

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Защита в операционных системах

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

Настройка начальных параметров коммутатора,
(тема отчета)

Направление/специальность подготовки

10.05.02. «Информационная безопасность телекоммуникационных систем»

(код и наименование направления/специальности)

Студентка:

Иванова А. У. ИБС-12 _____

(Ф.И.О.) (№ группы) (подпись)

Преподаватель:

Беккель Л. С. _____

(Ф.И.О.) (подпись)

Оглавление

Оглавление

Задание 2.2.3.4. Настройка начальных параметров коммутатора.....	3
Задание 1.2.4.5. Представление сети.....	17
Задание 2.1.4.6. Навигация по IOS.....	22
Вывод.....	35

Задание 2.2.3.4. Настройка начальных параметров коммутатора

Задачи:

Часть 1. Проверка конфигурации коммутатора по умолчанию

Часть 2. Настройка основных параметров коммутатора

Часть 3. Настройка баннера MOTD (сообщения дня)

Часть 4. Сохранение файлов конфигурации в NVRAM

Часть 5. Настройка коммутатора S2

Часть 1. Проверка конфигурации коммутатора по умолчанию

Шаг 1. Войдите в привилегированный режим EXEC.

Привилегированный режим EXEC дает доступ ко всем командам коммутатора. Но поскольку многие привилегированные команды задают рабочие параметры, привилегированный доступ должен быть защищен паролем во избежание несанкционированного использования.

Набор команд привилегированного режима EXEC включает команды, которые доступны в пользовательском режиме EXEC, а также команду **configure**, открывающую доступ к остальным командным режимам.

А. Щелкните **S1**, а затем вкладку **CLI**. Нажмите клавишу ввода.

Б. Перейдите в привилегированный режим EXEC, выполнив команду **enable**. (рис.1)

Команда для ввода: «Switch> enable»

```
Switch>enable  
Switch#
```

(Рис.1 Результат ввода команды «Switch> enable» в коммутаторе S1)

Результат: Switch#

Обратите внимание, что командная строка изменилась, отображая переключение в привилегированный режим EXEC.

Шаг 2. Изучите текущую конфигурацию коммутатора.

A. Введите команду **show running-config**.

```
Switch# show running-config
```

Б. Ответьте на следующие вопросы.

1. Сколько у коммутатора интерфейсов FastEthernet?

Ответ: 24

2. Сколько у коммутатора интерфейсов Gigabit Ethernet?

Ответ: 2

3. Каков диапазон значений, отображаемых в линиях vty?

Ответ: 0-15

4. Какая команда отображает текущее содержимое энергонезависимого ОЗУ (NVRAM)?

Ответ: startup-config is not present

5. Почему коммутатор отвечает сообщением startup-config is not present?

Ответ: Потому что файл конфигурации не был сохранен в ПЗУ

Часть 2. Настройка основных параметров коммутатора

Шаг 1. Присвойте коммутатору имя. (рис.2)

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки. Обратите внимание, как изменяется командная строка при переходе между режимами командной строки коммутатора.

Команды для ввода:

«Switch# configure terminal».

«Switch(config)# hostname S1».

«S1(config)# exit».

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

(Рис.2 Присвоение коммутатору имя S1)

Шаг 2. Обеспечьте безопасный доступ к консоли.

Для безопасного доступа к консоли перейдите в режим config-line и установите для консоли пароль **letmein**. (рис.3)

Команды для ввода:

«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#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
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

(Рис.3 Обеспечение безопасного доступа к консоли, установка пароля в коммутаторе S1)

Для чего нужна команда **login**?

Ответ: Команда login настраивает коммутатор для аутентификации при входе в систему. Если включена процедура входа и настроен пароль, пользователь консоли должен будет ввести пароль, чтобы получить доступ к интерфейсу командной строки Введите ваш ответ здесь.

Шаг 3. Убедитесь, что доступ к консоли защищен.

Выйдите из привилегированного режима, чтобы убедиться, что для консольного порта установлен пароль. (рис.4)

Команда для ввода:

«S1# **exit**»

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

```
S1#exit

S1 con0 is now available

Press RETURN to get started.

|

User Access Verification
Password:
```

(Рис 4. Проверка установления пароля для консольного порта в коммутаторе S1)

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

Шаг 4. Защитите доступ к привилегированному режиму.

Установите для **enable** пароль **c1\$c0**. Этот пароль ограничивает доступ к привилегированному режиму. (рис.5)

Примечание. Символ **0** в **c1\$c0** — это ноль, а не заглавная буква «O». Настройка пароля будет оценена как выполненная успешно только после того как вы зашифруете его на шаге 8.

Команды для ввода:

```
«S1> enable»
```

```
«S1# configure terminal»
```

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

```
«S1(config)# exit»
```

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

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password c1$c0
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

(Рис.5 Установка пароля, ограничивающего доступ к привилегированному режиму в коммутаторе S1)

Шаг 5. Убедитесь, что доступ к привилегированному режиму защищен.

А. Введите команду **exit** еще раз, чтобы выйти из коммутатора.

Б. Нажмите **<Enter>**, после чего вам будет предложено ввести пароль.

User Access Verification

Password:

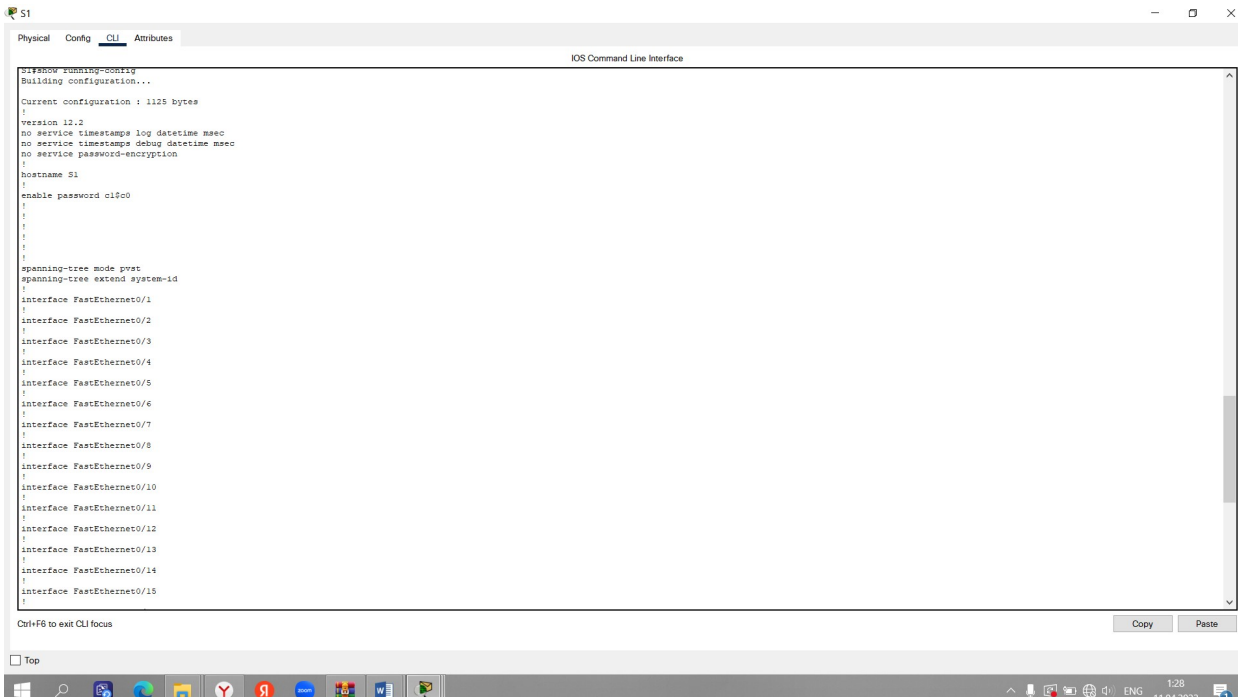
В. Первый пароль — это пароль для консоли, который был задан для **line con 0**. Введите этот пароль, чтобы вернуться в пользовательский режим EXEC.

Г. Введите команду для доступа к привилегированному режиму.

Д. Введите второй пароль, который был задан для ограничения доступа к привилегированному режиму EXEC.

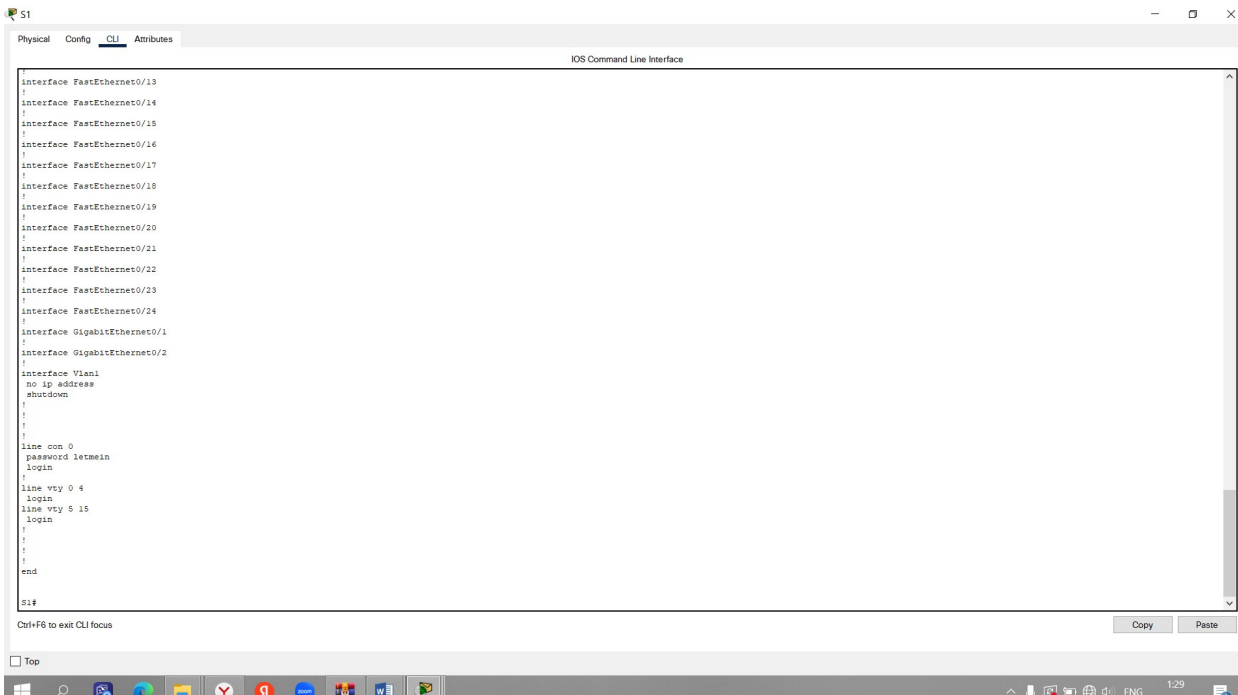
Е. Проверьте конфигурацию, изучив содержимое файла running-configuration. (рис.6-7)

Команда для ввода: «S1# **show running-config**»



```
IOS Command Line Interface
Building configuration...
Current configuration : 1125 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
enable password c1$c0
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
Ctrl+F6 to exit CLI focus
```

(Рис.6 Содержимое файла running-configuration в коммутаторе S1)



```
IOS Command Line Interface
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
password letmein
login
!
!
line vty 0 4
login
line vty 5 15
login
!
!
!
end
S1#
Ctrl+F6 to exit CLI focus
```

(Рис.7 Содержимое файла running-configuration в коммутаторе S1)

Обратите внимание, что пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может быть небезопасно, так как пароль может увидеть любой находящийся рядом человек.

Шаг 6. Настройте зашифрованный пароль для защиты доступа к привилегированному режиму.

Пароль **enable password** нужно заменить на новый зашифрованный пароль с помощью команды **enable secret**. Установите для **enable secret** пароль **itsasecret**. (рис.8)

Команды для ввода:

«S1# **config t**»

«S1(config)# **enable secret itsasecret**»

«S1(config)# **exit**»

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret itsasecret
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#|
```

(Рис.8 Настройка зашифрованного пароля для защиты доступа к привилегированному режиму в коммутаторе S1)

Примечание. Пароль **enable secret** имеет приоритет перед паролем **enable password**. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим EXEC нужно ввести пароль **enable secret**.

Шаг 7. Убедитесь, что в файл конфигурации добавлен пароль enable secret.

А. Введите команду **show running-config** еще раз, чтобы проверить новый пароль **enable secret**. (рис.9)

Примечание. Команду **show running-config** можно сократить до

Команда для ввода:

«S1# **show run**»

```
S1#show run
Building configuration...

Current configuration : 1172 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password c1$c0
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

(Рис.9 Проверка установления пароля enable secret в файл конфигурации в коммутаторе S1)

Б. Что отображается при выводе пароля enable secret?

Ответ: 5 \$1\$mERr\$ILwq/b7kc/7X/ejA4osn0

В. Почему пароль enable secret отображается не так, как задан?

Ответ: Он хранится в зашифрованном виде. Команда «enable secret» обеспечивает большую безопасность, потому что пароль шифруется.

Шаг 8. Зашифруйте пароли enable и console.

Как было видно в шаге 7, пароль **enable secret** зашифрован, а пароли **enable password** и **console** хранятся в виде обычного текста. Сейчас мы зашифруем эти открытые пароли с помощью команды **service password-encryption**. (рис.10)

Команды:

«S1# **config t**»

«S1(config)# **service password-encryption**»

«S1(config)# **exit**»

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#|
```

(Рис.10 Шифрование открытых паролей enable и console в коммутаторе S1)

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

Ответ: Команда service password-encryption шифрует все текущие и будущие пароли.

Часть 3. Настройка баннера MOTD (сообщения дня)

Шаг 1. Настройте баннер MOTD (сообщения дня).

В набор команд Cisco IOS входит команда, позволяющая настроить сообщение, которое будут видеть все, кто входит в систему на коммутаторе. Это сообщение называется сообщением дня или баннером MOTD (message of the day). Текст баннера нужно заключить в двойные кавычки или использовать разделитель, отличный от любого символа в строке MOTD. (рис.11)

Команды:

```
«S1# config t»
```

```
«S1(config)# banner motd "This is a secure system. Authorized Access Only!"»
```

```
«S1(config)# exit»
```

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

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#banner motd "This is a secure system. Authorized Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#|
```

(Рис.11 Настройка баннера MOTD в коммутаторе S1)

1. Когда будет отображаться этот баннер?

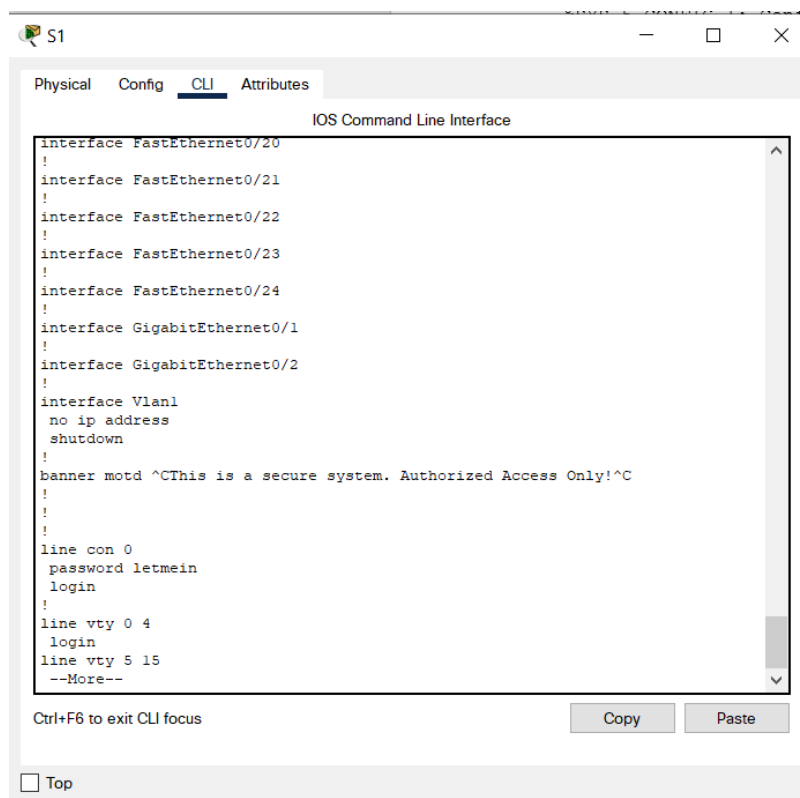
Ответ: Баннер будут отображаться, когда кто-то получит доступ к коммутатору через консольный порт.

2. Зачем на всех коммутаторах должен быть баннер MOTD?

Ответ: это предупреждение для пользователя.

Часть 4. Сохранение файлов конфигурации в NVRAM

Шаг 1. Проверьте правильность конфигурации с помощью команды «show run.» (рис.12)



(Рис.12 Проверка правильности конфигурации в коммутаторе S1)

Шаг 2. Сохраните файл конфигурации.

Вы завершили основную настройку коммутатора. Теперь выполните резервное копирование файла конфигурации в NVRAM и убедитесь, что внесенные изменения не были потеряны при перезагрузке системы или отключении питания. (рис.13)

Команды:

«S1# copy running-config startup-config»

Destination filename [startup-config]?[Enter]

Building configuration...

[OK]

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

(Рис.13 Сохранение файлов конфигурации в коммутаторе S1)

Какова самая короткая версия команды copy running-config startup-config?

Ответ: Copy run start.

Шаг 3. Изучите файл загрузочной конфигурации.

Какая команда отображает содержимое NVRAM?

Ответ: show startup-config.

Все ли внесенные изменения были записаны в файл?

Ответ: да.

Часть 5. Настройка коммутатора S2

Вы завершили настройку коммутатора S1. Теперь настройте коммутатор S2. Если вы не можете вспомнить команды, вернитесь к частям 1–4.

Настройте для коммутатора S2 следующие параметры.

A. Имя устройства: S2. (рис.14)

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#exit
S2#
```

(Рис.14 Настройка имени устройства S2)

Б. Защитите доступ к консоли паролем letmein. (рис.15)

```
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#exit
S2(config)#exit
S2#
```

(Рис.15 Защита доступа к консоли, установка пароля в коммутаторе S2)

В. Задайте пароль enable password c1\$c0 и пароль enable secret itsasecret.
(рис.16-17)

```
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#enable password c1$c0
S2(config)#exit
S2#
```

(Рис.16 Настройка пароля enable password c1\$c0 в коммутаторе S2)

```
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#enable secret itsasecret
S2(config)#exit
S2#
```

(Рис.17 Настройка пароля enable secret itsasecret в коммутаторе S2)

Г. Введите следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе:

«Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law». (рис.18)


```

S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Authorized access only/ Unauthorized access is
prohibited and violators will be prosecuted to full extent of the law."
S2(config)#exit
S2#

```

(Рис.18 Настройка сообщения для пользователей в коммутаторе S2)

Д. Зашифруйте все открытые пароли. (Рис.19)

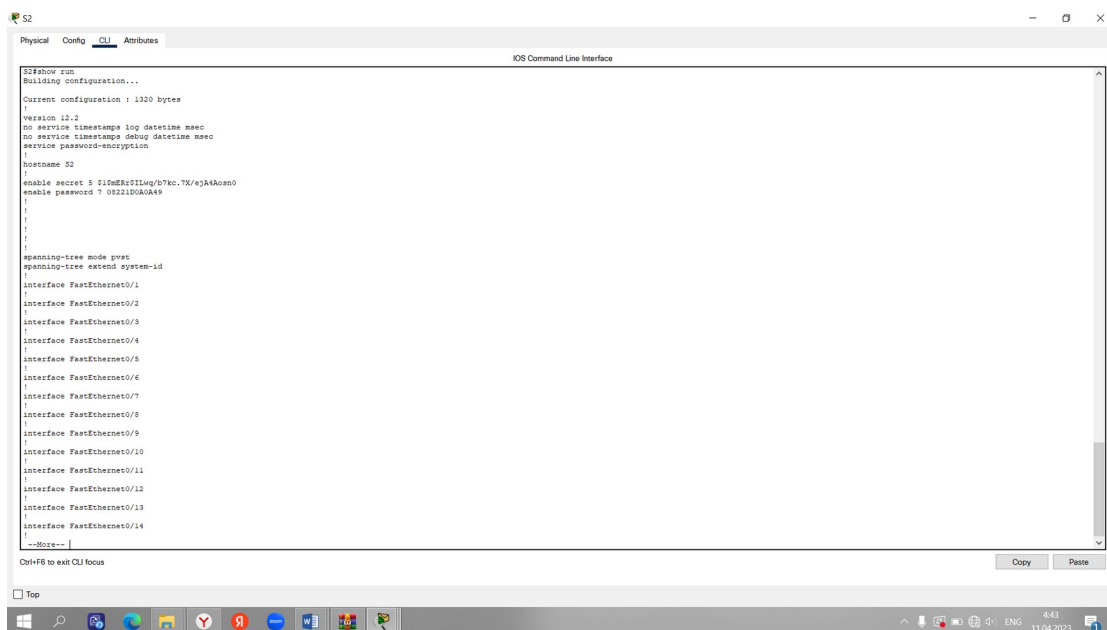
```

S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#service password-encryption
S2(config)#exit
S2#

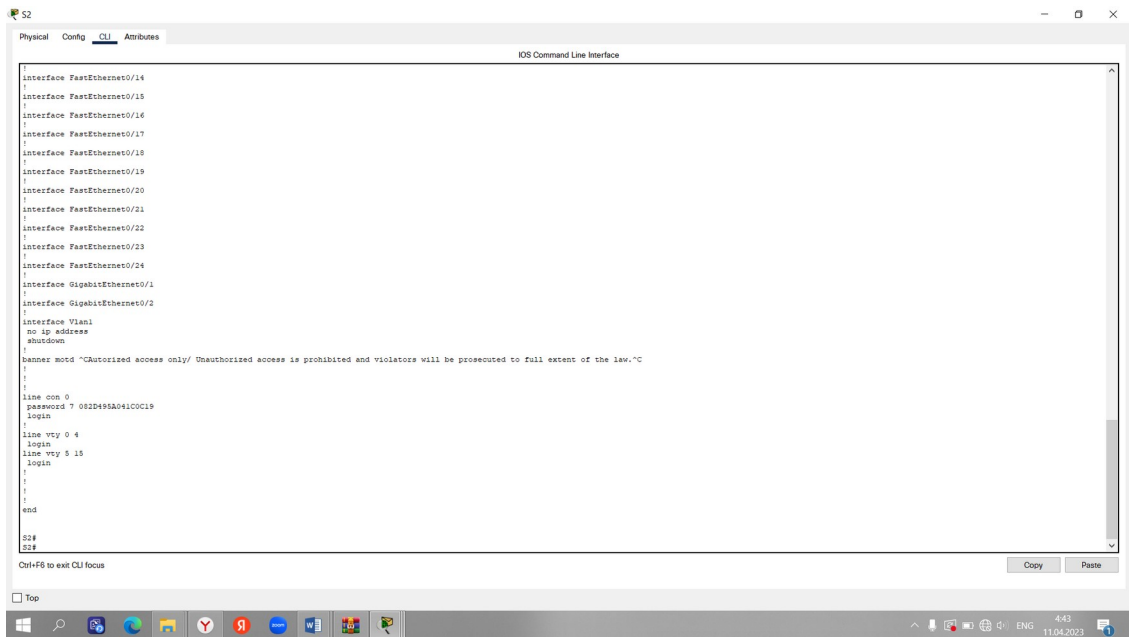
```

(Рис.19 Шифрование всех открытых паролей на коммутаторе S2)

Е. Проверьте правильность конфигурации. (рис.20-21)



(Рис.20 Проверка правильности конфигурации в коммутаторе S2)



(Рис.21 Проверка правильности конфигурации в коммутаторе S2)

Ж. Сохраните файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора. (рис.22)

```
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

(Рис.22 Сохранение файла конфигурации в коммутаторе S2)

Задание 2.3.2.5. Обеспечение базовой связности.

Таблица адресации:

Устройство	интерфейс	IP-адрес	Subnet Mask (Маска подсети)
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0

PC2	NIC	192.168.1.2	255.255.255.0
-----	-----	-------------	---------------

Задачи

Часть 1. Базовая настройка коммутаторов S1 и S2

Часть 2. Настройка ПК

Часть 3. Настройка интерфейса управления коммутатором.

Часть 1. Базовая настройка коммутаторов S1 и S2

Выполните следующие действия на коммутаторах S1 и S2.

Шаг 1. Настройте имя узла для коммутатора S1.

А. Щелкните S1 и откройте вкладку CLI.

Б. Введите нужную команду, чтобы присвоить узлу имя S1.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#exit
S2#
```

Шаг 2. Настройте пароли для консоли и привилегированного режима EXEC.

А. В качестве пароля для консоли введите **cisco**.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
S1#
```

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#exit
S2#
```

Б. В качестве пароля для привилегированного режима EXEC введите **class**.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password class
S1(config)#exit
S1#
```

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#enable password class
S2(config)#exit
S2#
```

Шаг 3. Проверьте пароли, настроенные для коммутатора S1.

```
hostname S1
!
enable password class
'

line con 0
 password cisco
 login

hostname S2
!
enable password class
```

```
line con 0
 password cisco
 login
```

Как можно проверить правильность настройки паролей?

Ответ: После выхода из пользовательского режима EXEC коммутатор запросит у вас пароль для доступа к интерфейсу консоли и предложит вам второй раз при доступе к привилегированному режиму EXEC. Вы также можете использовать команду **показать выполнение** для просмотра паролей.

Шаг 4. Настройте баннер MOTD

Введите текст предупреждения о несанкционированном доступе. Ниже представлен пример текста.

Authorized access only. Violators will be prosecuted to the full extent of the law.

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#banner motd "Authorized access only. Violators will be prosecuted
to the full extent of the law."
S1(config)#exit
S1#
```

```
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Authorized access only. Violators will be prosecuted
to the full extent of the law."
S2(config)#exit
S2#
```

Шаг 5. Сохраните файл конфигурации в NVRAM.

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Какую команду необходимо для этого выполнить?

Ответ: S1# copy running-config startup-config (copy run start)

Шаг 6. Повторите шаги 1–5 для коммутатора S2.

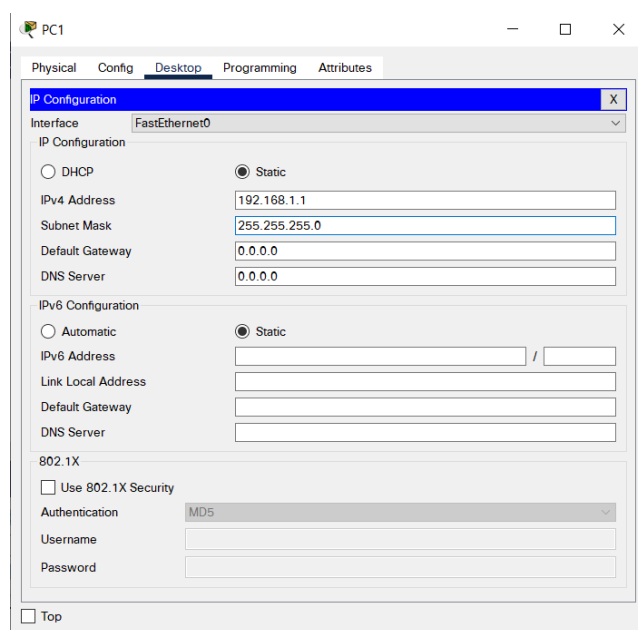
Часть 2. Настройка ПК

Настройте IP-адрес для PC1 и PC2.

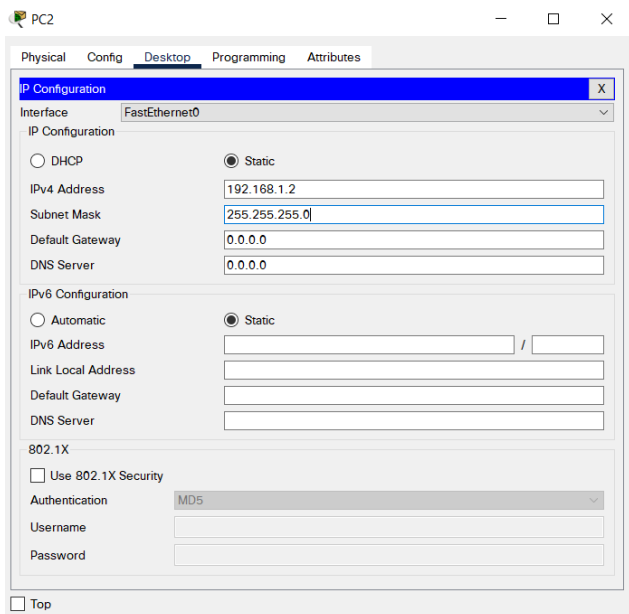
Шаг 1. Настройте IP-адреса для обоих ПК.

А. Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол).

Б. Выберите **IP Configuration** (Настройка IP-адресов). В таблице адресации выше можно увидеть, что PC1 назначен IP-адрес 192.168.1.1 и маска подсети 255.255.255.0. Введите эти данные для PC1 в окне **IP Configuration** (Настройка IP-адресов).



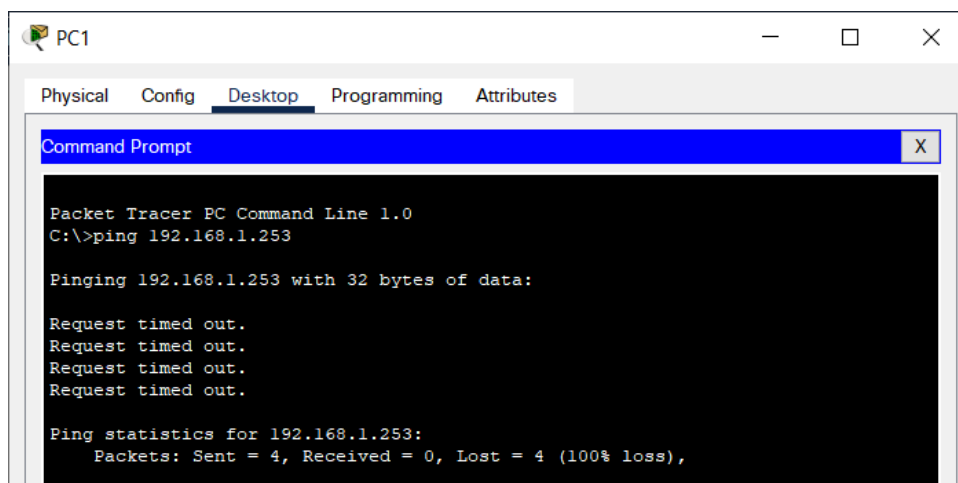
В. Повторите шаги 1а и 1б для компьютера PC2.



Шаг 2. Проверьте подключение к коммутаторам.

А. Щелкните PC1. Закройте окно **IP Configuration** (Настройка IP-адресов), если оно открыто. На вкладке **Desktop** (Рабочий стол) нажмите **Command Prompt** (Командная строка).

Б. Введите команду **ping** с IP-адресом коммутатора S1 и нажмите клавишу ВВОДА.



Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

Был ли эхо-запрос обработан успешно? Дайте пояснение.

Ответ: Нет, поскольку коммутаторы не были настроены с IP-адресом.

Часть 3. Настройка интерфейса управления коммутатором

Настройте IP-адреса для коммутаторов S1 и S2.

Шаг 1. Настройте IP-адрес для коммутатора S1.

Коммутаторы можно использовать в режиме «plug & play». Это значит, что они могут начать работать и без предварительной настройки. Коммутаторы пересылают данные между портами, опираясь на MAC-адреса. Для чего тогда нужно настраивать IP-адреса?

Ответ: Для удаленного подключения к коммутатору необходимо назначить ему IP-адрес. Конфигурация по умолчанию на коммутаторе заключается в том, чтобы управление коммутатором осуществлялось через VLAN 1.

Чтобы настроить IP-адрес на коммутаторе S1, используйте следующие команды.

```
S1# configure terminal
```

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

```
S1(config)# interface vlan 1
```

```
S1(config-if)# ip address 192.168.1.253 255.255.255.0
```

```
S1(config-if)# no shutdown
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state  
to up
```

```
S1(config-if)#
```

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

```
S1#
```



```

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.253 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#

```

Зачем вы вводите команду **no shutdown**?

Ответ: Команда **no shutdown** административно переводит интерфейс в активное состояние.

Шаг 2. Настройте IP-адрес для коммутатора S2.

Используя данные из таблицы адресации, настройте IP-адрес для S2.

```

S2#configure terminal
^
% Invalid input detected at '^' marker.

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.254 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

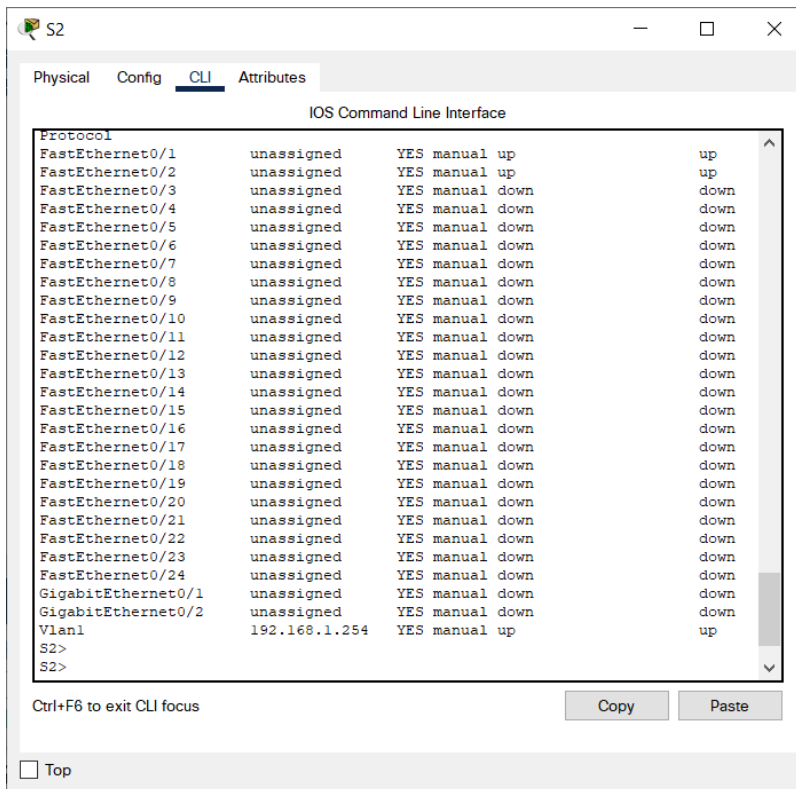
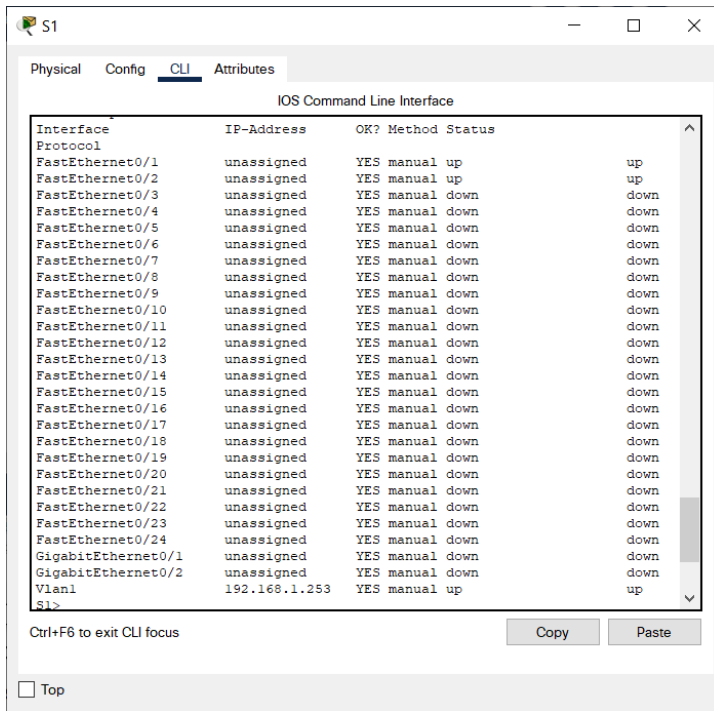
S2(config-if)#
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#

```

Шаг 3. Проверьте настройки IP-адресов на коммутаторах S1 и S2.

Команда **show ip interface brief** выводит сведения об IP-адресе, а также о состоянии всех портов и интерфейсов коммутатора. Для этого можно также использовать команду **show running-config**.



Шаг 4. Сохраните конфигурации для S1 и S2 в NVRAM.

```
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
S2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Какая команда сохраняет файл конфигурации из RAM в NVRAM?

Ответ: S1# copy running-config startup-config (copy run start)

Шаг 5. Проверьте подключение к сети.

Подключение к сети можно проверить с помощью команды **ping**. Очень важно, чтобы подключения работали во всей сети. В случае сбоя необходимо устранить неполадку. Проверьте связь коммутаторов S1 и S2 с компьютерами PC1 и PC2.

А. Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол).

Б. Нажмите **Command Prompt** (Командная строка).

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=7ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 4ms
```

В. С помощью команды ping проверьте доступность IP-адреса компьютера PC2.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Г. С помощью команды `ping` проверьте доступность IP-адреса коммутатора S1.

```
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Д. С помощью команды `ping` проверьте доступность IP-адреса коммутатора S2.

```
C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Примечание. Команду `ping` можно использовать в интерфейсе командной строки коммутатора и на PC2.

Все эхо-запросы должны быть обработаны успешно. Если результат первой проверки — 80 %, повторите попытку. Теперь результат должен быть 100 %. Позже вы узнаете, почему первая проверка иногда завершается неудачно. Если проверить связь с устройствами не удастся, проверьте конфигурацию на наличие ошибок.

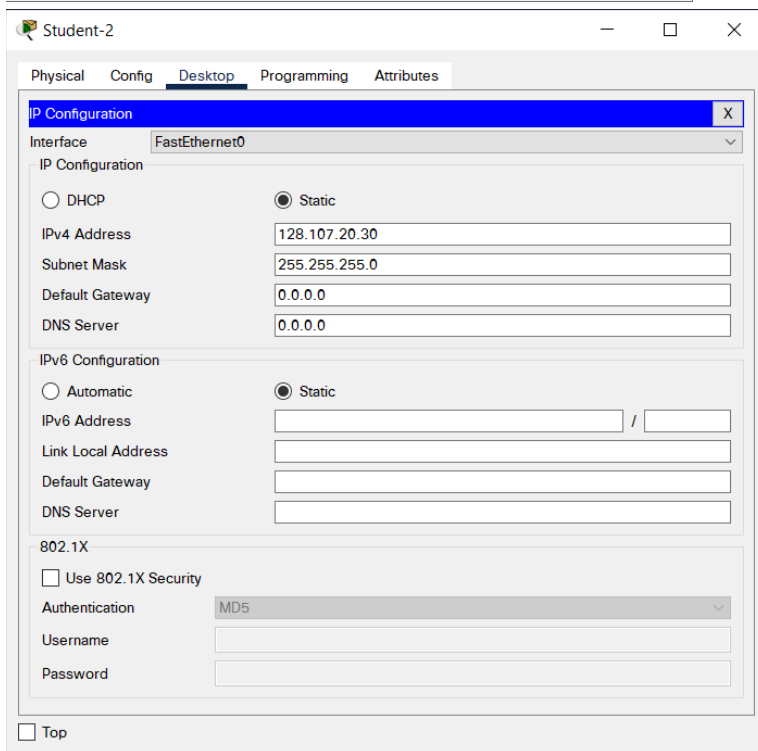
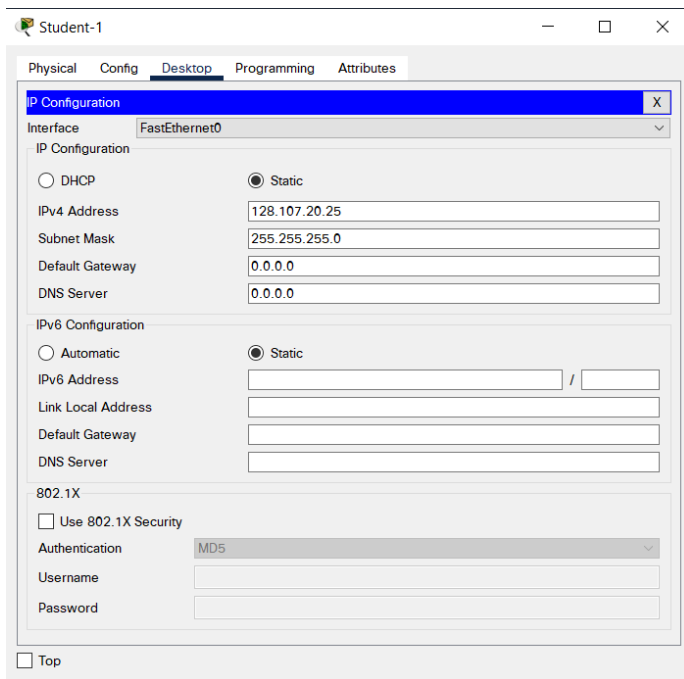
Задание 2.4.1.2 Отработка комплексных практических навыков.

Таблица адресации

Устройство	интерфейс	IP-адрес	Subnet Mask (Маска подсети)
Class-A	VLAN 1	128.107.20.10	255.255.255.0
Class-B	VLAN 1	128.107.20.15	255.255.255.0
Student-1	NIC	128.107.20.25	255.255.255.0
Student-2	NIC	128.107.20.30	255.255.255.0

Задачи

- Настройте имена узлов и IP-адреса на двух коммутаторах под управлением операционной системы Cisco IOS с помощью интерфейса командной строки (CLI).
- Используя команды Cisco IOS, задайте параметры доступа или ограничьте доступ к конфигурации устройства.
- С помощью команд IOS сохраните текущую конфигурацию.
- Настройте на двух хостах IP-адреса.
- Проверьте подключение между двумя оконечными устройствами (ПК).



Сценарий

Менеджер попросил вас, нового специалиста по обслуживанию локальных сетей, продемонстрировать навыки настройки небольшой локальной сети. Вам предстоит настроить исходные параметры на двух коммутаторах под управлением Cisco IOS, а также настроить параметры IP-адресации на узлах для создания сквозного подключения. Необходимо использовать два коммутатора и два узла (ПК) в активной сети с кабельным подключением.

Требования

- Используйте консольное подключение для доступа к каждому коммутатору.
- Задайте коммутаторам имена **Class-A** и **Class-B**.
- Используйте пароль **R4Xe3** для всех линий.
- Используйте скрытый (secret) пароль **C4aJa**.

- Зашифруйте все незашифрованные пароли.
- Включите слово **warning** (предупреждение) в баннер MOTD (сообщение дня).
- Настройте адресацию для всех устройств в соответствии с таблицей адресации.
- Сохраните настройки.
- Убедитесь в наличии соединения между всеми устройствами.

Примечание. Нажмите **Check Results** (Проверить результаты), чтобы увидеть результаты выполненных настроек. Нажмите **Reset Activity** (Сброс упражнения), чтобы создать новый набор требований. Если вы нажмете эту кнопку до того, как завершите выполнение упражнения, все настройки будут потеряны.

Isomorph Index: 0002

```

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Class-A
Class-A(config)#line console 0
Class-A(config-line)#password R4Xe3
Class-A(config-line)#login
Class-A(config-line)#line vty 0 15
Class-A(config-line)#password R4Xe3
Class-A(config-line)#login
Class-A(config-line)#exit
Class-A(config)#enable secret C4aJa
Class-A(config)#service password-encryption
Class-A(config)#banner motd "Warning!"
Class-A(config)#int vlan 1
Class-A(config-if)#ip address 128.107.20.10 255.255.255.0
Class-A(config-if)#no shutdown

Class-A(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Class-A(config-if)#exit
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console

Class-A#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Class-A#

```

Top

```
Student-2
Physical Config Desktop Programming Attributes
Terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Class-B
Class-B(config)#line console 0
Class-B(config-line)#password R4Xe3
Class-B(config-line)#login
Class-B(config-line)#line vty 0 15
Class-B(config-line)#password R4Xe3
Class-B(config-line)#login
Class-B(config-line)#exit
Class-B(config)#enable secret C4aJa
Class-B(config)#service password-encryption
Class-B(config)#banner motd "Warning!"
Class-B(config)#int vlan 1
Class-B(config-if)#ip address 128.107.20.15 255.255.255.0
Class-B(config-if)#no shutdown

Class-B(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Class-B(config-if)#exit
Class-B(config)#exit
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Class-B#
Class-B#
```

Top

Вывод

В ходе выполнения лабораторных работ: «Советы по использованию справки и навигации», «Представление сети» и «Навигация по IOS» были изучены базовые функции «Packet Tracer», произведен обзор программы «CisloPacket Tracer», получен доступа к коммутатору Cisco через консольный порт последовательного подключения, отображены и настроены основных параметров устройства, получен доступа к маршрутизатору Cisco с помощью консольного кабеля mini-USB. Также были даны ответы на вопросы, проверяющие усвоение теоретического материала, прикреплены все 36

снимков экрана на каждом выполненном шаге лабораторной работы. Все данные отображены в отчете и отправлены преподавателю на проверку