуру таблицы маршрутизации на следующем примере (рисунок 6.1).

```

C:\Documents and Settings\Admin>route print
=====
Список интерфейсов
Их1 ..... MS TCP Loopback interface
Их2 ...00 13 d4 54 9c a9 ..... Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Con
troller - [Имя]ЕЕ яврзЕЕт шьр ярьЕЕт
=====
Активные маршруты:
Сетевой адрес      Маска сети        Адрес шлюза       Интерфейс         Метрика
0.0.0.0            0.0.0.0           10.14.0.3         10.14.1.39        10
10.14.0.0          255.255.128.0     10.14.1.39        10.14.1.39        10
10.14.1.39         255.255.255.255   127.0.0.1         127.0.0.1         10
10.255.255.255    255.255.255.255   10.14.1.39        10.14.1.39        10
127.0.0.0         255.0.0.0         127.0.0.1         127.0.0.1         1
224.0.0.0         240.0.0.0         10.14.1.39        10.14.1.39        10
255.255.255.255   255.255.255.255   10.14.1.39        10.14.1.39        1
Основной шлюз:    10.14.0.3
=====
Постоянные маршруты:
Отсутствует

```

Рисунок 6.1.

Каждая запись в таблице маршрутизации (представляющая собой информацию о маршруте) состоит из информационных полей, перечисленных ниже.

**Сеть назначения (Network Destination).** Данное поле содержит сведения об адресе хоста-получателя пакета или сети, в которой этот хост располагается. Принимая решение о маршрутизации пакета, система просматривает именно это поле. Если в данном поле не будет найдено записи о конкретном адресе сети или хоста, маршрутизатором будет использован маршрут по умолчанию.

**Маска подсети (Netmask).** Это поле в сочетании с предыдущим полем используется для вычисления идентификатора IP-сети.

**Шлюз (Gateway).** В этом поле указывается адрес, по которому будет должен быть передан согласно данному маршруту. Адрес пересылки может быть аппаратным адресом или адресом в межсетевой среде. В большинстве случаев в этом поле указывается следующий в цепочке маршрутизатор, который должен будет принять решение о дальнейшей маршрутизации сообщения.

**Интерфейс (Interface).** В этом поле указывается сетевой интерфейс, с которого будет осуществляться передача сообщения согласно данному маршруту. Данное поле необходимо в ситуации, когда маршрутизатор имеет множество сетевых интерфейсов, подключенных к разным подсетям. Фактически данное поле указывает, в какую именно подсеть необходимо передать сообщение.

**Метрика (Metric).** Стоимость маршрута, характеризующая меру его предпочтения. Из множества альтернативных маршрутов будет выбран тот, что обладает наименьшей стоимостью (т. е. меньшим значением метрики). Некоторые алгоритмы маршрутизации сохраняют только один маршрут для любого идентификатора сети в таблице маршрутизации, даже когда существует несколько маршрутов. В этом случае метрика используется маршрутизатором, чтобы определить какой именно маршрут необходимо сохранить в таблице маршрутизации.

## 1.2 Рабочее задание

Необходимо просмотреть таблицу маршрутизации локального компьютера при помощи утилиты route и выполнить задание в соответствии с вариантом, указанным в таблице 6.1.

Таблица 6.1 – Варианты заданий

Номер варианта	Задание
1	Получить подробную информацию о маршрутах в таблице маршрутизации локального компьютера (ключ PRINT)
2	Добавить маршрут в таблицу маршрутизации (ключ ADD)
3	Добавить маршрут в таблицу маршрутизации (ключ ADD) таким образом, чтобы он остался в таблице после перезагрузки компьютера (ключ -p)
4	Удалить маршрут из таблицы маршрутизации (ключ DELETE)
5	Изменить уже существующий маршрут в таблице маршрутизации (ключ CHANGE)
6	Получить информацию только о конкретном маршруте из таблицы маршрутизации (ключ PRINT)
7	Очистить таблицу маршрутизации от записей для всех шлюзов (ключ -f)

### 1.3 Контрольные вопросы

1. Дайте понятие маршрутизации в сетях передачи данных.
2. Какое устройство выполняет функции маршрутизации в сетях передачи данных?
3. Дайте понятие программного и аппаратного маршрутизатора.
4. Дайте понятие одноадресной маршрутизации.
5. Дайте понятие и опишите назначение таблицы маршрутизации.
6. Опишите три типа маршрутов (записей в таблице маршрутизации): маршрут к хосту, маршрут к сети, маршрут по умолчанию.
7. Назовите все поля и их назначения записи в таблице маршрутизации.

### Лабораторная работа №7 ФОРМАТ И КЛАССЫ IP-АДРЕСОВ

#### Цель работы:

- Изучить эталонную модель протоколов ISO/OSI и стек протоколов TCP/IP;
- Изучить IP-адресацию и правила назначения IP-адресов.

#### Методические указания

*Протокол*– это набор правил, описывающих метод передачи информации по сети. Понятие протокола является исключительно важным для компьютерных сетей. Это связано с тем, что сеть может объединять компьютеры разных типов, работающие под управлением разных операционных систем. Чтобы эти компьютеры могли обмениваться друг с другом информацией, они должны «разговаривать на одном языке», то есть использовать одни и те же протоколы - правила передачи информации по сети.

Стек протоколов TCP/IP является протокольной основой Интернет. Ключевым моментом при этом является IP-адресация.

IP-адрес– это уникальный числовой адрес, однозначно идентифицирующий узел, группу узлов или сеть. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел (так называемых «октетов»), разделенных точками, каждое из которых может принимать значения в диапазоне от 0 до 255, например:

128.10.2.30 - традиционная десятичная форма представления адреса,

10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса по следующим правилам:

- Если адрес начинается с 0, то сеть относят к классу А, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей). В сетях класса А количество узлов должно быть больше 216, но не превышать 224.
- Если первые два бита адреса равны 10, то сеть относится к классу В и является сетью средних размеров с числом узлов 28- 216. В сетях класса В под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В таблице 1 приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Таблица 1

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	$2^{24} \cdot 2$
B	10	128.0.0.0	191.255.0.0	$2^{16} \cdot 2$
C	110	192.0.0.0	223.255.255.0	$2^8 \cdot 2$
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

- если IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;

0 0 0 0 ..... 0 0 0 0

- если в поле номера сети стоят 0, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;

0 0 0 0 .....0 Номер узла

- если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);

1 1 1 1 .....1 1

- если в поле адреса назначения стоят сплошные 1, то пакет, имеющий такой адрес рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);

Номер сети 1111.....11

- адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

Уже упоминавшаяся форма группового IP-адреса - multicast - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения в отличие от широковещательных называются мультивещательными. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

#### Ход работы:

1. Ознакомиться с теоретическими сведениями по теме. Особенно внимательно изучить материал, относящийся к IP-адресации.
2. На основе примера, разобранный для сетей класса А, заполнить третью колонку таблицы 1.
3. Выполнить аналогичные расчеты и заполнить четвертую и пятую колонки таблицы 1.

Для выполнения задания 2 необходимо выполнить следующие действия:

1. Перевести каждое число IP-адреса в двоичную форму. Для перевода можно воспользоваться программой «Калькулятор», установив «Вид/Инженерный».
2. По первым битам IP-адреса определить класс сети.
3. В соответствии с классом определить маску сети по умолчанию.
4. Выписать только те биты IP-адреса, которые соответствуют единичным битам в маске сети. Представить эти биты в точечной нотации. Это будет номер сети.
5. Выписать те биты IP-адреса, которые соответствуют нулевым битам в маске сети. Представить их в точечной нотации. Это будет номер хоста.

6. В двоичном представлении IP-адреса биты, соответствующие номеру хоста, заменить единицами. Представить получившийся адрес в точечной нотации. Это будет широковещательный адрес.

### Задание 1

1. Ознакомьтесь с теоретическими сведениями по теме «Протоколы. IP-адресация».
2. Заполните таблицу 2 «Характеристики сетей различных классов».

Таблица 2

№	Характеристика сети	Класс сети		
		A	B	C
1	2	3	4	5
1	Формат первого байта IP-адреса			
2	Число байтов для номера сети			
3	Число байтов для номера хоста			
4	Минимальный номер сети в точечной нотации			
5	Максимальный номер сети в точечной нотации			
6	Число различных сетей			
7	Минимальный номер хоста в точечной нотации			
8	Максимальный номер хоста в точечной нотации			
9	Число различных хостов			
10	Маска сети по умолчанию			

1. Для IP-адреса, указанного в индивидуальном задании, считая, что маска сети задана по умолчанию, определите:
  1. Класс сети;
  2. Число сетей в этом классе;
  3. Маску сети по умолчанию;
  4. Номер сети;
  5. Номер хоста;
  6. Минимальный номер сети;
  7. Максимальный номер сети;

8. Широковещательный адрес.

2. Используя маску, указанную в индивидуальном задании, определите

1. Число хостов;
2. Маску сети (в десятичной нотации);
3. Номер сети;
4. Номер хоста;
5. Минимальный номер хоста;
6. Максимальный номер хоста;
7. Широковещательный адрес.

### Пример выполнения задания 2

Пусть IP-адрес 64.10.20.30

Переводим числа в двоичный формат:

$64_{10} = 01000000_2$

$10_{10} = 00001010_2$

$20_{10} = 00010100_2$

$30_{10} = 00011110_2$

Записываем двоичную форму представления IP-адреса:

01000000.00001010.00010100.00011110

Первые биты адреса – 01, значит, это сеть класса А.

Маска сети по умолчанию: 255.0.0.0

Записываем в двоичной форме маску сети и IP-адрес:

Маска: 11111111.00000000.00000000.00000000

IP-адрес: 01000000.00001010.00010100.00011110

---

Эти биты А эти биты

соответствуют    соответствуют

номеру сети        номеру хоста

Значит, номер сети -  $01000000_2$  или  $64_{10}$

номер хоста -  $00001010.00010100.00011110_2$  или  $10.20.30_{10}$

Заменяем в IP-адресе номер хоста единицами, получим широковещательный адрес 01000000.111111.111111.111111<sub>2</sub>или 64.255.255.255

Следовательно:

IP-адрес 64.10.20.30

Класс сети А

Маска сети 255.0.0.0

Номер сети 64

Номер хоста 10.20.30

Широковещательный адрес 64.255.255.255

При выполнении задания 3 по индивидуальному варианту (таблица 3) необходимо вначале определить маску сети. Маска содержит столько единичных битов, сколько указано в числе после дробной черты. Остальные вычисления выполняются подобно заданию 2.

### **Контрольные вопросы**

1. Что такое протокол?
2. Назовите уровни модели протоколов модели ISO/OSI и назначение протоколов каждого уровня.
3. Назовите уровни стека протоколов TCP/IP и назначение протоколов каждого уровня.
4. Приведите примеры протоколов, входящих в стек TCP/IP.
5. Что такое IP-адрес?
6. Каковы правила назначения IP-адресов?
7. Как проанализировать IP-адрес?

### **Варианты индивидуальных заданий**

Таблица 3

№	IP-адрес к заданию 3	IP-адрес к заданию 4
1.	192.168.72.33	192.168.72.33/20
2.	190.172.55.40	190.172.55.40/21
3.	123.232.14.72	123.232.14.72/18
4.	196.232.66.54	196.232.66.54/25
5.	193.123.55.67	193.123.55.67/26



6.	191.172.55.42	191.172.55.42/20
7.	178.66.57.18	178.66.57.18/20
8.	10.0.0.20	10.0.0.20/12
9.	67.192.44.89	67.192.44.89/12
10.	128.34.67.11	128.34.67.11/18
11.	193.34.126.44	193.34.126.44/26
12.	156.32.11.93	156.32.11.93/23
13.	167.168.169.170	167.168.169.17/20
14.	145.44.11.77	145.44.11.77/22
15.	132.45.171.99	132.45.171.99/26
16.	198.164.55.55	198.164.55.55/26
17.	192.77.121.144	192.77.121.144/25
18.	12.13.14.15	12.13.14.15/19
19.	44.57.62.39	44.57.62.39/18
20.	152.15.66.5	152.15.66.5/20
21.	132.45.171.99	132.45.171.99/27
22.	198.164.155.5	198.164.155.5/26
23.	192.77.11.44	192.77.11.44/29
24.	12.130.140.150	12.130.140.150/14
25.	44.57.162.31	44.57.162.31/18
26.	152.154.66.65	152.154.66.65/20
27.	152.15.66.17	152.15.66.17/22
28.	132.45.171.88	132.45.171.88/21

### **Лабораторная работа №8 ПОДСЕТИ И МАСКИ ПОДСЕТЕЙ**

#### **Цели работы:**

- научиться определять адрес подсети и адрес хоста по маске подсети;
- научиться определять количество и диапазон адресов возможных узлов в подсетях;
- научиться структурировать сети с использованием масок.

**Задание 1.** Определить, находятся ли два узла А и В в одной подсети или в разных подсетях, если адреса компьютера А и компьютера В соответственно равны: 26.219.123.6 и 26.218.102.31, маска подсети 255.192.0.0.

### Указания к выполнению

1. Переведите адреса компьютеров и маску в двоичный вид.
2. Для получения двоичного представления номеров подсетей обоих узлов выполните операцию логического умножения AND над IP-адресом и маской каждого компьютера.
3. Двоичный результат переведите в десятичный вид.
4. Сделайте вывод.

Процесс решения можно записать следующим образом:

Компьютер А:

IP-адрес: 26.219.123.6 = 00011010. 11011011. 01111011. 00000110

Маска подсети: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Компьютер В:

IP-адрес: 26.218.102.31 = 00011010. 11011010. 01100110. 00011111

Маска подсети: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Получаем номер подсети, выполняя операцию AND над IP-адресом и маской подсети.

Компьютер А:

00011010. 11011011. 01111011. 00000110

AND

11111111. 11000000. 00000000. 00000000

-----  
00011010. 11000000. 00000000. 00000000

26        192        0        0

Компьютер В:

00011010. 11011010. 01100110. 00011111

AND

11111111. 11000000. 00000000. 00000000

-----  
00011010. 11000000. 00000000. 00000000

26        192        0        0

Ответ: номера подсетей двух IP-адресов совпадают, значит компьютеры А и В находятся в одной подсети. Следовательно, между ними возможно установить прямое соединение без применения шлюзов.

**Задание 2.** Определить количество и диапазон IP-адресов в подсети, если известны номер подсети и маска подсети. Номер подсети – 26.219.128.0, маска подсети – 255.255.192.0.

### Указания к выполнению

1. Переведите номер и маску подсети в двоичный вид.

Номер подсети: 26.219.128.0 = 00011010. 11011011. 10000000. 00000000

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

2. По маске определите количество бит, предназначенных для адресации узлов (их значение равно нулю). Обозначим их буквой К.

3. Общее количество адресов равно  $2K$ . Но из этого числа следует исключить комбинации, состоящие из всех нулей или всех единиц, так как данные адреса являются особыми. Следовательно, общее количество узлов подсети будет равно  $2K - 2$ . В рассматриваемом примере  $K = 14$ ,  $2K - 2 = 16\ 382$  адресов.

4. Чтобы найти диапазон IP-адресов нужно найти начальный и конечный IP-адреса подсети. Для этого выделите в номере подсети те биты, которые в маске подсети равны единице. Это разряды, отвечающие за номер подсети. Они будут совпадать для всех узлов данной подсети, включая начальный и конечный:

Номер подсети: 26.219.128.0 = 00011010. 11011011. 10000000. 00000000

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

5. Чтобы получить начальный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить нулями, за исключением крайнего правого бита, который должен быть равен единице. Полученный адрес будет первым из допустимых адресов данной подсети:

Начальный адрес: 26.219.128.1 = 00011010. 11011011. 10000000. 00000001

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

6. Чтобы получить конечный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить единицами, за исключением крайнего правого бита, который должен быть равен нулю.

Полученный адрес будет последним из допустимых адресов данной подсети:

Конечный адрес: 26.219.191.254 = 00011010. 11011011. 10111111. 11111110

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

Ответ: Для подсети 26.219.128.0 с маской 255.255.192.0: количество возможных адресов: 16 382, диапазон возможных адресов: 26.219.128.1 – 26.219.191.254.

**Задание 3.** Организации выделена сеть класса С: 212.100.54.0/24. Требуется разделить данную сеть на 4 подсети с количеством узлов в каждой не менее 50. Определить маски и количество возможных адресов новых подсетей.

### Указания к выполнению

1. В сетях класса С (маска содержит 24 единицы – 255.255.255.0) под номер узла отводится 8 бит, т. е. сеть может включать  $2^8 - 2 = 254$  узла.

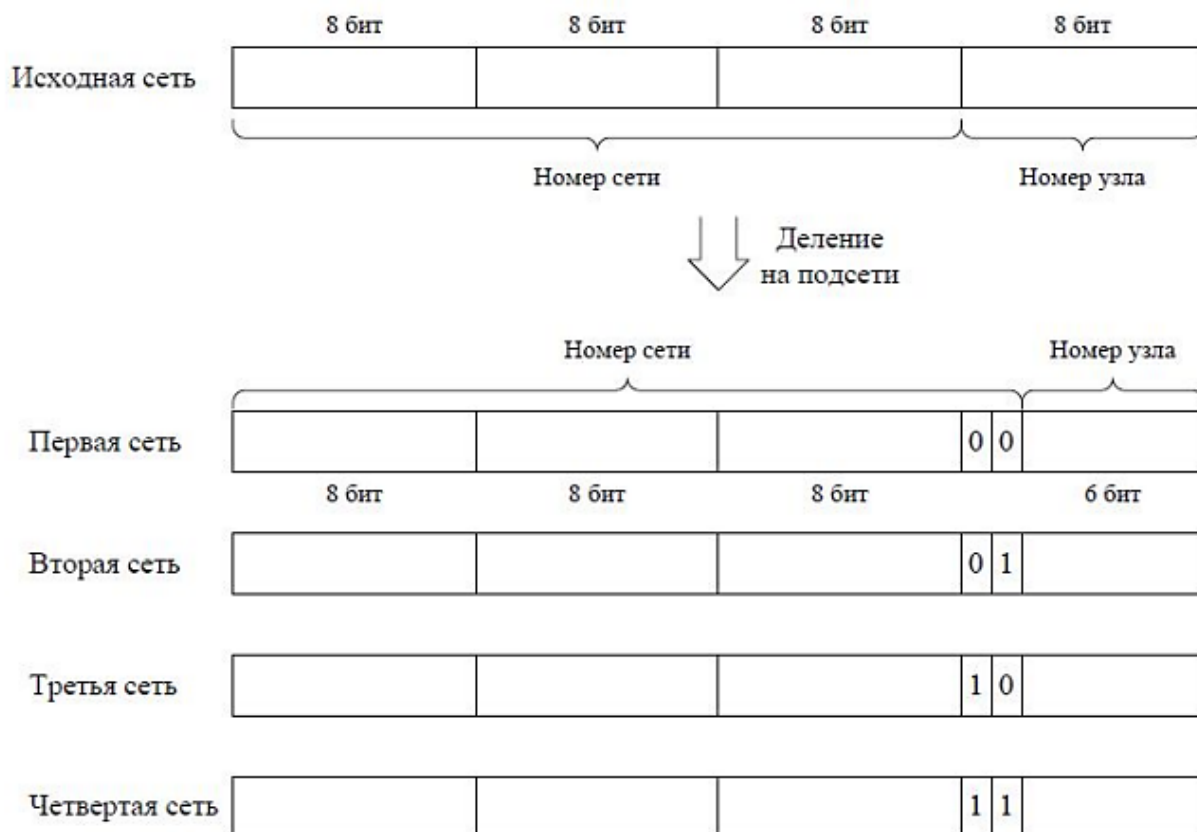
2. Требование деления на 4 подсети по 50 узлов в каждой может быть выполнено:  $4 \cdot 50 = 200 < 254$ . Однако число узлов в подсети должно быть кратно степени двойки.

Относительно 50 ближайшая большая степень –  $2^6 = 64$ . Следовательно, для номера узла нужно отвести 6 бит, вместо 8, а маску расширить на 2 бита – до 26 бит (см. рис.).

3. В этом случае вместо одной сети с маской 255.255.255.0 образуется 4 подсети с маской 255.255.255.192 и количеством возможных адресов в каждой – 62 (не забывайте про два особых адреса).

4. Номера новых подсетей отличаются друг от друга значениями двух битов, отведенных под номер подсети. Эти биты равны 00, 01, 10, 11.

Ответ: маска подсети – 255.255.255.192, количество возможных адресов – 62



### Самостоятельная работа

**Задание 1.** Определить, находятся ли два узла А и В в одной подсети или в разных подсетях.

1. IP-адрес компьютера А: 94.235.16.59; IP-адрес компьютера В: 94.235.23.240; Маска подсети: 255.255.240.0.
2. IP-адрес компьютера А: 131.189.15.6; IP-адрес компьютера В: 131.173.216.56; Маска подсети: 255.248.0.0.
3. IP-адрес компьютера А: 215.125.159.36; IP-адрес компьютера В: 215.125.153.56; Маска подсети: 255.255.224.0.

**Задание 2.** Определить количество и диапазон адресов узлов в подсети, если известны номер подсети и маска подсети.

1. Номер подсети: 192.168.1.0, маска подсети: 255.255.255.0.
2. Номер подсети: 110.56.0.0, маска подсети: 255.248.0.0.

3. Номер подсети: 88.217.0.0, маска подсети: 255.255.128.0.

**Задание 3.** Определить маску подсети, соответствующую указанному диапазону IP-адресов.

1. 119.38.0.1 – 119.38.255.254.
2. 75.96.0.1 – 75.103.255.254.
3. 48.192.0.1 – 48.255.255.254.

**Задание 4.** Организации выделена сеть класса В: 185.210.0.0/16. Определить маски и количество возможных адресов новых подсетей в каждом из следующих вариантов разделения на подсети:

1. Число подсетей – 256, число узлов – не менее 250.
2. Число подсетей – 16, число узлов – не менее 4000.
3. Число подсетей – 5, число узлов – не менее 4000. В этом варианте укажите не менее двух способов решения.

### **Контрольные вопросы**

1. Может ли быть IP-адрес узла таким? Укажите неверные варианты IP-адрес. Ответ обоснуйте. – 192.168.255.0 – 167.234.56.13 – 224.0.5.3 – 172.34.267.34 – 230.0.0.7 – 160.54.255.255
2. Может ли маска подсети быть такой? Укажите неверные варианты. Ответ обоснуйте. – 255.254.128.0 – 255.255.252.0 – 240.0.0.0 – 255.255.194.0 – 255.255.128.0 – 255.255.255.244 – 255.255.255.255
3. Можно ли следующие подсети разделить на N подсетей. Если это возможно, то укажите варианты разбиения с максимально возможным количеством подсетей или узлов в каждой подсети. Ответ обоснуйте.
  - 165.45.67.0, маска 255.255.255.224, N=3
  - 235.162.56.0, маска 255.255.255.224, N=6
  - 234.49.32.0, маска 255.255.255.192, N=3

## СПИСОК ЛИТЕРАТУРЫ

1. Топорков, С. С. Компьютерные сети для продвинутых пользователей / Топорков С. С. - М : ДМК Пресс. - 192 с. (Серия "С компьютером на ты!"). URL : <https://www.studentlibrary.ru/book/ISBN5940740936.html> (дата обращения: 10.03.2025).
2. Проскуряков, А. В. Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / Проскуряков А. В. - Ростов н/Д : Изд-во ЮФУ. URL : <https://www.studentlibrary.ru/book/ISBN9785927527922.html> (дата обращения: 10.03.2025).
3. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. – М. ; Вологда : Инфра-Инженерия. URL : <https://znanium.com/catalog/product/1902692> (дата обращения: 10.03.2025).