

Московский государственный технический университет им. Н. Э.
Баумана

Кафедра ИУ-4
«Проектирование и технология производства ЭС»

Журнал практических работ

по курсу:
«Основы телекоммуникационных технологий»

Для студентов приборостроительных специальностей
20 __ / __ учебный год

Студент		Группа	
Преподаватель		Допуск	

№ работы	1	2	3	4
Оценка				

Москва
2019

Студент:		Допуск:	
Отчет по лабораторной работе №1 часть 1 «Монтаж сетевых разъемов 8p8c»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Получить практические навыки

Задачи работы:

Изучить состав и структуру

Выявить особенности применения

Краткий конспект теоретической части:

Registered Jack:

8P8C:

T568A и T568B:

Витая пара:

Количество используемых пар в различных стандартах:

Необходимые приспособления для обжима витой пары:

Задание 1. Дайте описание каждому типу кабеля:

UTP	
FTP	
STP	
S/UTP	
S/FTP	
S/STP	

Основные этапы обжима витой пары:

1. Убрать внешнюю изоляцию с конца кабеля. Проверьте, чтобы не было повреждений на внутренних проводниках.

2. Расположить проводники в нужной последовательности. Подровнять проводники, обрезав их настолько, чтобы внешняя оболочка немного входила в коннектор.

3. Вставить проводники в коннектор до тех пор, пока не будут видны их торцы.

4. Провести обжим при помощи специального инструмента.

5. Провести визуальный контроль. Ножи в коннекторе должны прорезать изоляцию и создать надежный контакт.

6. Повторить шаги 1-5 для второго конца кабеля.

7. Проверить качество обжима при помощи тестера.

Задание 2. Произведите обжим прямого кабеля и кроссовера. Засчитывается кабель, проверенный на тестере. Зарисуйте схему расположения проводников:

Прямой кабель	Кроссовер
Схема проводников:	Схема проводников:

Студент:		Допуск:	
Отчет по лабораторной работе №1 часть 2 «Знакомство с беспроводными сетями»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

<hr/> <hr/>

Задачи работы:

<hr/> <hr/>

Краткий конспект теоретической части:

Понятие Wi-Fi:

<hr/> <hr/> <hr/>

Различные версии стандарта 802.11:

<hr/> <hr/> <hr/>

Технология MIMO:

<hr/> <hr/> <hr/>

Каналы и частотные диапазоны Wi-Fi:

<hr/> <hr/> <hr/>

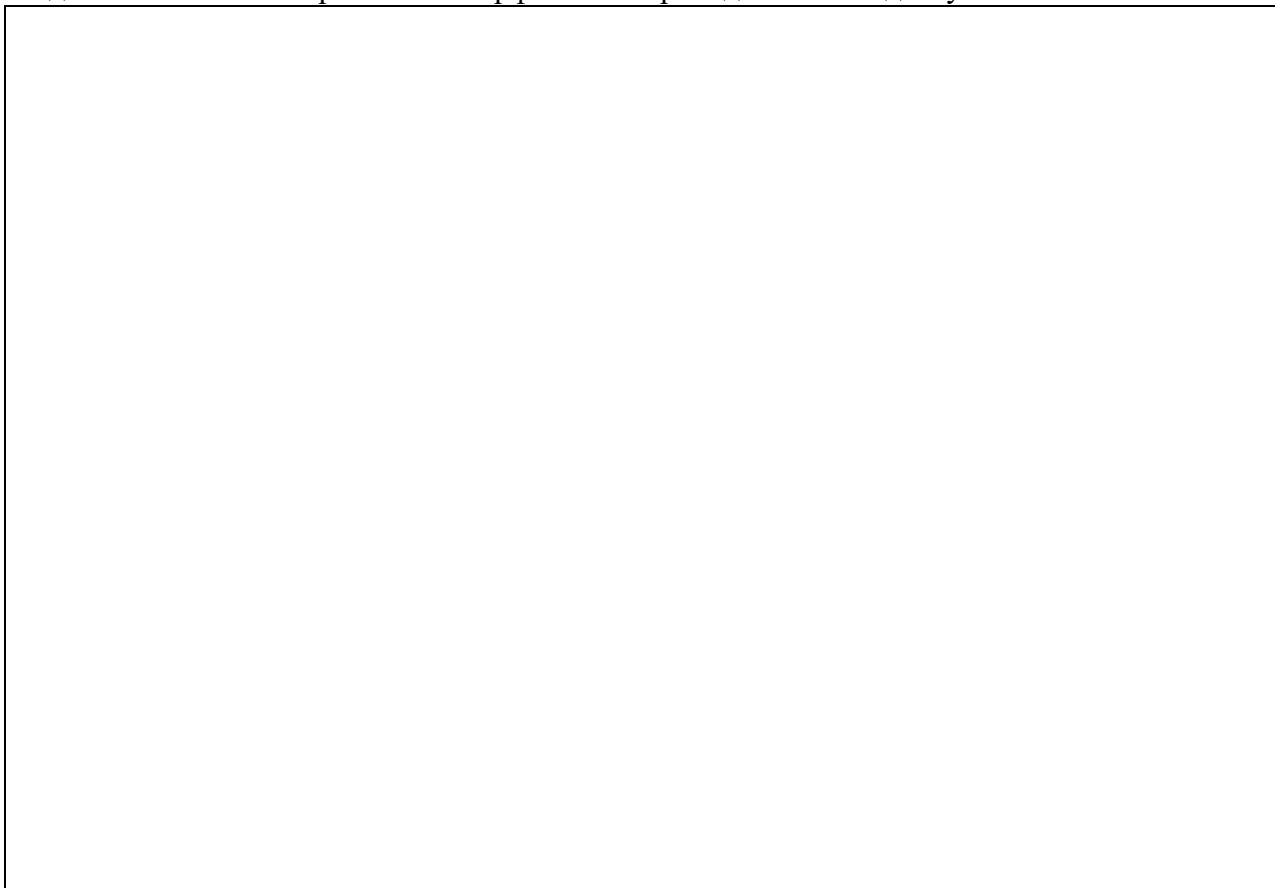
Бесшовный роуминг Wi-Fi сети:

<hr/> <hr/> <hr/>

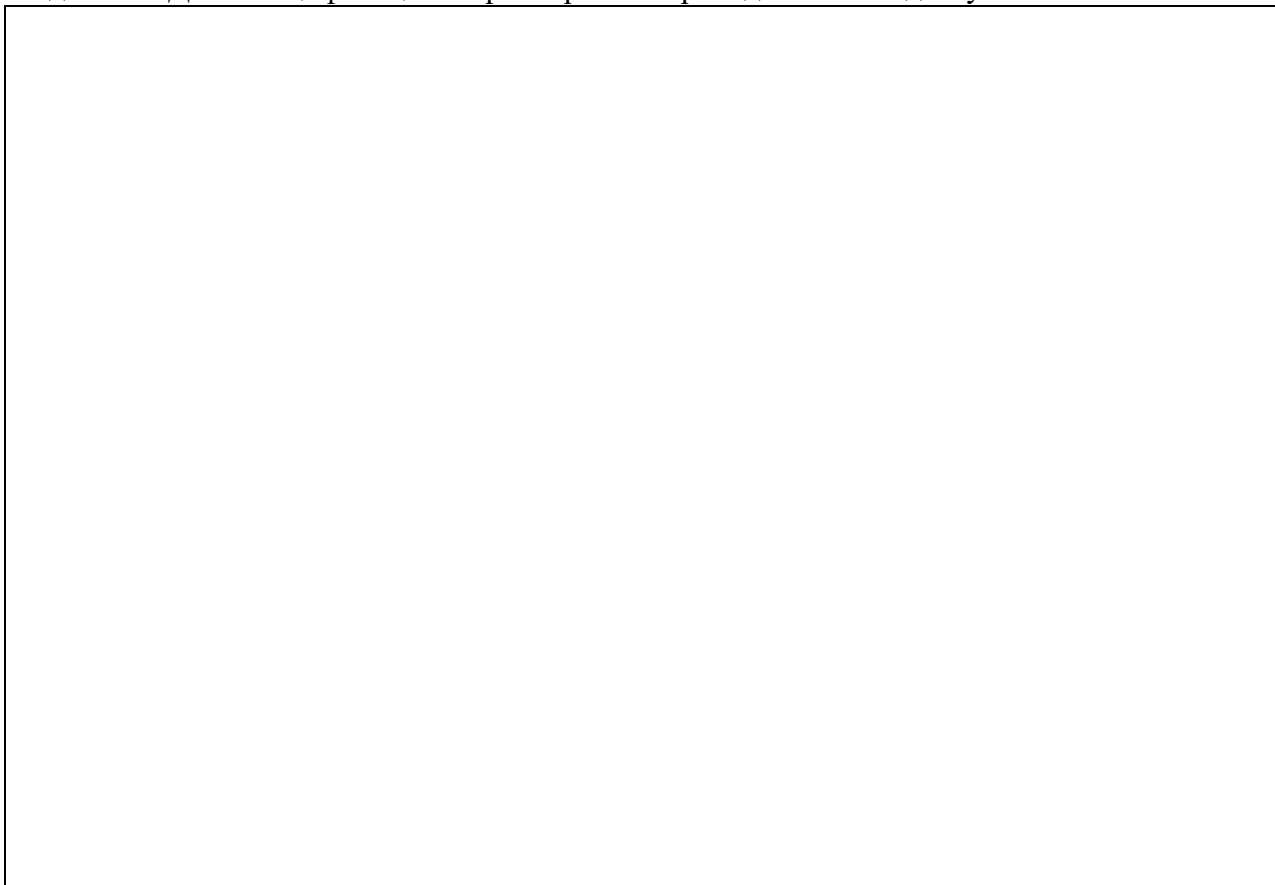
Технология WPS и почему это плохо:

<hr/> <hr/> <hr/>

Задание 1. Вклеить скриншот интерфейса беспроводной точки доступа.



Задание 2. Дать спецификацию параметров беспроводной точки доступа.



Задание 3. Описать топологию беспроводной сети.

Задание 4. Вклеить скриншот сканера эфира (например, Wifi Analyzer).

Контрольные вопросы 1:

1. Сколько пар проводников используется в стандартах 10BASE-T, 100 BASE-TX, 1000 BASE-T?
2. В каких случаях следует использовать прямой кабель, а в каких - кроссовер?
3. Приведите пример устройств, которые можно запитать при помощи технологии PoE.
4. Опишите особенности монтажа розетки по стандарту RJ45.
5. Как называется инструмент для обжима разъемов 8p8c?

Контрольные вопросы 2:

1. В чем отличие WiFi от IEEE 802.11?
2. Опишите различия между стандартами IEEE 802.11a, b, g, n.
3. Топологии сети, реализуемые при использовании технологии WiFi.
4. Что такое Ad-hoc?
5. Каналы в Wi-Fi.
6. Назовите отличия WEP от WPA.
7. Сколько пользователей можно подключать к точкам доступа?
8. Модуляция сигнала и ее влияние на пропускную способность.

Студент:		Допуск:	
Отчет по лабораторной работе №2 часть 1 «Работа с гипервизорами и виртуальными машинами»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Ознакомиться с технологиями виртуализации и работой виртуальных машин, ознакомиться с их особенностями

Задачи работы:

Краткий конспект теоретической части:

Понятие виртуализации:

Понятие гипервизора:

Понятие виртуальной машины:

Применение виртуальных машин частными лицами и организациями:

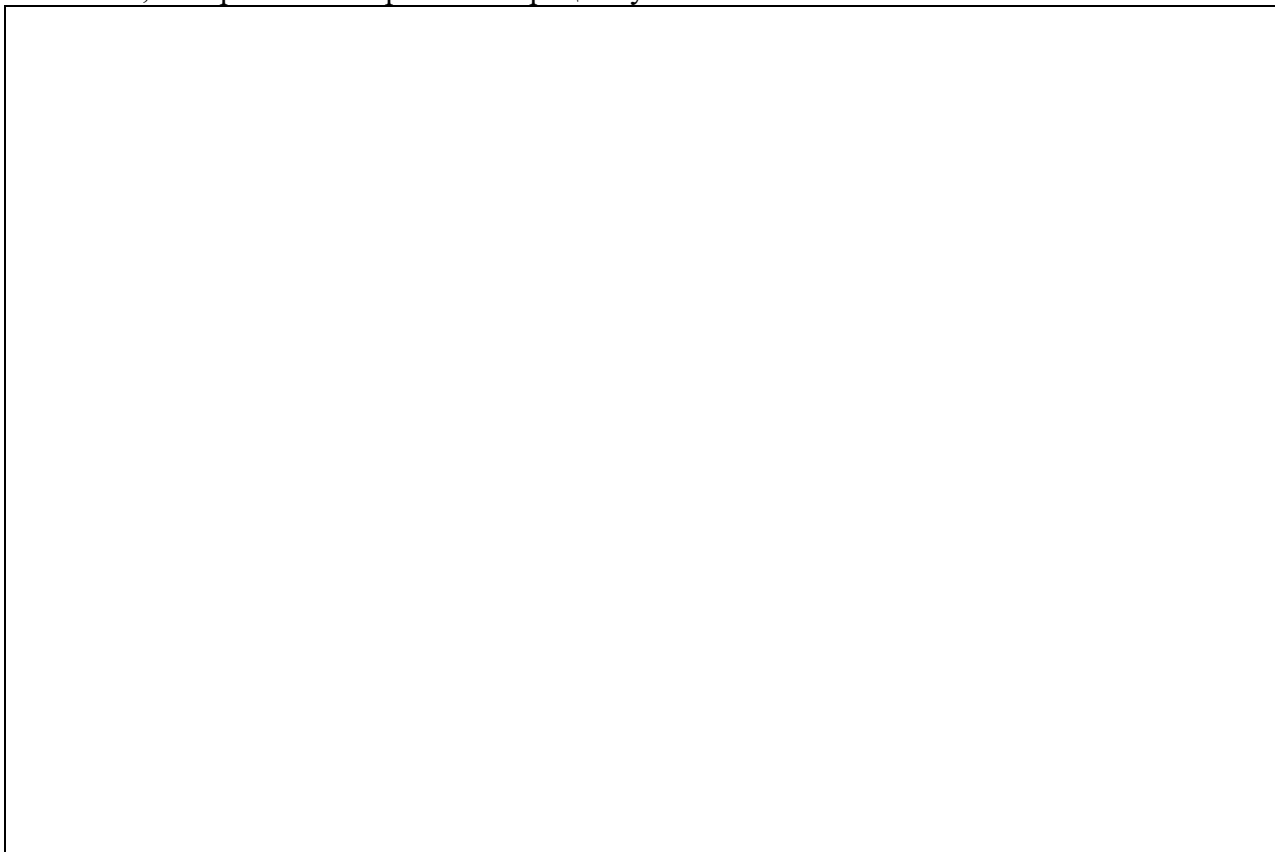
Варианты обеспечения доступа в сеть для VM:

Варианты удаленного доступа к VM:

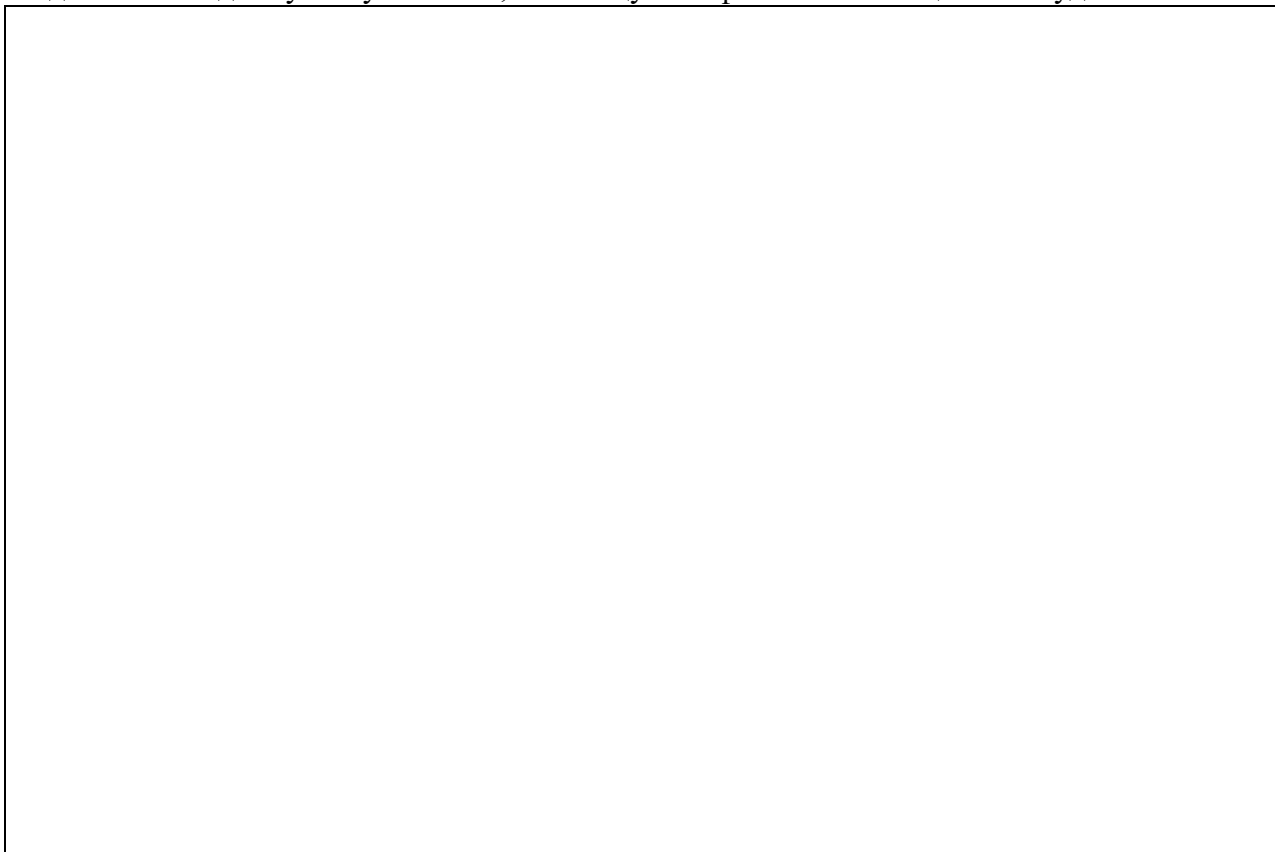
Задание 1. Провести обзор представленных на рынке гипервизоров с указанием их преимуществ и недостатков.

Задание 2. Установить программное обеспечение для виртуализации (гипервизор), отобразить на скриншоте стартовую страницу интерфейса.

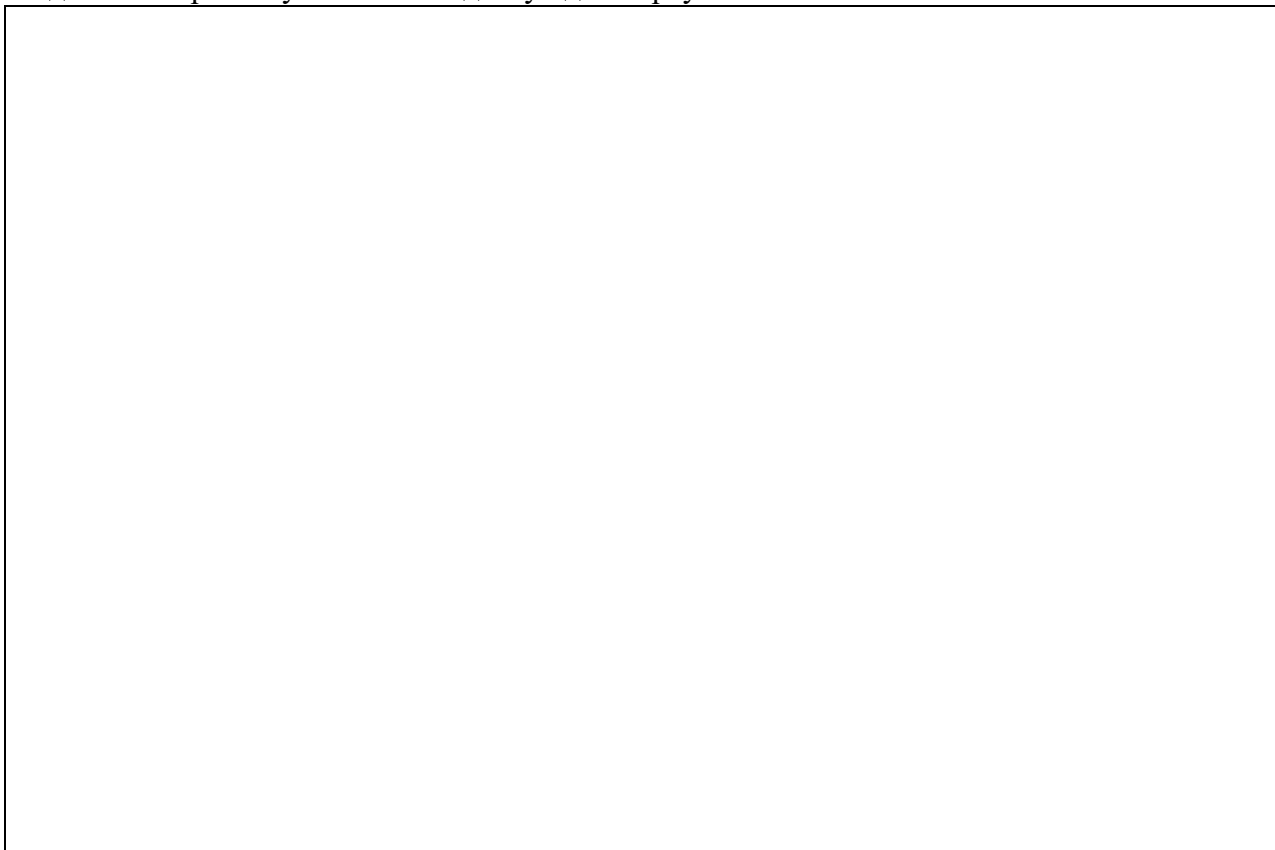
Задание 3. Создать новую виртуальную машину под управлением ОС семейства MS Windows, отобразить на скриншоте процесс установки.



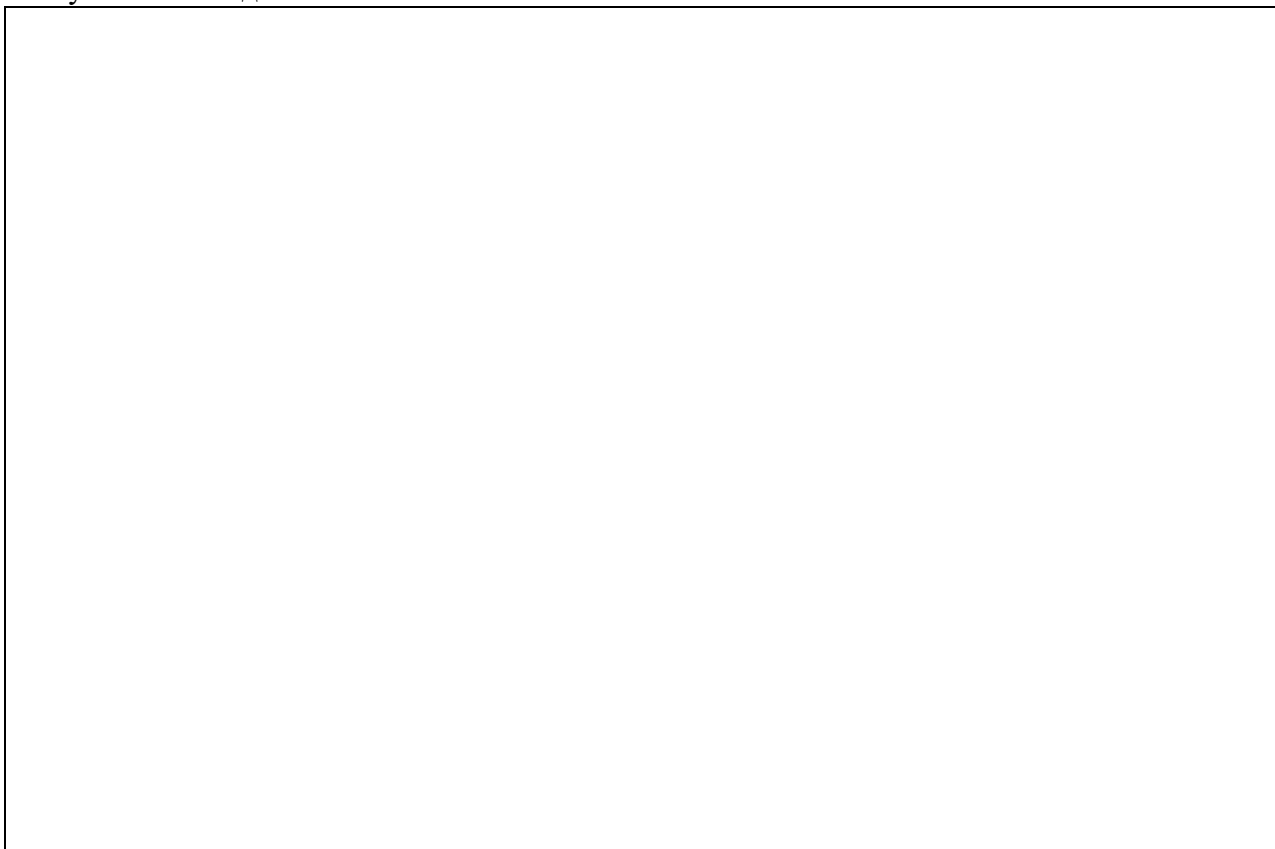
Задание 4. Создать учетную запись, состоящую из фамилии и инициалов студента.



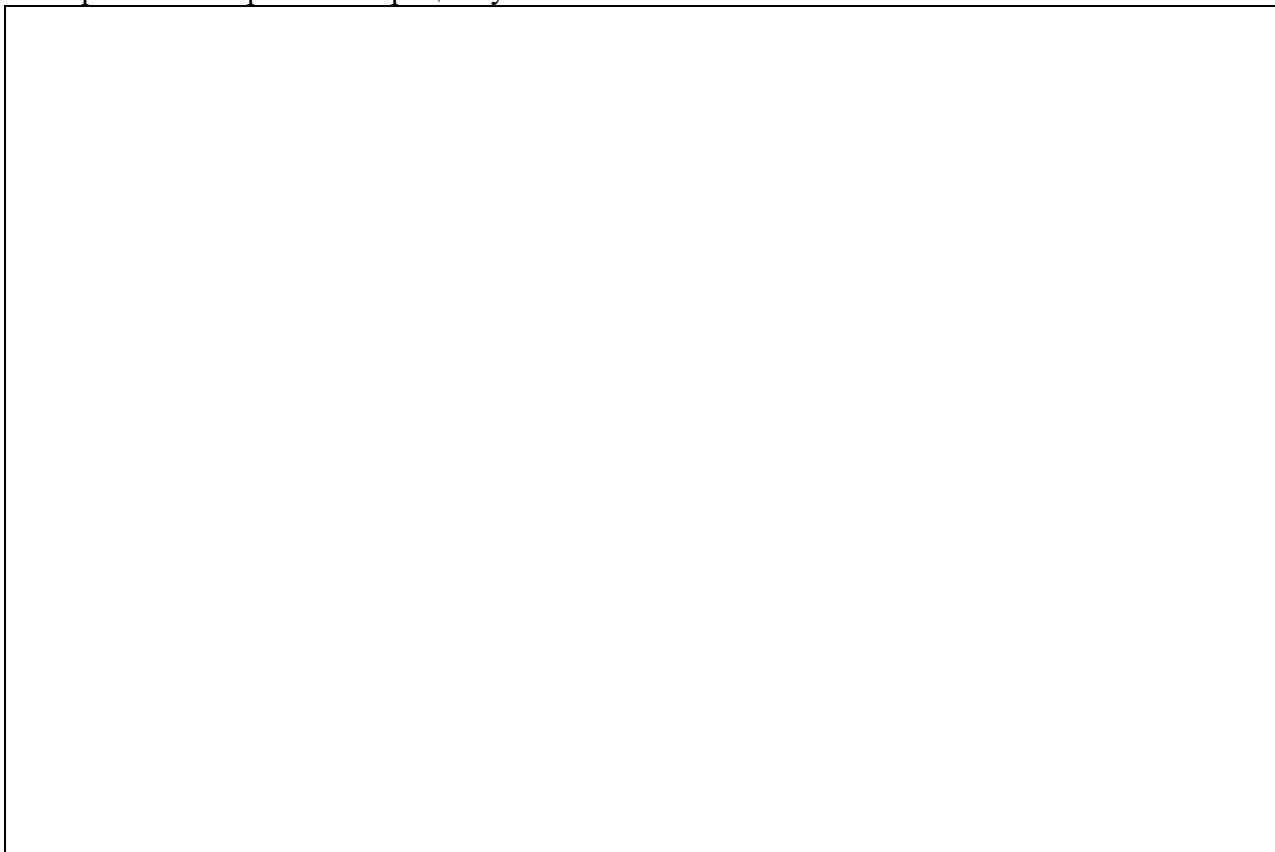
Задание 5. Организуйте сетевой доступ для виртуальной машины.

A large, empty rectangular box with a thin black border, intended for the student to provide their solution to task 5.

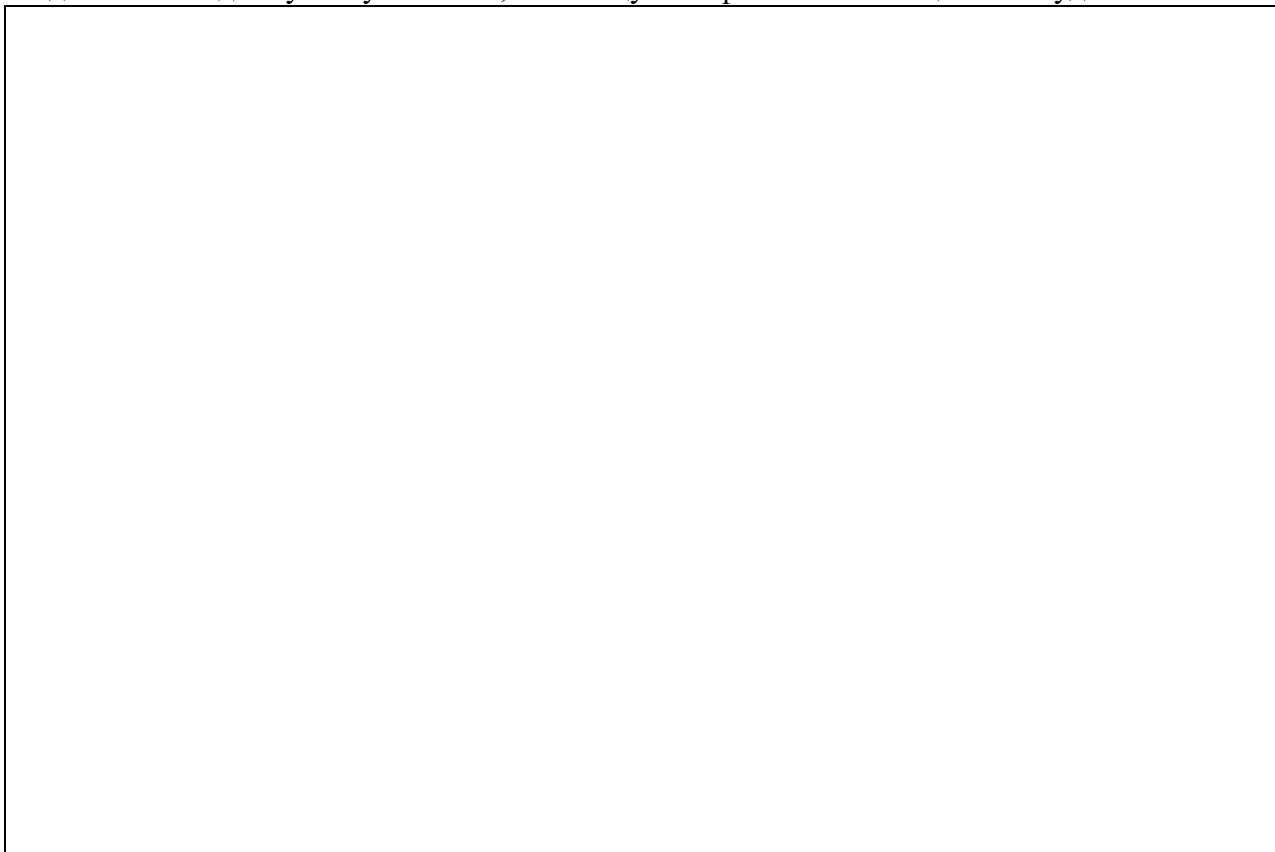
Задание 6. Подключитесь по протоколу RDP к виртуальной машине, используя настройки, полученные в заданиях 4 и 5.

A large, empty rectangular box with a thin black border, intended for the student to provide their solution to task 6.

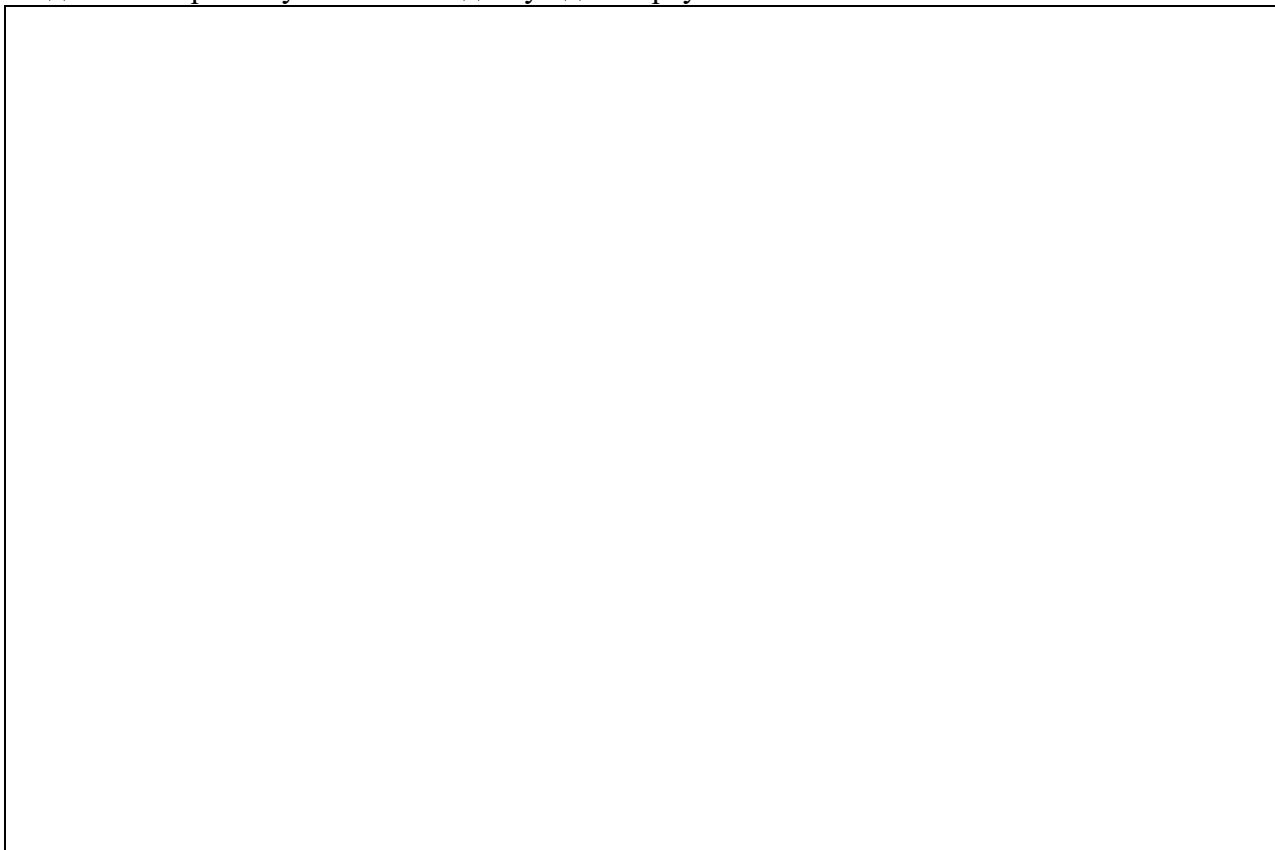
Задание 7. Создать новую виртуальную машину под управлением ОС семейства Linux, отобразить на скриншоте процесс установки.



Задание 8. Создать учетную запись, состоящую из фамилии и инициалов студента.



Задание 9. Организуйте сетевой доступ для виртуальной машины.

A large, empty rectangular box with a thin black border, intended for the student to provide their solution for task 9.

Задание 10. Подключитесь по протоколу SSH к виртуальной машине, используя настройки, полученные в заданиях 8 и 9.

A large, empty rectangular box with a thin black border, intended for the student to provide their solution for task 10.

Студент:		Допуск:	
Отчет по лабораторной работе №2 часть 2 «Установка и конфигурирование web- серверов»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Задачи работы:

Краткий конспект теоретической части:

Клиент-серверная архитектура:

Понятие веб-сервера:

Основные и дополнительные функции веб-сервера:

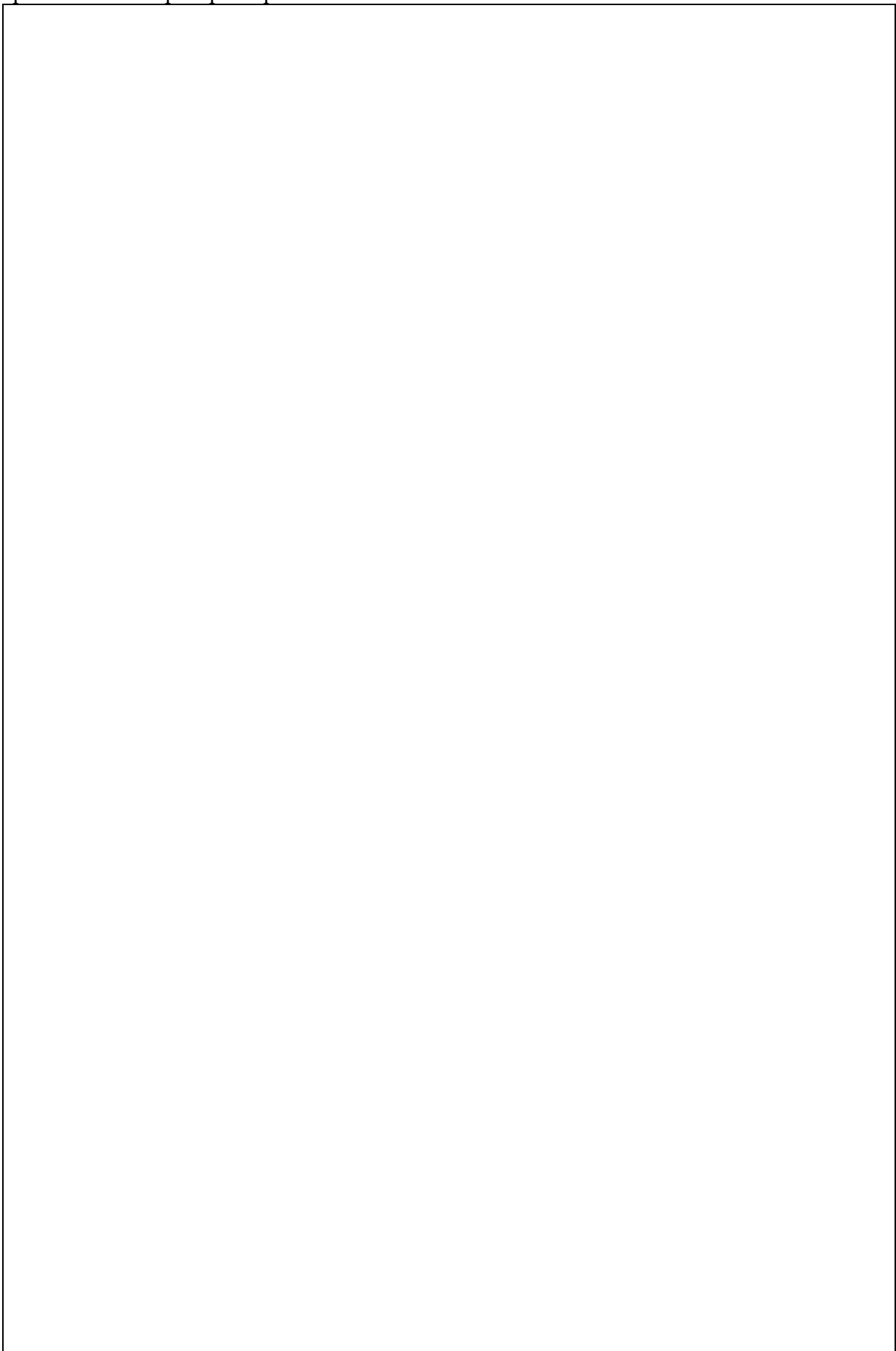
Протоколы, используемые веб-серверами:

Различие между HTTP и HTTPS:

Установка SSL-сертификатов на веб-сервер:

Задание 1. Проанализировать рынок веб-серверов.

Задание 2. Установить разные веб-серверы на виртуальные машины, развернутые в рамках 2й лабораторной работы.



Задание 3. Настроить один из веб-серверов в режиме прокси. Показать результат и конфигурационный файл

Задание 4. Добавить на проксирующий веб-сервер обработку https так, чтобы на клиентском устройстве не возникало ошибки проверки сертификата сервера. Показать результат на клиенте, сертификат и конфигурационный файл сервера.

Контрольные вопросы 1

1. Что такое виртуальная машина?
2. Классификация типов виртуализации.
3. Применение ВМ.
4. Основные этапы создания ВМ.
5. Варианты сетевых настроек ВМ.
6. Различие между подключением через консоль гипервизора и по протоколам RDP и SSH.

Контрольные вопросы 2

1. Описать общие принципы клиент-серверной архитектуры.
2. Дать определение тонкого и толстого клиента, указать различия.
3. Что такое веб-сервер и какие функции он может выполнять?
4. Можно ли поддерживать работу сайта на домашнем ПК?
5. Как можно расширить функционал веб-сервера? Приведите примеры.
6. Каков механизм работы веб-сервера в режиме прокси-сервера?
7. Какова роль удостоверяющих центров?
8. Какие условия необходимо соблюсти, чтобы сертификат сервера проходил проверку на клиентском устройстве?

Студент:		Допуск:	
Отчет по лабораторной работе №3 «Основы работы в командной оболочке и сетевой диагностики»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Получить навыки работы в командной оболочке bash

Задачи работы:

Краткий конспект теоретической части:

Стандартные порты сетевых служб:

Командная оболочка и терминал:

Структура каталогов в Linux и Windows:

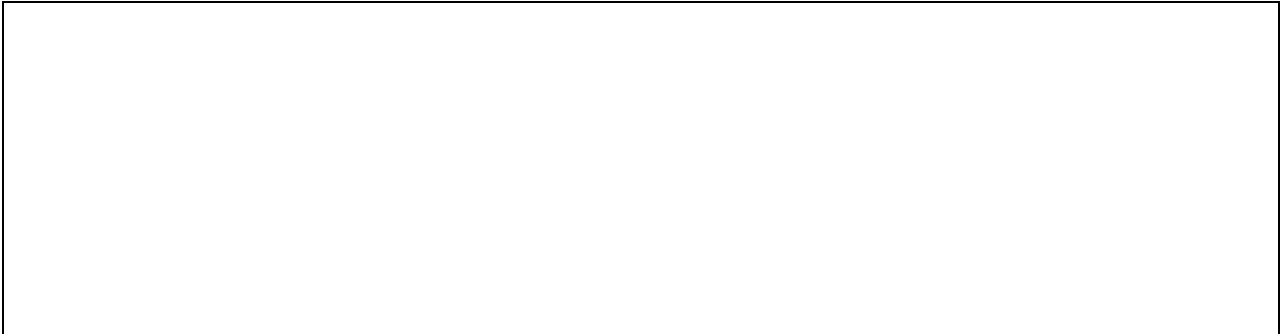
Диагностика сетевых неисправностей и роль сетевой модели в ней:

Структура Ethernet-фрейма и IP-пакета:

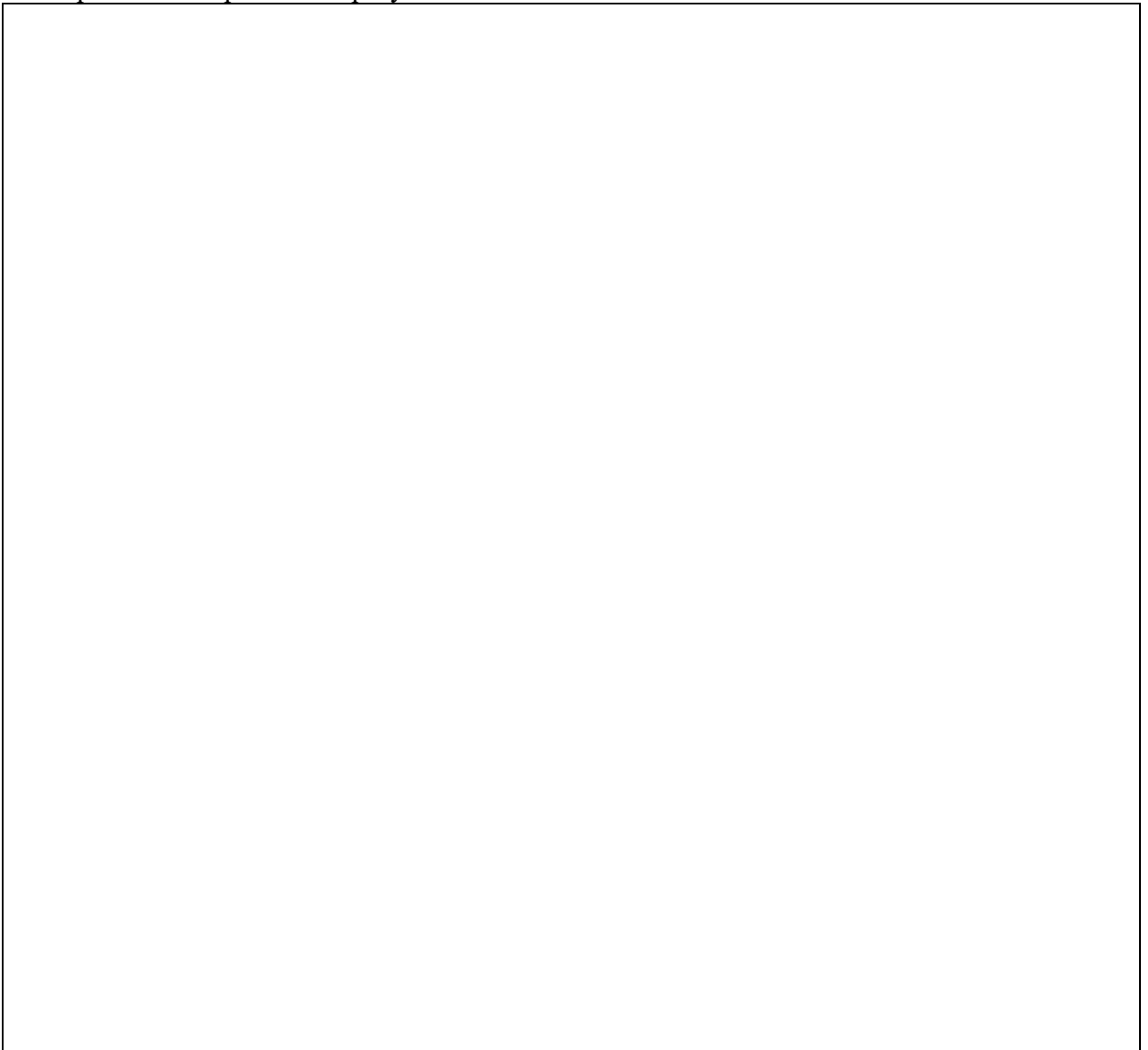
Получение справки по командам:

1 КОМАНДНАЯ ОБОЛОЧКА

Задание 1. Наберите на клавиатуре произвольный набор символов, не являющийся командой. Вклейте скриншот с результатом:



Задание 2. Введите несколько команд. Первая команда *date*. Она выводит текущее время и дату. Родственная ей команда *cal* по умолчанию выводит календарь текущего месяца. Чтобы увидеть объем свободного пространства на дисках, введите *df*. Аналогично, чтобы увидеть объем свободного пространства в памяти, введите команду *free*. Отобразите на скриншотах результаты выполнения этих команд:



2 НАВИГАЦИЯ ПО ДЕРЕВУ КАТАЛОГОВ

Задание 3. Выведите подробное о содержимое директории /etc или /bin используя абсолютный и относительный путь, находясь в домашнем каталоге.

3 ОПЕРАЦИИ С ФАЙЛАМИ И КАТАЛОГАМИ

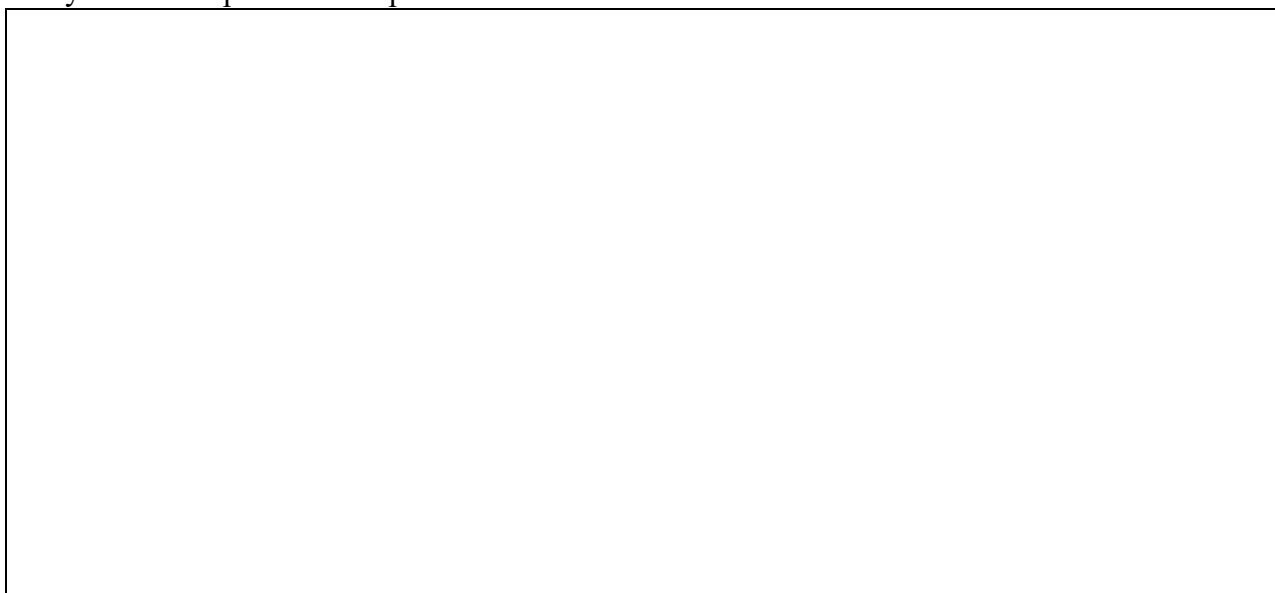
Задание 4. Отобразите на скриншотах результаты выполнения команд:

Переместитесь в домашнюю директорию и покажите это.	
Создайте директорию labs, в ней создайте директории dir1, dir2, dir3	
В каталоге dir1 создайте два файла file1, file2, а в каталоге labs - символические ссылки на них.	
Из каталога dir1 скопируйте file1 и переместите file2 в каталог dir2	
Покажите содержимое каталога labs в подробном виде	
Удалите каталог labs со всем его содержимым	

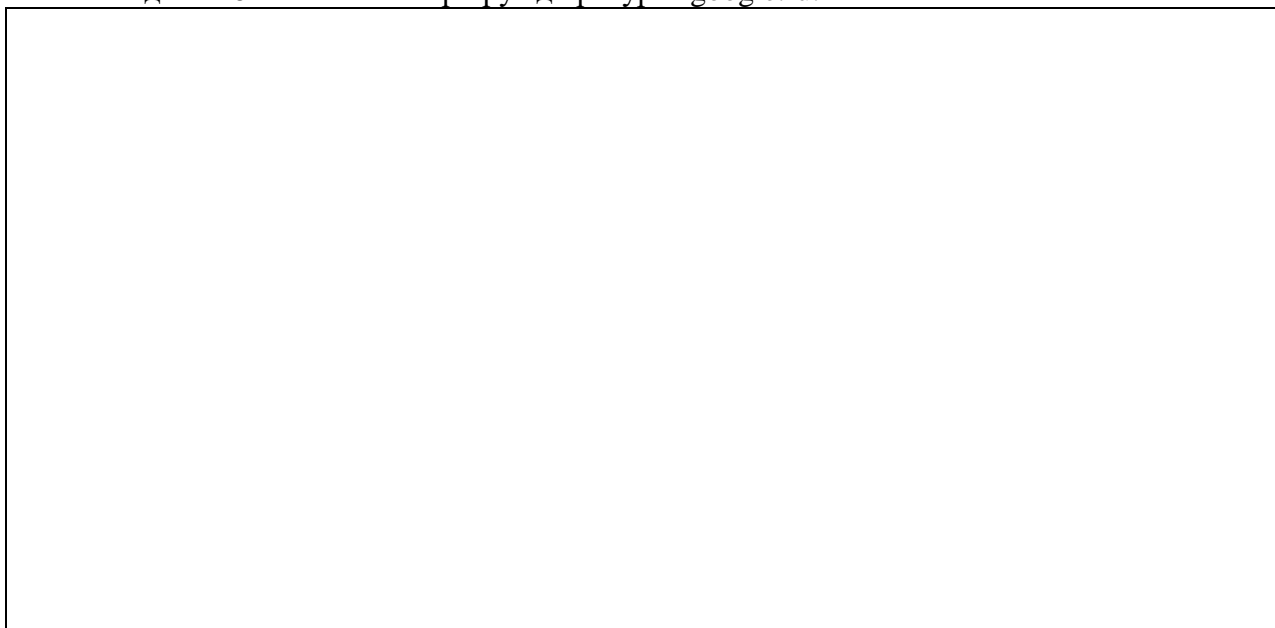
4 ОСНОВЫ СЕТЕВОЙ ДИАГНОСТИКИ

1	2	3	4	5	6	7
А	Б	В	Г	Д	Е	Ё
8	9	10	11	12	13	14
Ж	З	И	Й	К	Л	М
15	16	17	18	19	20	21
Н	О	П	Р	С	Т	У
22	23	24	25	26	27	28
Ф	Х	Ц	Ч	Ш	Щ	Ъ
29	30	31	32	33		
Ы	Ь	Э	Ю	Я		

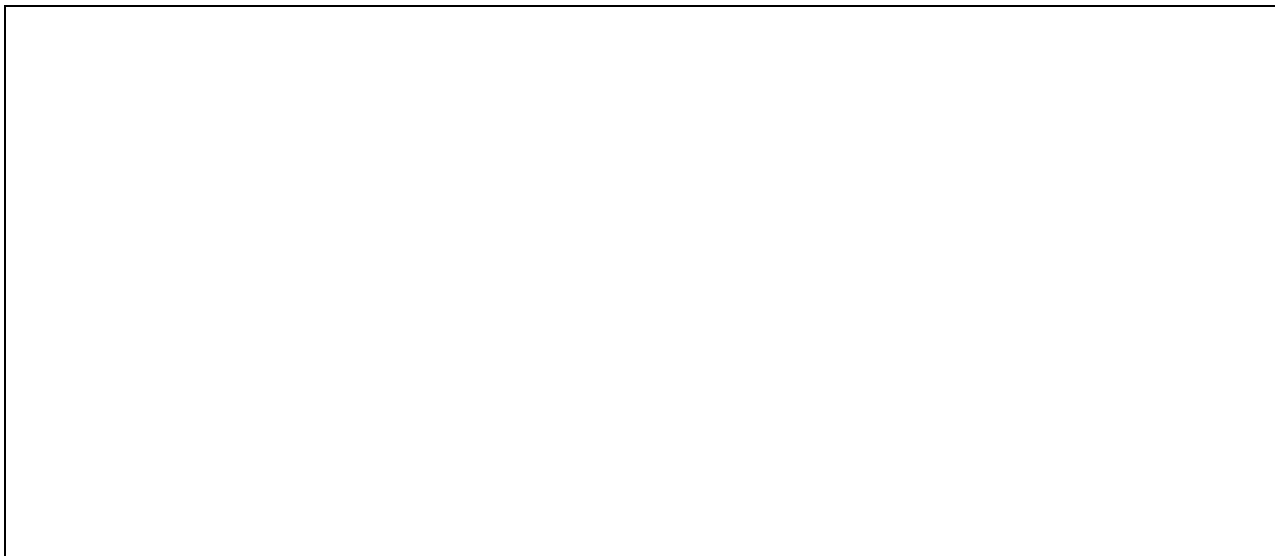
Задание 5. Отправьте несколько ICMP-запросов до сервера google.ru. Количество запросов должно соответствовать порядковому номеру первой буквы фамилии студента. Результат отобразить на скриншоте.



Задание 6. Покажите маршрут до ресурса google.ru.



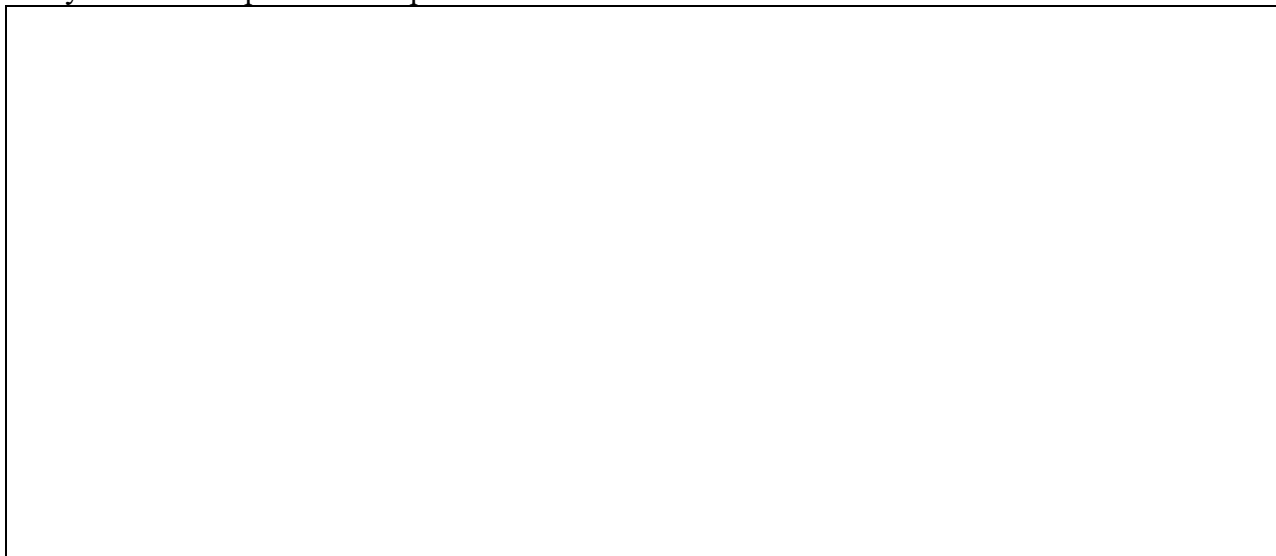
Задание 7. Покажите маршрут к ресурсу `google.com`, используя технологии `proxy`, `VPN` или `Tor`.



Задание 8. Показать работу команд `wget` и `curl` на примере сайта `iu4.ru`. Результаты отобразить на скриншоте.

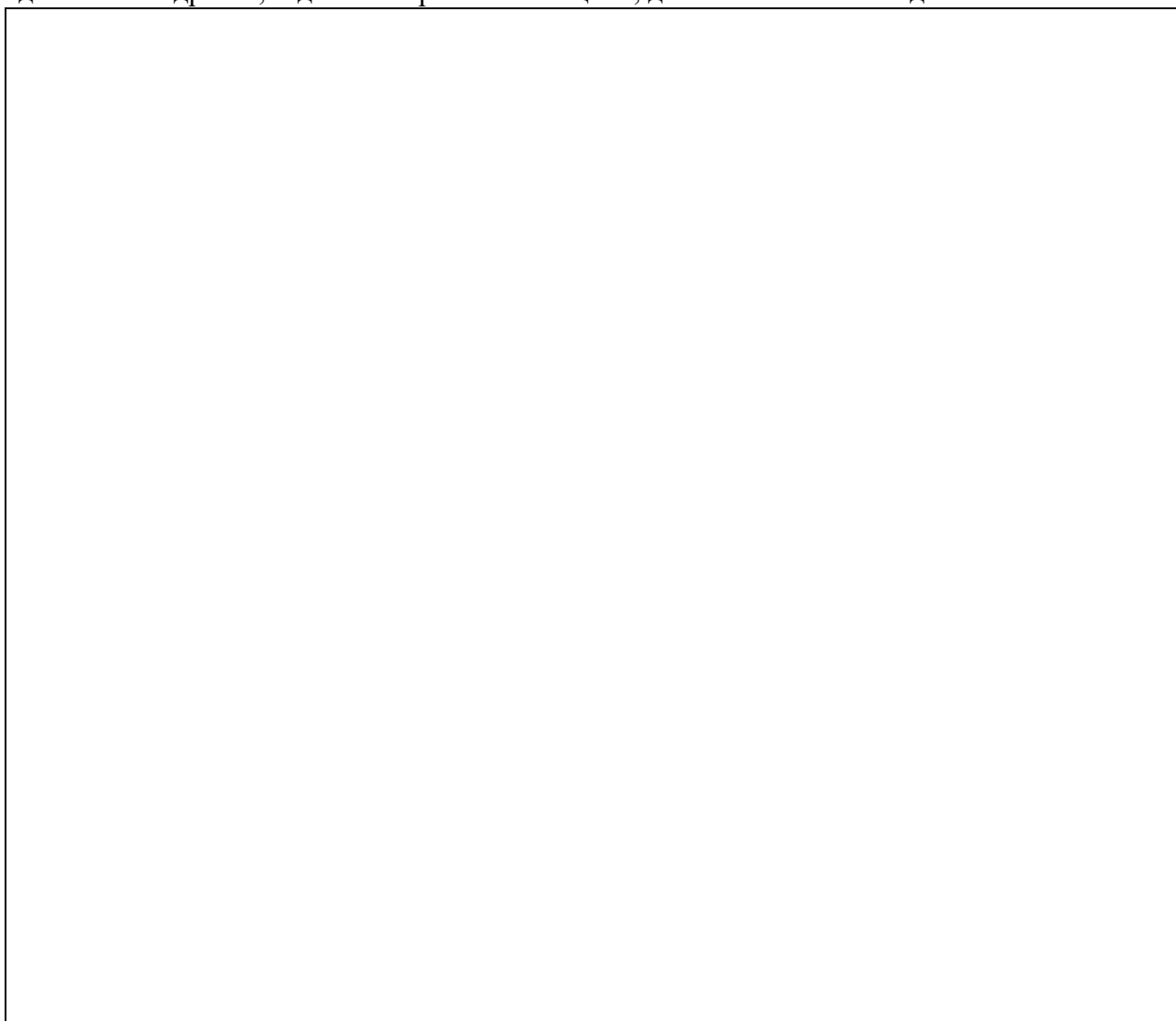


Задание 9. Проверьте работу программы ftp, скачав с ее помощью какой-либо файл. Результаты отобразите на скриншоте.

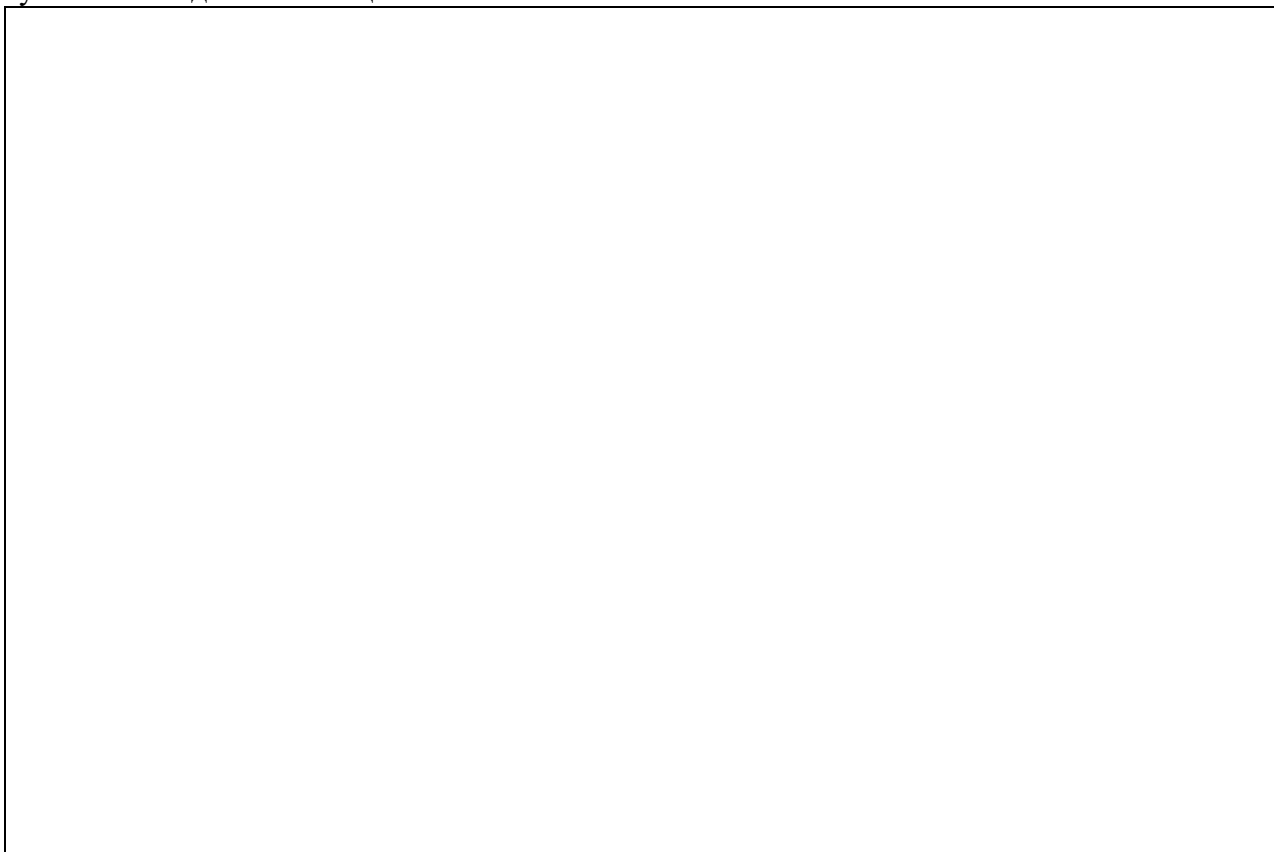


5 СЕТЕВОЙ СКАНЕР NMAP

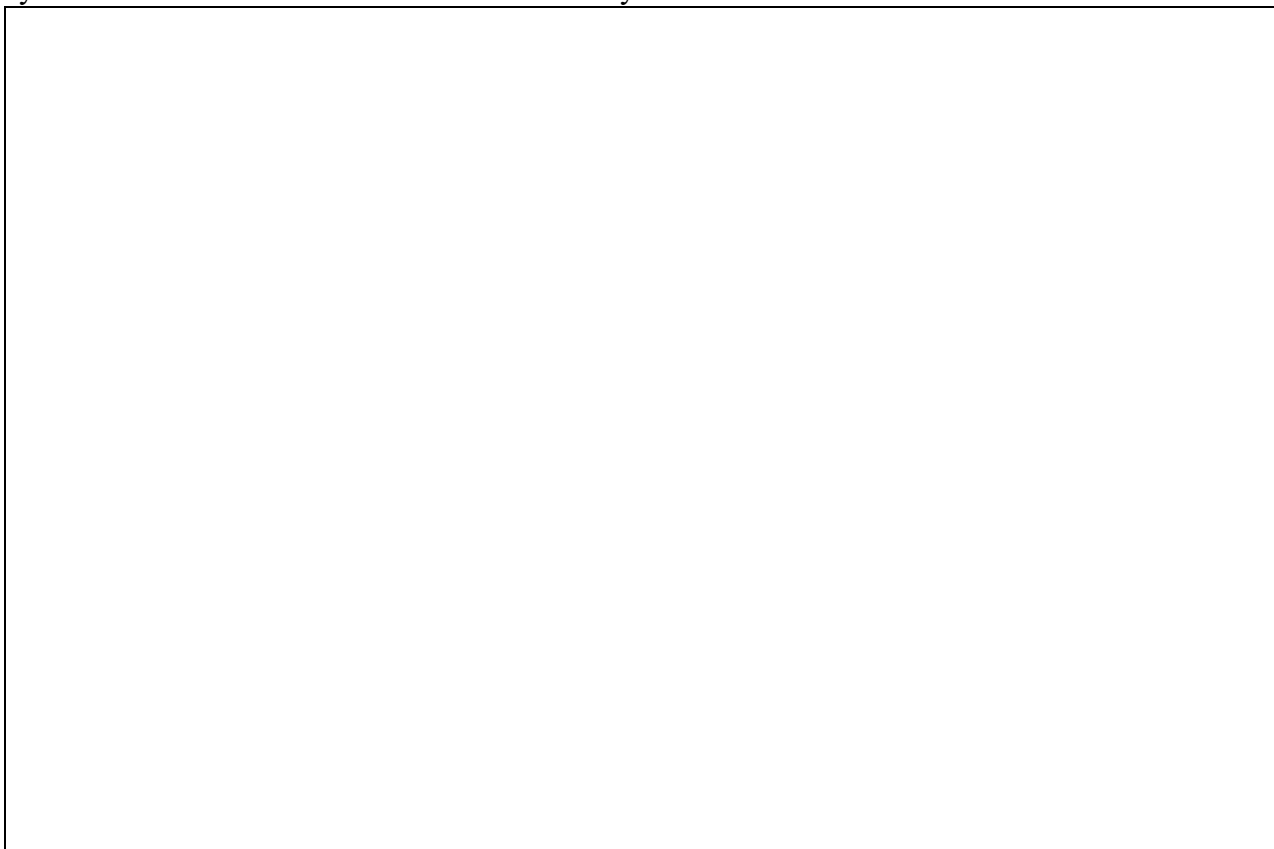
Задание 1. Используя пинг-сканирование (опция -sP), покажите, что одинаковые диапазоны адресов, заданные в разных нотациях, действительно совпадают.



Задание 2. Выясните, используя документацию, в каком режиме осуществляет сканирование nmap с опциями -A -T4 и отобразить на скриншоте результат сканирования узла iu4.ru с данными опциями.



Задание 3. Используя соответствующие ключи, покажите только открытые порты узла из вашей локальной сети или любого публичного хоста.



6 АНАЛИЗАТОР ПАКЕТОВ WIRESHARK

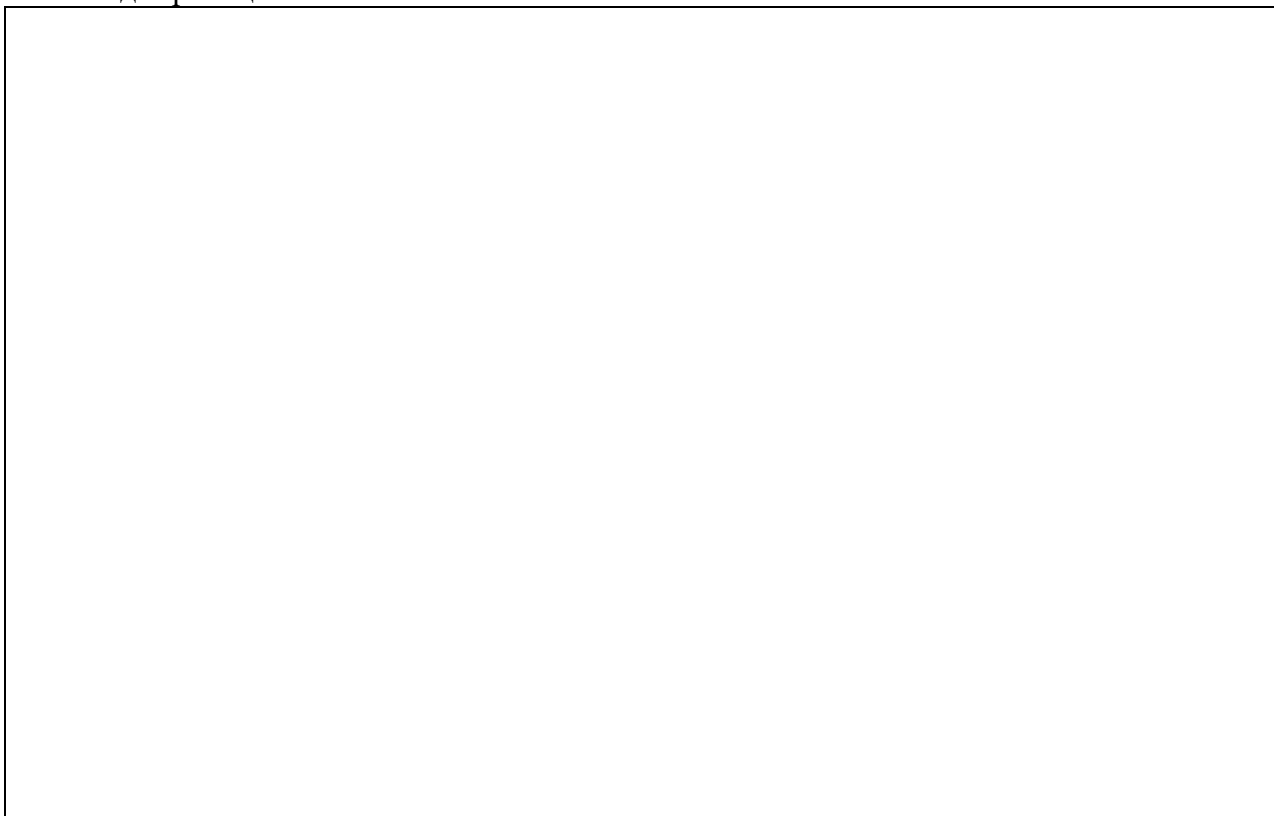
Задание 4. Запустите Wireshark, подождите, пока начнут захватываться пакеты, после чего покажите детальную информацию одного из них.

--

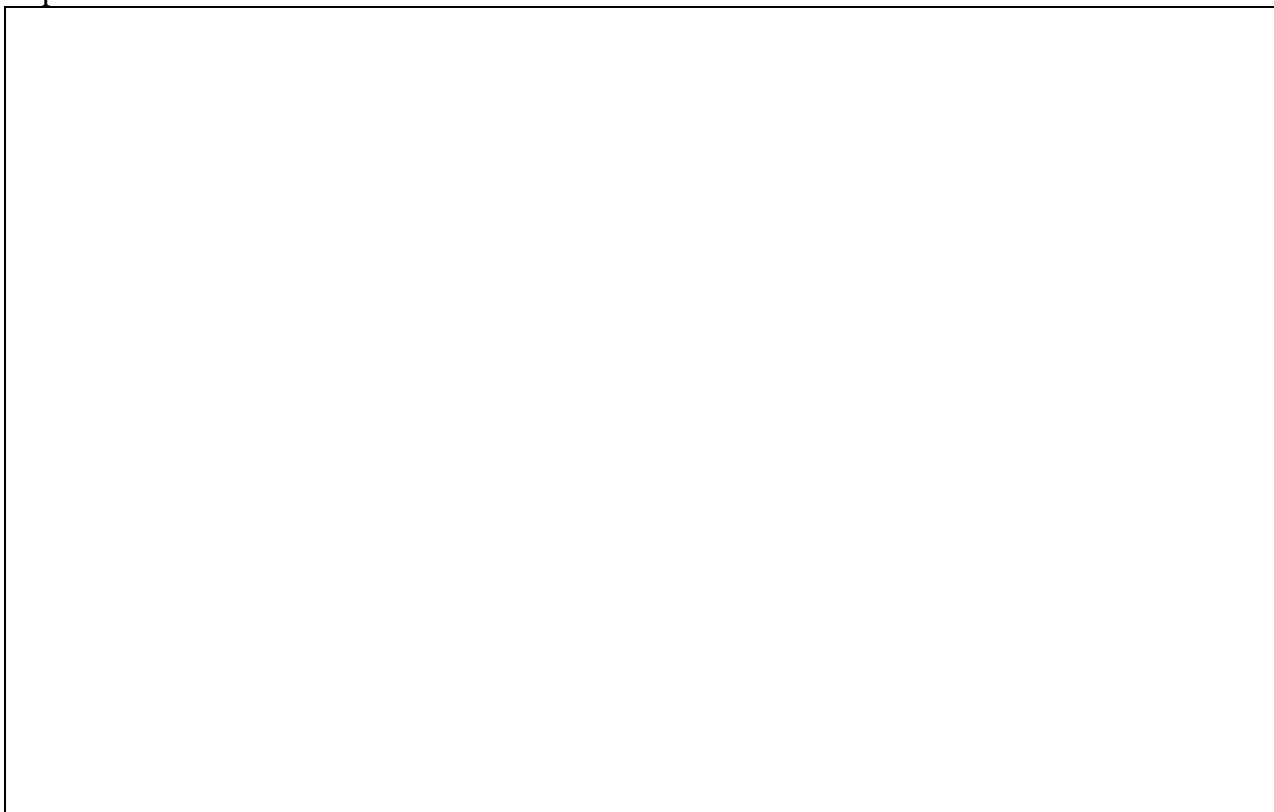
Задание 5. Напишите соответствующие фильтры:

Протокола http	
Определенного IP-адреса назначения	
Определенного значения поля TTL	
Сегментов с флагом SYN	
Всего трафика кроме ICMP, DNS и ARP протоколов	

Задание 6. Запустите Wireshark, откройте в браузере страницу iu4.ru, дождитесь ее загрузки, остановите сканирование. Покажите, что с помощью сканера можно получить html-код страницы.



Задание 7. Запустите Wireshark, в nmap начните SYN-сканирование хоста, о котором достоверно известно, что он в сети. Изучите, как отвечает узел в случае закрытого и открытого порта, обратив особое внимание на установку флагов в ответном tcp-сегменте.



Контрольные вопросы 1:

1. В чем отличие между командной оболочкой и терминалом?
2. Что такое приглашение к вводу и какую информацию оно содержит?
3. Что такое команда?
4. Каков будет вывод команды «ls -lah etc/nginx/», если мы находимся в домашней директории?
5. В чем различие между абсолютными и относительными путями?
6. Что такое параметры и аргументы команд?
7. В чем различие между жесткими и символическими ссылками?

Контрольные вопросы 2:

1. Как работает утилита ping?
2. Как указать количество отправляемых пакетов?
3. Что означают звездочки в выводе команды traceroute?
4. Какую информацию позволяет получить команда netstat?
5. Что такое тоннель ssh и как он может применяться?
6. В чем заключается принцип работы прокси-сервера?
7. В чем заключается принцип работы VPN-сервера?
8. В чем заключается принцип работы узлов сети Tor?

Контрольные вопросы 3:

1. Почему не следует проводить активное сканирование «чужих» сетей?
2. Чем различаются SYN- и ping-сканирования?
3. Какой диапазон портов будет просканирован с опцией -p *?
4. Можно ли при помощи Wireshark получить загруженные файлы?
5. Позволяет ли Wireshark обнаруживать вторжения в систему?
6. Приведите пример использования регулярных выражений в качестве аргументов Nmap и Wireshark.

Студент:		Допуск:	
Отчет по лабораторной работе №4 «Знакомство с ПО Cisco Packet Tracer»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Задачи работы:

Краткий конспект теоретической части:

Отличие эмулятора от симулятора:

ПО для удаленного подключения к консоли:

Протокол ICMP:

Протокол ARP:

Структура IP-пакета:

Аппаратная конфигурация коммутаторов Cisco:

1 ЗАГРУЗКА И УСТАНОВКА ПО CISCO PACKET TRACER

Cisco Packet Tracer является бесплатно распространяемым симулятором сети и ее компонентов, позволяющая оценить поведение сетевых устройств, изучить пути следования трафика при различных конфигурациях узлов сети, а также построить сложную сетевую топологию, не имея под рукой дорогостоящего оборудования. Следует принять во внимание, что СРТ является симулятором, а не эмулятором, то есть при аналогичных входных параметрах позволяет получить в качестве результата то же самое, что и оригинал, однако используя иные механизмы и алгоритмы обработки данных.

Загрузить дистрибутив можно бесплатно (правда, все же с регистрацией) с официального сайта сетевой академии Cisco, например, по ссылке:

<https://www.netacad.com/group/offerings/packet-tracer/>

Загрузить можно как версию для ОС семейства Windows, так и для Ubuntu. Процесс установки прост, при первом запуске необходимо будет ввести данные учетной записи сетевой академии, после чего появится окно программы, как на рисунке 1.

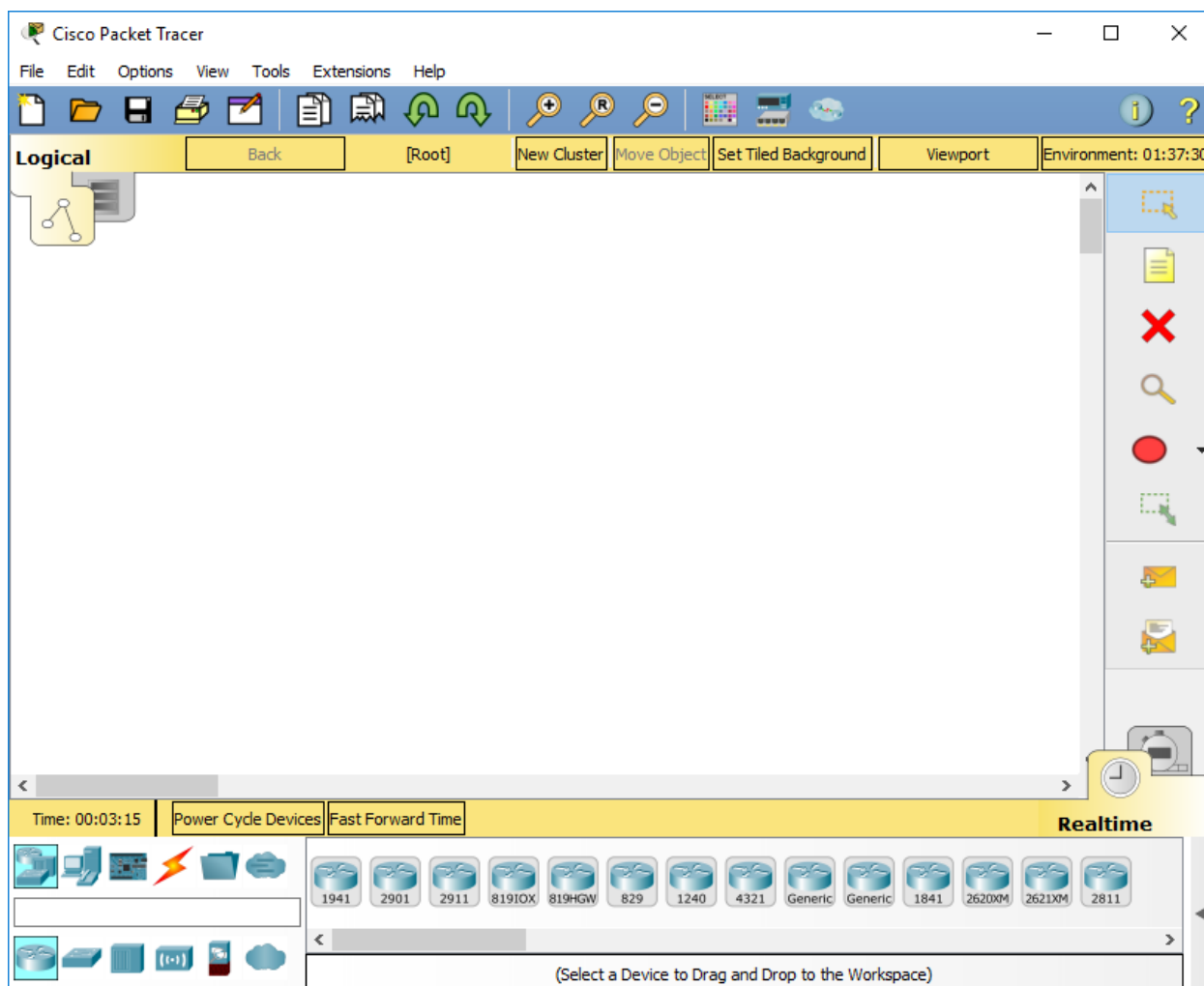


Рисунок 1 – Интерфейс Cisco Packet Tracer

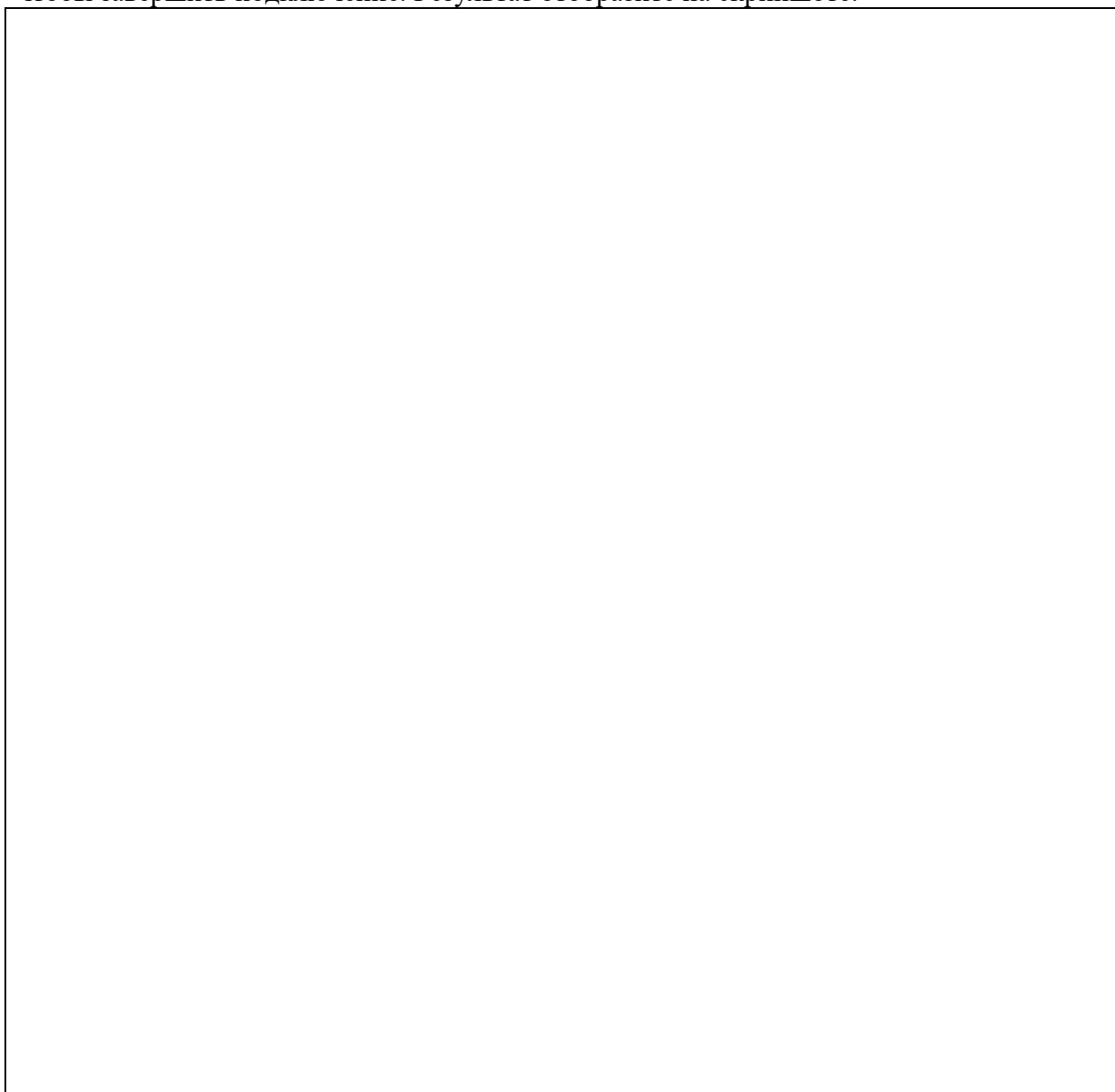
Именно в нем и будут производиться все действия.

2 НАЧАЛЬНАЯ НАСТРОЙКА СЕТЕВЫХ УСТРОЙСТВ

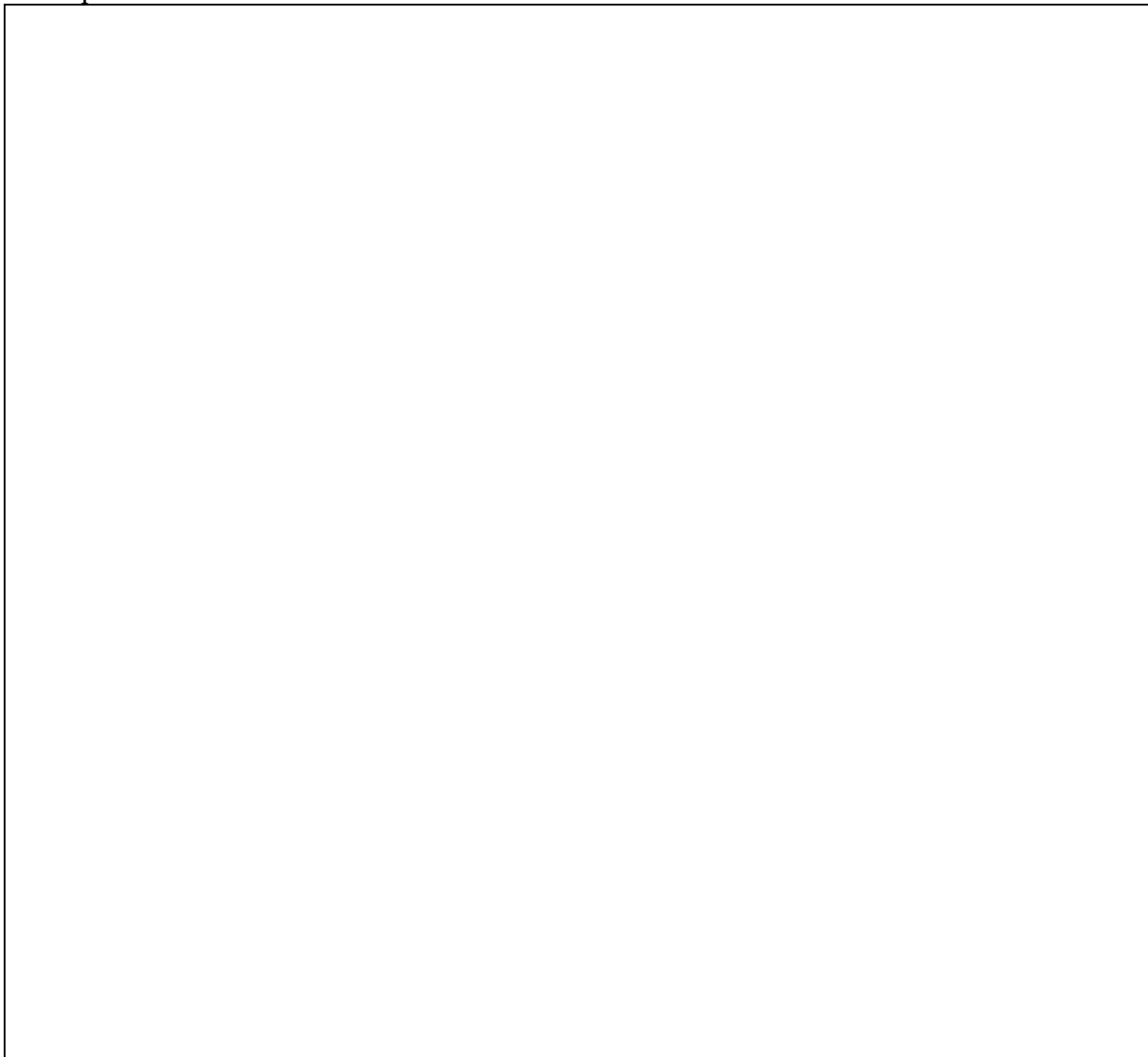
Задание 1. Выберите наиболее подходящий способ доступа для каждого случая.

	Консоль	Telnet/SSH
Вы находитесь в аппаратной, где нужно настроить новый коммутатор		
Сетевой администратор дает вам специальный кабель, с помощью которого нужно подключиться к коммутатору		
Вы получаете доступ к IOS по сети через другие промежуточные устройства		

Задание 2. Подключите PC1 к S1 с помощью консольного кабеля. Щелкните значок Connections (Подключения) (в виде молнии) в левом нижнем углу окна Packet Tracer. Выберите светло-голубой консольный кабель, щелкнув по нему. Указатель мыши примет вид разъема. Щелкните PC1. В окне будет показан вариант для подключения RS-232. Перетащите другой конец консольного подключения к коммутатору S1 и щелкните коммутатор, чтобы открыть список подключений. Выберите порт Console (Консольный), чтобы завершить подключение. Результат отобразите на скриншоте.



Задание 3. Установите сеанс диалога с коммутатором S1. Щелкните PC1 и откройте вкладку Desktop (Рабочий стол). Щелкните значок приложения Terminal (Терминал). Проверьте правильность параметров конфигурации портов, заданных по умолчанию. Каково значение параметра в битах в секунду? _____. Нажмите ОК. В появившемся окне может отображаться несколько сообщений. В окне должно появиться сообщение Press RETURN to get started!. Нажмите клавишу ввода. Отобразите результат на скриншоте.



Задание 4. Изучите справку по IOS. В IOS доступна справка по командам в зависимости от уровня работы. В данный момент отображается приглашение User EXEC (Пользовательский режим EXEC), и устройство ожидает ввода команды. Самый простой способ вызова справки — ввести вопросительный знак (?) в командной строке, чтобы получить список команд.

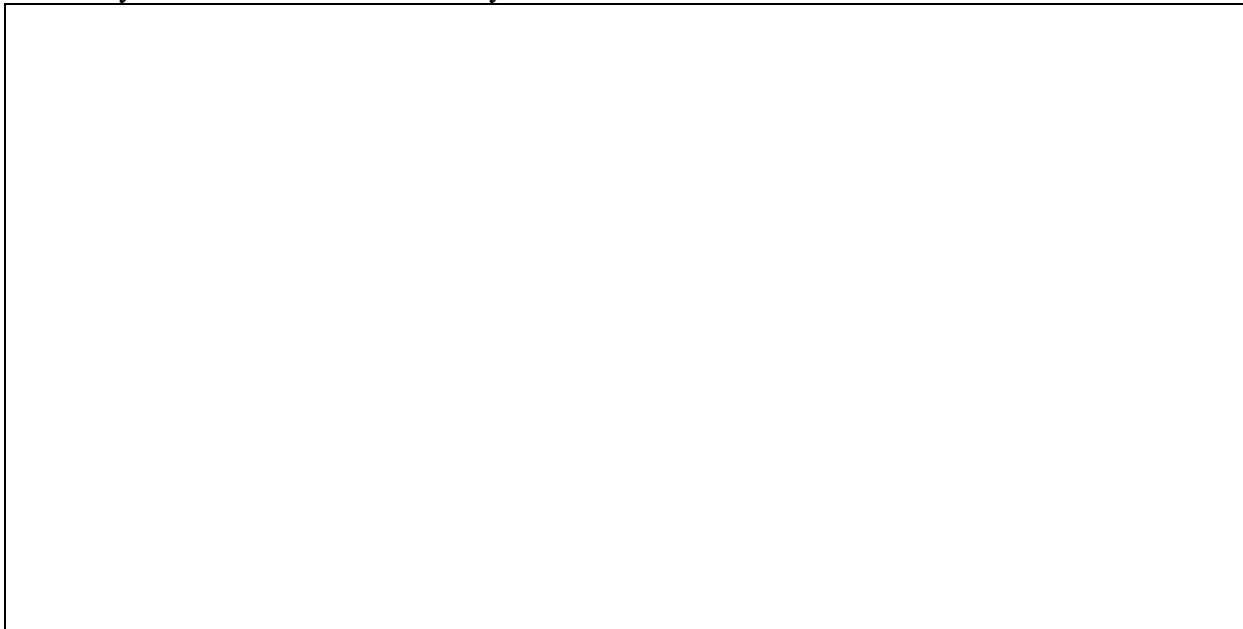
Какая команда начинается с буквы «с»? _____.

В командной строке введите t с вопросительным знаком в конце (?). Какие отображаются команды? _____.

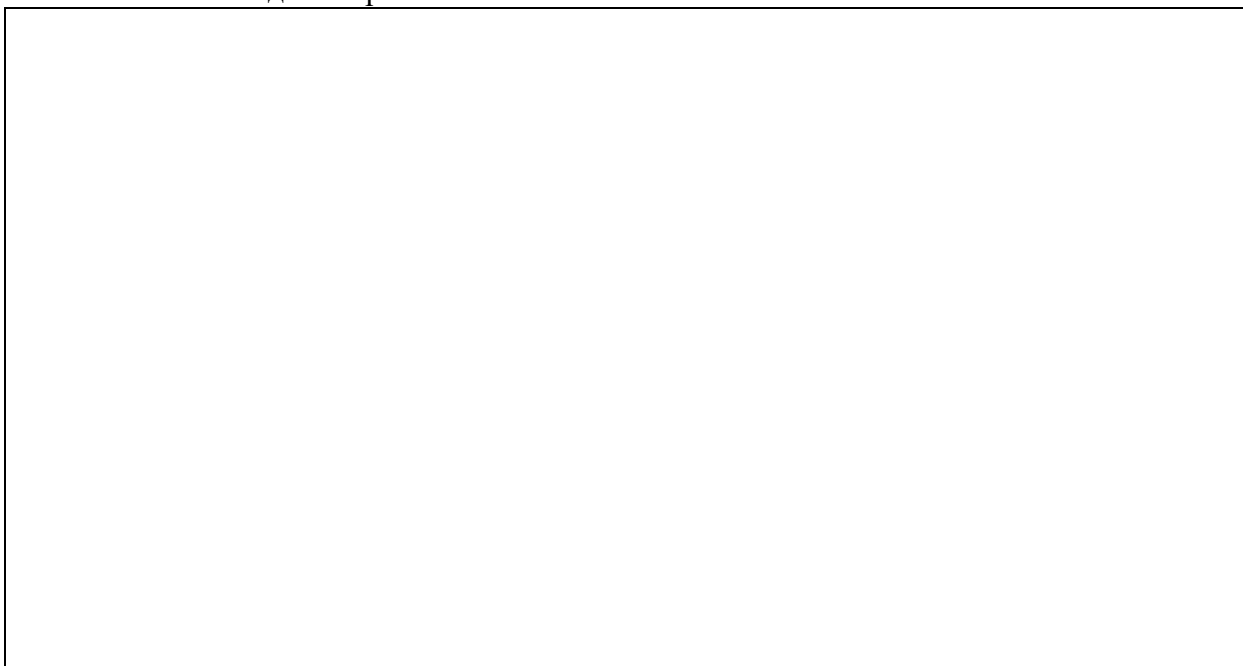
В командной строке введите te с вопросительным знаком в конце (?). Какие отображаются команды? _____.

Справка такого вида называется контекстной. Чем подробнее вводятся команды, тем больше сведений может предоставить справка.

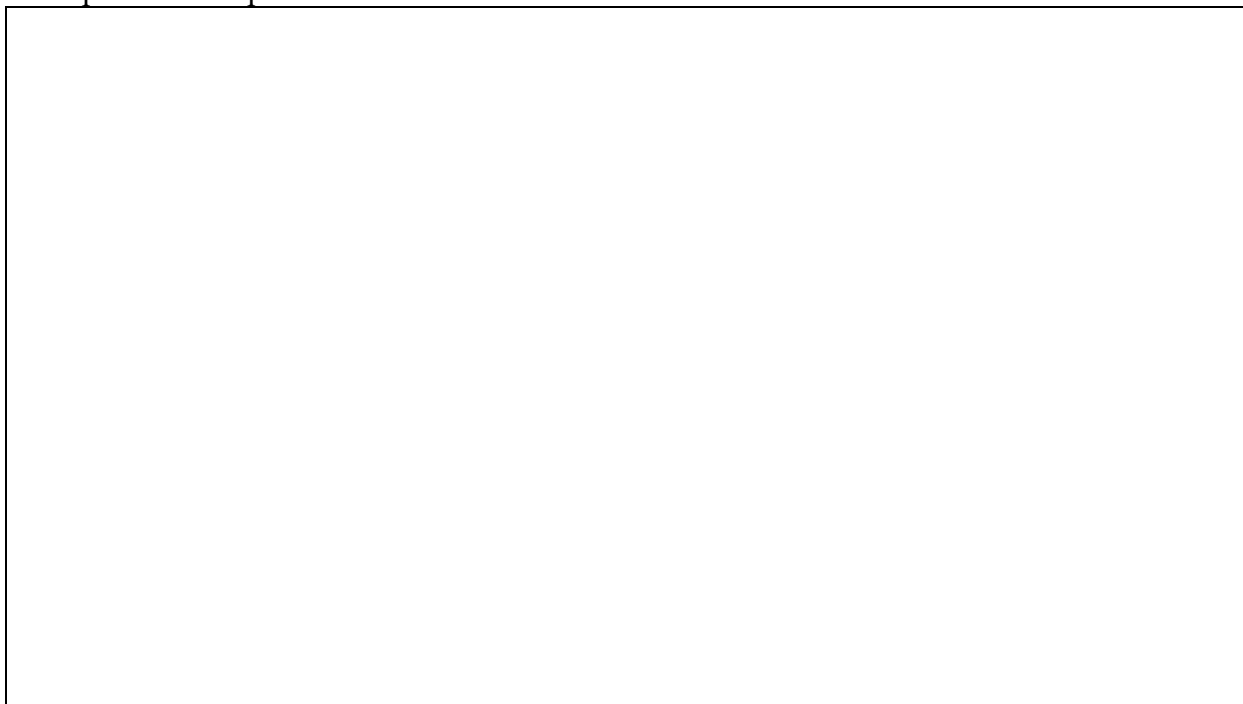
Задание 5. Войдите в привилегированный режим EXEC. Введите ep и нажмите клавишу TAB. Что отображается после нажатия клавиши TAB? _____. Это называется завершением команды (или завершение нажатием клавиши TAB). Введя часть команды, можно нажать клавишу TAB и завершить частичный ввод этой команды. Если введенных символов достаточно для уникального определения команды (например, как в случае с командой enable), оставшаяся часть будет введена автоматически. Введите te<Tab> в командной строке и отобразите результат на скриншоте. После чего введите команду enable и нажмите клавишу ввода.



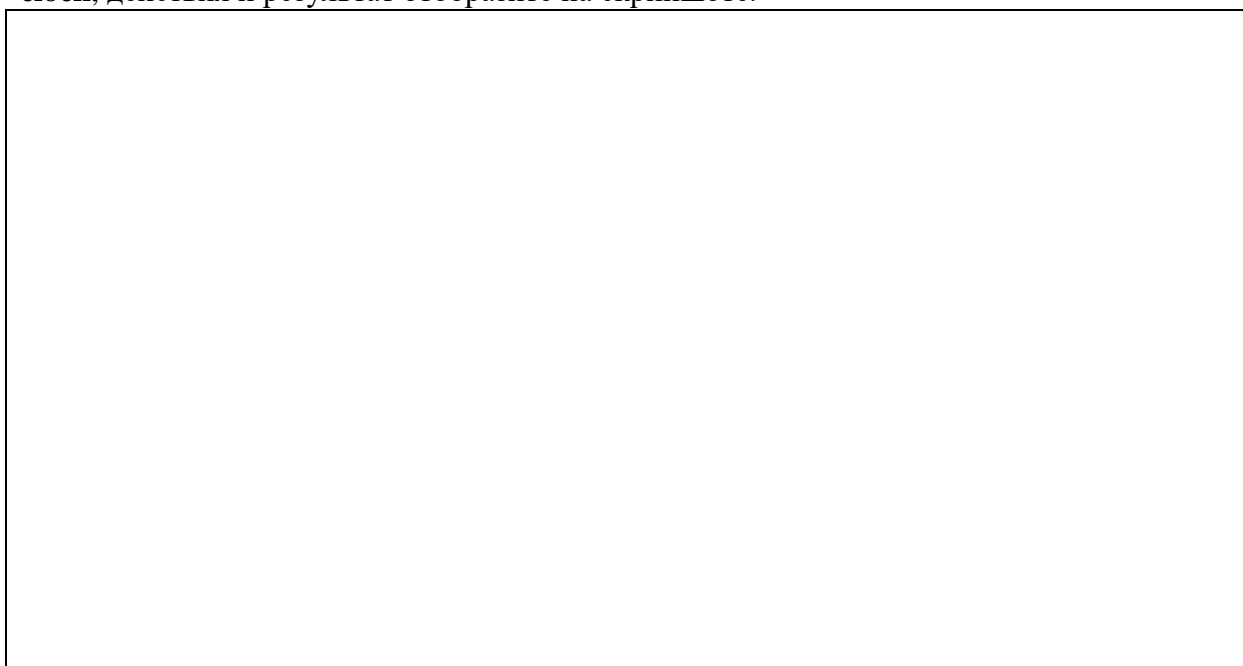
Задание 6. Войдите в режим глобальной конфигурации. В привилегированном режиме EXEC одна из команд, начинающихся с буквы «c», — configure. Введите либо команду полностью, либо столько символов, сколько будет нужно для уникального определения команды. Нажмите клавишу <Tab>, чтобы выполнить команду, и нажмите клавишу ввода. Нажмите клавишу ввода, чтобы принять параметр по умолчанию, заключенный в квадратные скобки, —[terminal]. Отобразите на скриншоте, как изменилась командная строка.



Задание 7. Используйте команду **clock**, чтобы подробнее изучить справку и синтаксис команды. Введите **show clock** в привилегированном режиме EXEC. Результат отобразите на скриншоте.



Используйте контекстную справку и команду **clock**, чтобы установить текущее время на коммутаторе. Введите команду **clock** и нажмите клавишу ввода. IOS вернет сообщение «% Incomplete command». Это означает, что для команды **clock** требуются дополнительные параметры. В справке можно получить дополнительные сведения, если ввести после команды пробел и вопросительный знак (?). Настройте время с помощью команды **clock set**. Взяв за основу сведения, запрошенные при помощи команды **clock set ?**, введите время текущее время в 24-часовом формате (например, 15:00:00). Система может вернуть запрос на получение дополнительных сведений. Попробуйте установить текущую дату, используя запрошенный формат. По окончании выполните команду **show clock**, действия и результат отобразите на скриншоте.



Задание 8. Проверка конфигурации коммутатора по умолчанию. Войдите в привилегированный режим EXEC. Щелкните S1 и откройте вкладку CLI. Нажмите клавишу ввода. Перейдите в привилегированный режим EXEC, выполнив команду **enable**. Обратите внимание, что командная строка изменилась, отображая переключение в привилегированный режим EXEC. Изучите текущую конфигурацию коммутатора. Введите команду **show running-config**. Ответьте на следующие вопросы:

1. Сколько у коммутатора интерфейсов Fast Ethernet? _____
2. Сколько у коммутатора интерфейсов Gigabit Ethernet? _____
3. Каков диапазон значений, отображаемых в vty-линиях? _____
4. Какая команда отображает текущее содержимое энергонезависимого ОЗУ (NVRAM)?

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

Задание 9. Настройка основных параметров коммутатора.

Присвойте коммутатору имя (состоящее из инициалов и фамилии студента). Команду и результат выполнения отобразите на скриншоте.

Обеспечьте безопасный доступ к консоли. Для безопасного доступа к консоли перейдите в режим config-line и установите для консоли пароль. Команду и результат выполнения отобразите на скриншоте.

Убедитесь, что доступ к привилегированному режиму защищен. Выполните команду **exit**, чтобы выйти из коммутатора. Нажмите <Enter>, после чего вам будет предложено ввести пароль. Первый пароль — это пароль для консоли, который был задан для **line con 0**. Введите этот пароль, чтобы вернуться в пользовательский режим EXEC. Введите команду для доступа к привилегированному режиму. Введите второй пароль, который был задан для ограничения доступа к привилегированному режиму EXEC. Проверьте конфигурацию, изучив содержимое файла **running-configuration**.

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.

Настройте зашифрованный пароль для доступа к привилегированному режиму. Пароль **enable password** нужно заменить на новый зашифрованный пароль с помощью команды **enable secret**. Установите пароль к привилегированному режиму. 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**.

Убедитесь в том, что пароль **enable secret** добавлен в файл конфигурации. Введите команду **show running-config** еще раз, чтобы проверить новый пароль **enable secret**. Команду **show running-config** можно сократить до **show run**.

Что отображается в качестве пароля enable secret? _____

Почему пароль enable secret отображается не так, как было задано? _____

Зашифруйте пароли enable и console. Как было видно ранее, пароль **enable secret** зашифрован, а пароли **enable password** и **console** хранятся в виде обычного текста. Зашифруйте эти открытые пароли с помощью команды **service password-encryption**. Если установить на коммутаторе другие пароли, они будут храниться в файле конфигурации в виде обычного текста или в зашифрованном виде? Дайте пояснение. _____

Задание**. Найдите в сети Интернет сервисы расшифровки паролей, зашифрованных методом **service password-encryption**.

3 ПОСТРОЕНИЕ ПРОСТЕЙШИХ ТОПОЛОГИЙ

Введем в схему коммутатор и подключим к нему два компьютера, как на рисунке 2. Его можно найти во вкладке Network Devices, далее Switches, выбираем модель 2960.

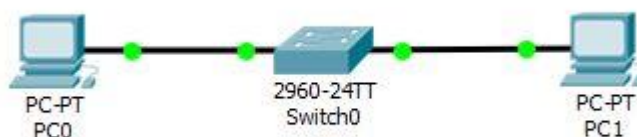
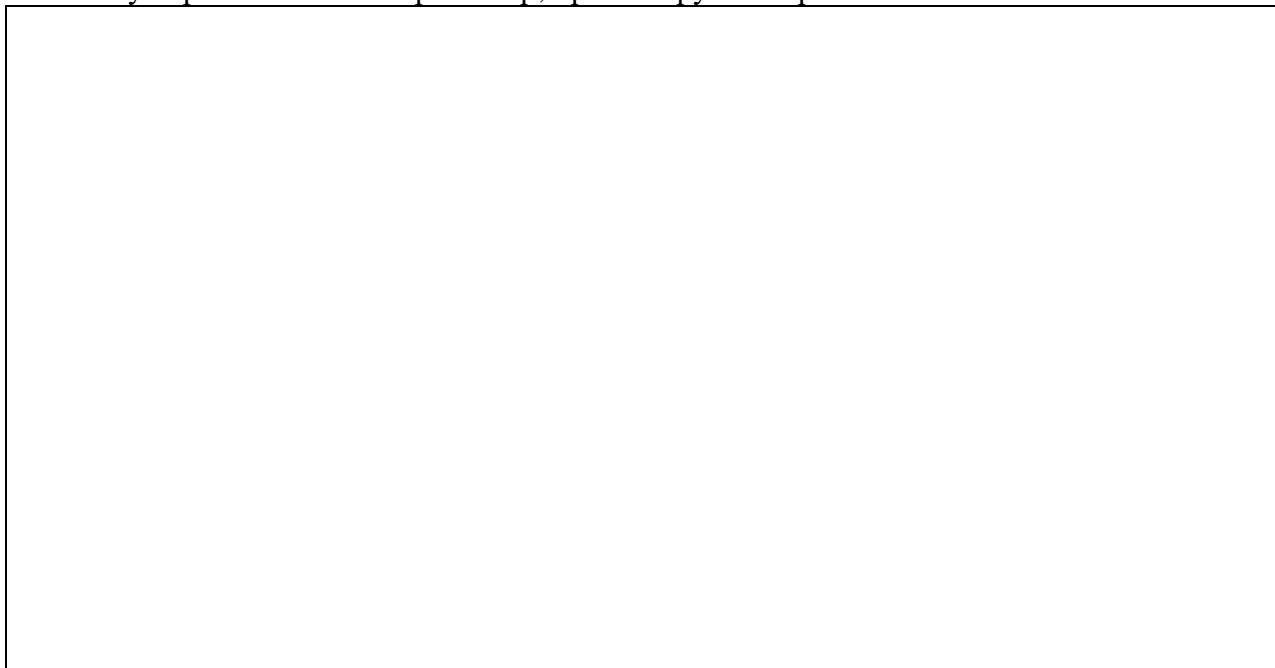


Рисунок 2 – Топология сети с коммутатором

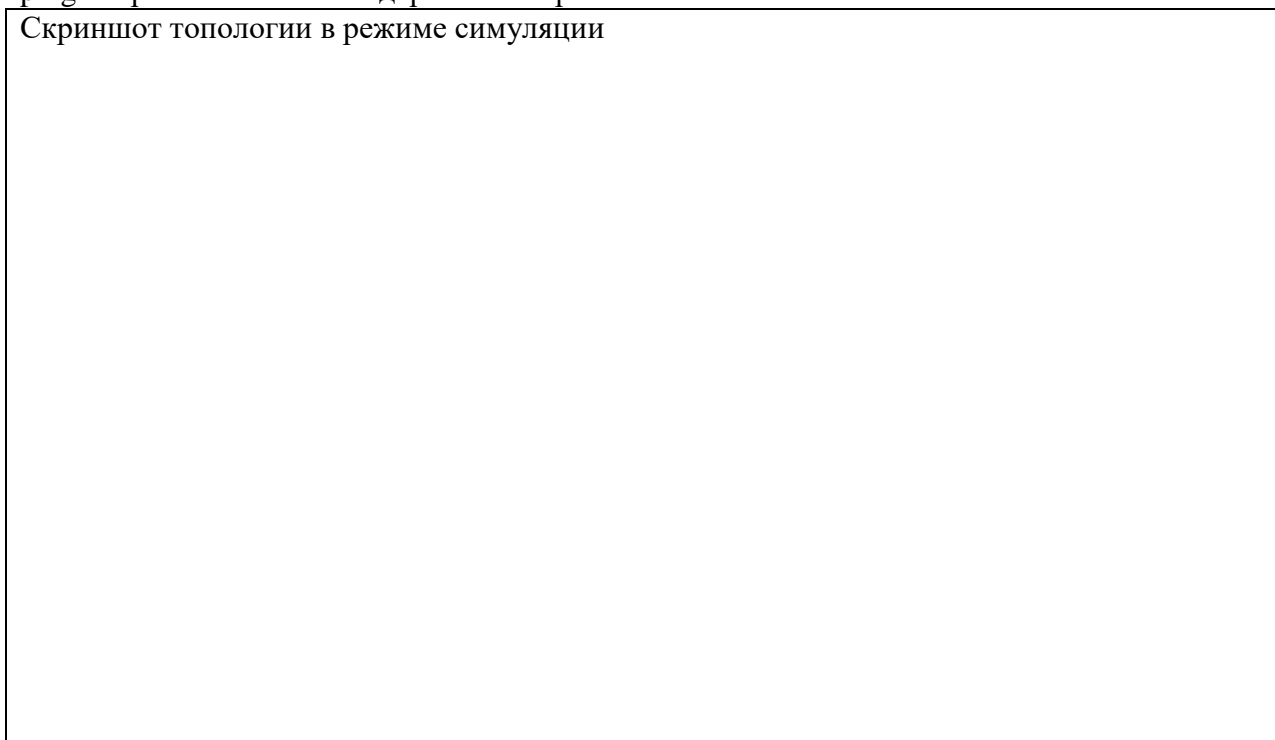
Задание 10. Постройте простейшую топологию по описанному выше примеру, используя прямой кабель и кроссовер; протестируйте ее работоспособность.



Такую топологию рассмотрим в режиме симуляции. Отличие от режима реального времени заключается в том, что в режиме симуляции можно наблюдать за перемещением каждого пакета, посмотреть его заголовки и содержимое. Активируется он в правом нижнем углу при помощи кнопки со знаком таймера. В появившейся вкладке можно настроить фильтры захватываемых пакетов, управлять скоростью симуляции, собственно запускать и останавливать ее. Там же находится список захваченных пакетов, согласно фильтрам. Настроим фильтры на захват пакетов протоколов ARP, DNS, FTP, HTTP, HTTPS, ICMP, SMTP, TCP, UDP.

Задание 2. Постройте описанную выше топологию, запустите в режиме симуляции ping-запрос и покажите содержимое образовавшегося ARP-пакета.

Скриншот топологии в режиме симуляции



Скриншот ARP-запроса

Скриншот ICMP-запроса

Контрольные вопросы:

1. Какие способы подключения к коммутатору вы знаете? В чем их различие?
2. Какие настройки позволят подключаться к коммутатору сразу в привилегированном режиме?
3. Что находится в файлах `running-config` и `startup-config`?
4. Какие типы памяти используются коммутатором и для чего?
5. Каков механизм и порядок загрузки коммутатора?
6. Как предотвратить несанкционированный доступ к устройству Cisco через консольный порт?
7. В чем различие между режимами симуляции и реального времени в СРТ?

Студент:		Допуск:	
Отчет по лабораторной работе №5 «Настройка маршрутизаторов и коммутаторов в СРТ»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Получить навыки построения топологий с применением VLAN

Задачи работы:

Краткий конспект теоретической части:

VLAN:

IEEE 802.1q:

Управляемый коммутатор:

Назначение access-порта:

Назначение trunk-порта:

native или первый VLAN:

1 ПОДКЛЮЧЕНИЕ МАРШРУТИЗАТОРА К ЛОКАЛЬНОЙ СЕТИ (LAN)

Исходные данные в этой задаче – топология (рисунок 1) и таблица адресации.

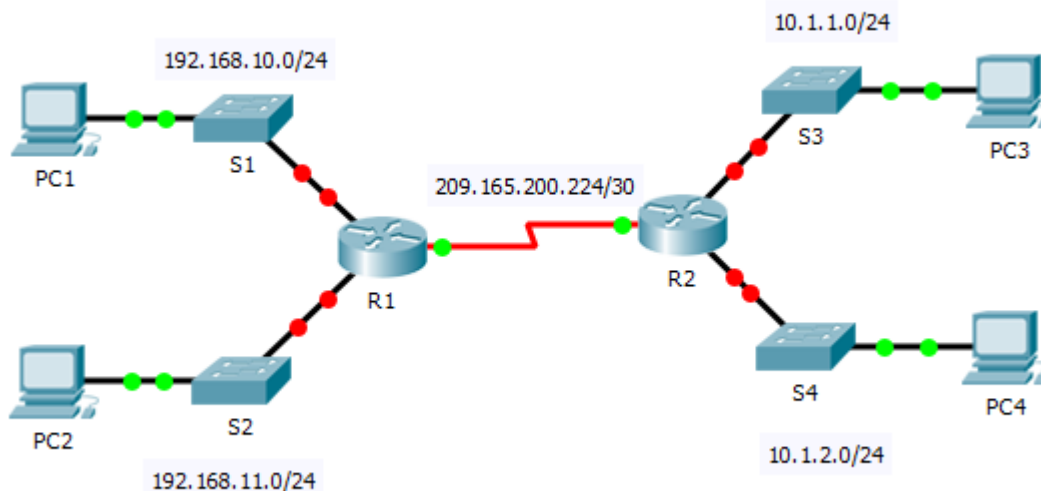


Рисунок 1 – Исходная топология

Таблица 1 – Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	
	G0/1	192.168.11.1	255.255.255.0	
	S0/0/0	209.165.200.225	255.255.255.252	
R2	G0/0	10.1.1.1	255.255.255.0	
	G0/1	10.1.2.1	255.255.255.0	
	S0/0/0	209.165.200.226	255.255.255.252	
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Задание 1. Разместите узлы топологии и соедините их. Покажите на скриншоте добавленный модуль к маршрутизаторам и состояние всех интерфейсов маршрутизатора.

Задание 2. Настройте адресацию всех интерфейсов всех узлов согласно таблице адресации. На скриншотах покажите результат такой настройки.

Задание 3. Покажите на скриншоте состояние таблицы маршрутизации на текущий момент и результаты отправки эхо-запросов с PC1 на PC2 и на PC3.

Задание 4. Добавьте необходимые статические маршруты. Покажите на скриншотах таблицы маршрутизации обоих роутеров.

Задание 5. Проследите путь ICMP-запроса из одного сегмента сети в другой. Покажите его результат на скриншоте. Как меняются заголовки канального уровня при переходах от одного узла к другому?

1 РАЗДЕЛЕНИЕ СЕТЕЙ НА ПОДСЕТИ

В этом упражнении вам предоставляется сетевой адрес 192.168.n.0/24 для подсети (n – номер варианта), и вы должны составить схему IP-адресации сети, изображенной в топологии. Для каждой локальной сети (LAN) в сети требуется достаточно пространства для, по крайней мере, 25 адресов для оконечных устройств, коммутатора и маршрутизатора. Для соединения между маршрутизаторами R1 и R2 потребуется по одному IP-адресу на каждом конце канала.

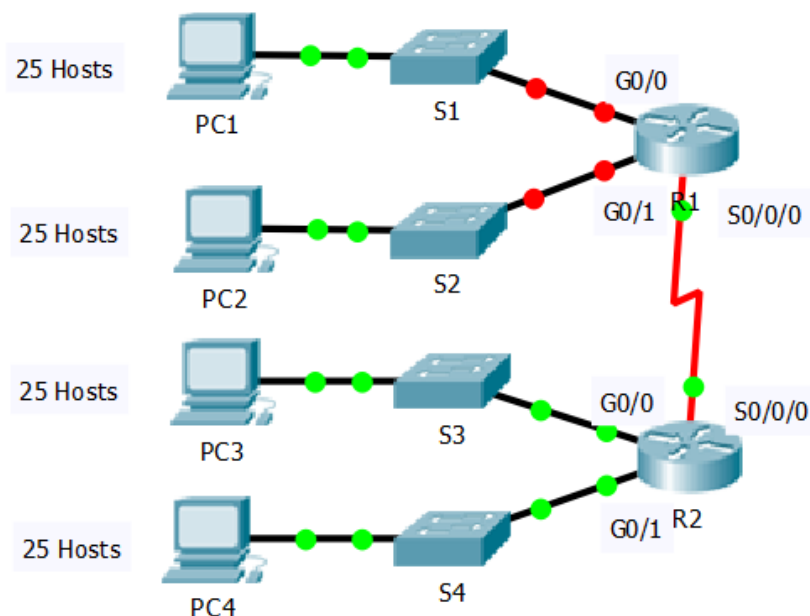


Рисунок 2 – Исходная топология

Таблица 2 – Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0			
	G0/1			
	S0/0/0			
R2	G0/0			
	G0/1			
	S0/0/0			
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			

Задание 1. Разбейте сеть 192.168.100.0/24 на нужное количество подсетей.

Сколько потребуется подсетей в соответствии с имеющейся топологией? _____

Сколько бит необходимо заимствовать для поддержки нескольких подсетей в таблице топологии? _____

Сколько в результате этого создается подсетей? _____

Сколько при этом в каждой подсети будет доступно узлов? _____

Заполните таблицу подсетей, перечислив десятичные значения всех доступных подсетей, первый и последний используемый адрес узла, и широковещательный адрес.

Номер	Адрес подсети	Первый используемый адрес узла	Последний используемый адрес узла	Широковещательный адрес

Задание 2. Выберите подсети для заданной топологии.

Назначьте подсеть 1 локальной сети, подключённой к интерфейсу GigabitEthernet 0/1 маршрутизатора R1. _____

Назначьте подсеть 2 локальной сети, подключённой к интерфейсу GigabitEthernet 0/0 маршрутизатора R1. _____

Назначьте подсеть 3 локальной сети, подключённой к интерфейсу GigabitEthernet 0/0 маршрутизатора R2. _____

Назначьте подсеть 4 локальной сети, подключённой к интерфейсу GigabitEthernet 0/1 маршрутизатора R2. _____

е. Назначьте подсеть 5 каналу WAN между маршрутизаторами R1 и R2.

Задание 3. Заполните таблицу адресации.

Задание 4. Проверьте работоспособность сети.

3 Сегментация виртуальных локальных сетей

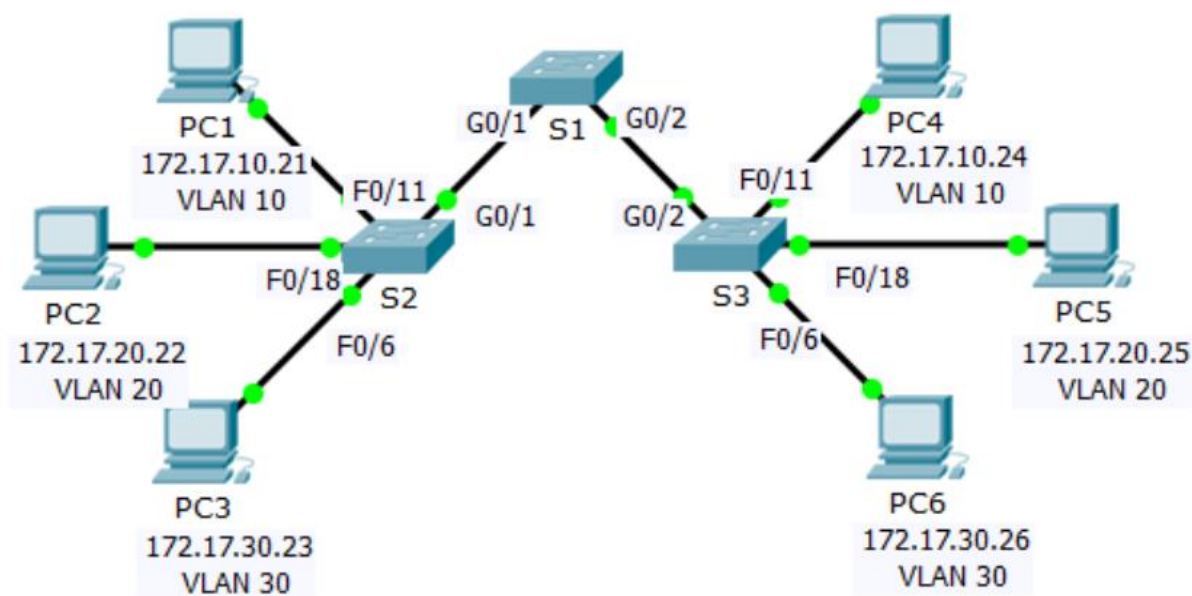


Таблица 1 – Команды для настройки VLAN

sw1(config)# vlan 2	Создание VLAN-а
sw1(config-vlan)# name test	Задание имени VLAN
sw1(config)# interface range fa0/1 - 2	Выбор диапазона интерфейсов для последующего конфигурирования
sw1(config-if)# switchport mode access	Выбор режима access для интерфейса
sw1(config-if)# switchport mode trunk	Выбор режима trunk для интерфейса
sw1(config-if)# switchport mode dynamic auto	Выбор режима DTP(Dynamic Trunk Protocol) для интерфейса
sw1(config-if)# switchport mode dynamic desirable	
sw1(config-if)# switchport nonegotiate	
sw# show dtp interface	Просмотр текущего режима DTP
sw1(config-if)# switchport access vlan 2	Настройка VLAN для интерфейса
sw1# show vlan brief	Просмотр информации о VLANax
sw1# show interfaces trunk	Просмотр информации о магистральных каналах
sw1(config-if)# switchport trunk native vlan 5	Изменение Native VLAN

Задание 1. Построить указанную топологию, настроить access и trunk порты. Показать конфигурационный файлы коммутаторов. Проследите движение трафика из одной сети в другую, обратив внимание на присвоение тега 802.Q

Задание 2. Заменить коммутатор S1 на маршрутизатор. Показать, как изменятся конфигурационные файлы.

Задание 3. Заменить маршрутизатор на коммутатор 3его уровня. Покажите движение ARP или ICMP запроса из одной сети в другую.

Студент:		Допуск:	
Отчет по лабораторной работе №6 «Настройка топологии сети небольшой компании»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Получить навыки построения топологий с применением VLAN

Задачи работы:

<hr/> <hr/> <hr/>

Краткий конспект теоретической части:

Общая концепция STP:

<hr/> <hr/> <hr/> <hr/> <hr/>

STP vs PVST vs RSTP:

<hr/> <hr/> <hr/> <hr/> <hr/>

Router-on-a-stick:

<hr/> <hr/> <hr/> <hr/> <hr/>

Протокол OSPF:

<hr/> <hr/> <hr/> <hr/> <hr/>

Протокол EIGRP:

<hr/> <hr/> <hr/> <hr/> <hr/>

Протокол BGP:

<hr/> <hr/> <hr/> <hr/> <hr/>

ПОСТРОЕНИЕ СЕТИ НЕБОЛЬШОЙ КОМПАНИИ

Постройте сеть согласно топологии, представленной на рисунке 1:

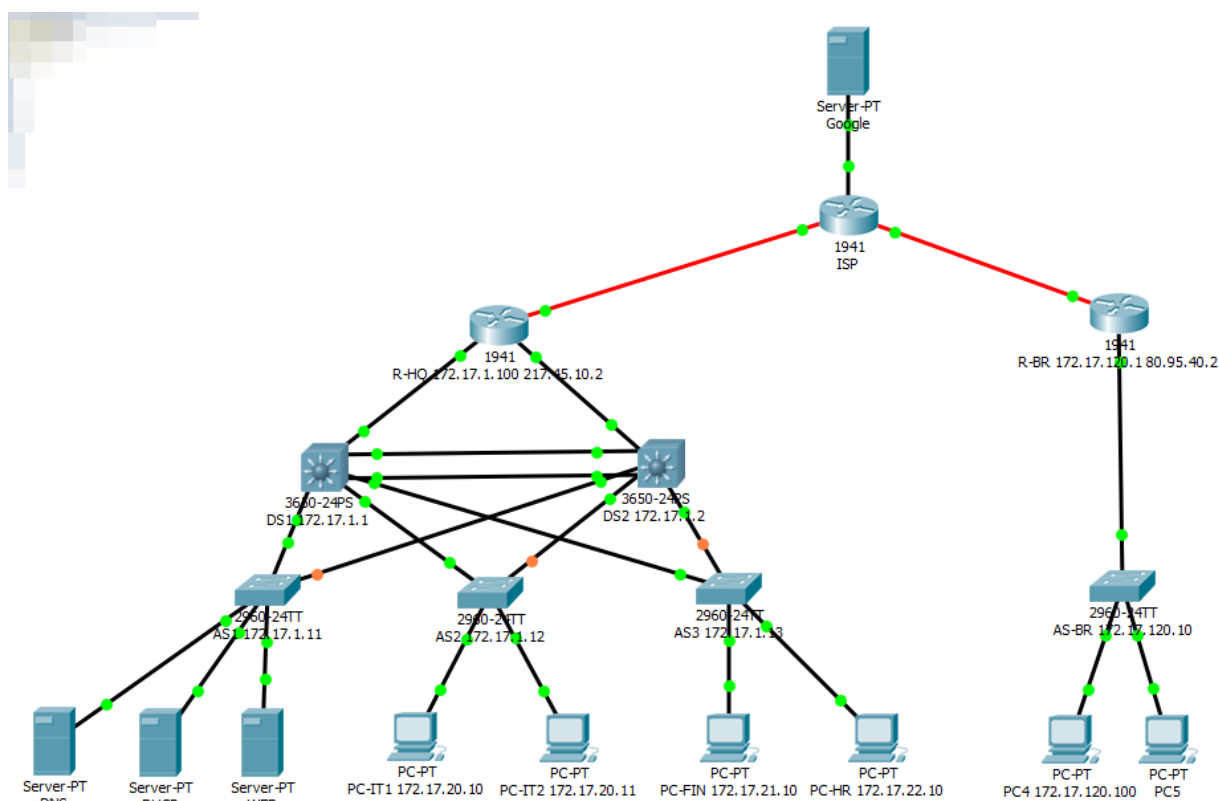


Рисунок 1- Общая топология сети

По согласованию разрешается вносить небольшие изменения, не нарушающие целевой функционал. При этом необходимо представить итоговую топологию сети.

1. Представить таблицу адресного пространства. Второй октет всех сетей должен соответствовать номеру варианта.
2. Представить листинги конфигурации всех сетевых устройств.
3. Перечислить технологии, применяемые для организации сетевого доступа.
4. Представить результаты show-команд и результатов эхо-запросов для проверки работоспособности служебных функций сети (VLAN, маршрутизация, NAT) и пользовательского доступа к сети. С компьютеров главного офиса и филиала должен быть настроен тоннель между филиалами и доступ в интернет.

Дополнительные задания, не описанные в методичке. Не обязательны к выполнению, однако за них можно получить бонус за сложность:

1. Настроить DHCP в сети главного офиса.
2. Настроить DNS в сети главного офиса, проверить разрешение доменного имени google.ru в IP-адрес 8.8.8.8.
3. Максимально уменьшить время сходимости STP за счет изменений таймеров.
4. Добавить в сеть офиса резервный маршрутизатор и настроить HSRP.
5. Настроить получение от провайдера маршрутной информации по BGP.

Контрольные вопросы:

1. Каков принцип работы технологии EtherChannel?
2. Что произойдет, если не указывать SVI пассивными интерфейсами для OSPF?
3. Почему после настройки EIGRP из таблицы маршрутизации R-HQ пропали маршруты, полученные по OSPF от DS1?
4. Каков принцип работы технологии GRE? Является ли она VPN?

Студент:		Допуск:	
Отчет по лабораторной работе №6 «Построение типовой топологии филиала»			
Дата выполнения		Дата защиты	
Оценка		Подпись	

Цель работы:

Получить навыки построения типовых топологий сети

Задачи работы:

Краткий конспект теоретической части:

Комплект документации:

ISO 27001:

Принцип «пяти девяток»:

Понятие SLA:

Понятие QOS:

IPSec:

1 ПРОЕКТ СЕТИ

Большинство компаний относится к предприятиям малого бизнеса. Соответственно, основная часть сетей — это небольшие сети.

Проектирование небольших сетей, как правило, не вызывает трудностей. Количество устройств в таких сетях и их типов существенно меньше по сравнению с большими сетями. Топологии таких сетей включают обычно один маршрутизатор, а также один или несколько коммутаторов. В небольших сетях также могут иметься беспроводные точки доступа (могут быть встроены в маршрутизатор) и IP-телефоны. Для соединения с Интернетом в небольшой сети обычно предусматривается одно WAN-подключение, реализованное посредством DSL-соединения, кабеля или Ethernet-соединения.

Для управления небольшими сетями требуются преимущественно те же навыки, что и для управления большими сетями. Основную часть работы составляют обслуживание, диагностика и устранение неисправностей существующего оборудования, а также обеспечение безопасности устройств и данных в сети. Управление небольшой сетью осуществляется сотрудником компании или лицом, привлеченным компанией на контрактной основе, в зависимости от масштаба предприятия и его типа.

В целях соответствия требованиям пользователей даже для небольших сетей требуется планирование и проектирование. На этапе планирования рассматриваются и учитываются все требования, стоимость и возможности внедрения.

В рамках реализации небольшой сети при проектировании необходимо в первую очередь учитывать тип промежуточных устройств, которые будут использоваться для поддержки сети. При выборе таких устройств нужно учесть ряд факторов, как показано на рисунке.

Стоимость коммутатора зависит от его производительности и функций. Под производительностью устройства подразумевается количество портов и их типы, а также производительность внутренней шины. Другие факторы, влияющие на стоимость оборудования - возможности сетевого управления, встроенные технологии безопасности и дополнительные продвинутое технологии коммутации. Следует также учитывать и стоимость прокладки кабелей, необходимых для подключения всех устройств к сети. Другим немаловажным фактором, влияющим на стоимость сети, является уровень резервирования, которым должна обладать сеть.

Скорость и типы портов (интерфейсов). Выбор количества и типа портов маршрутизатора или коммутатора имеет критическое значение. В более новых моделях компьютеров предусмотрены встроенные сетевые платы 1 Гбит/с. Некоторые рабочие станции и серверы уже оснащены портами 10 Гбит/с. Хотя при выборе устройств 2-го уровня, которые могут работать на более высоких скоростях, объем затрат возрастает, но это позволяет расширять сеть без замены центральных устройств.

Расширяемость. Сетевые устройства выпускаются в фиксированной и модульной конфигурации. В фиксированной конфигурации строго определены количество и тип портов или интерфейсов. У модульных устройств есть слоты расширения, позволяющие добавлять новые модули. Существуют коммутаторы, оснащенные дополнительными портами для создания высокоскоростных восходящих каналов. С помощью маршрутизаторов можно объединять сети различных типов. Следует внимательно подходить к выбору модулей и интерфейсов, подходящих для определенной среды.

Функции и сервисы операционной системы. В зависимости от версии операционной системы сетевое устройство может поддерживать различные функции и сервисы, например:

- безопасность;
- качество обслуживания (QoS);
- голос через IP (VoIP);
- коммутация уровня 3;

- преобразование сетевых адресов (NAT);
- протокол динамической конфигурации узла сети (DHCP).

В рамках развертывания небольшой сети необходимо планировать адресное пространство IP. Все узлы в пределах сети организации должны иметь уникальный адрес. Схему IP-адресации необходимо планировать, документировать и поддерживать в актуальном состоянии с учетом типа устройств, получающих адрес.

Примеры различных типов устройств, которые учитываются при проектировании схемы IP-адресации:

- устройства для конечных пользователей;
- серверы и периферийные устройства;
- узлы, доступные из интернета;
- промежуточные устройства.

Планирование и документирование схемы IP-адресации позволяет администраторам отслеживать устройства по типам. Например, если всем серверам назначается адрес узла в пределах диапазона 50–100, трафик сервера можно будет с легкостью отследить по IP-адресу. Это особенно удобно, если устранять неполадки, связанные с сетевым трафиком, с помощью анализатора протоколов.

Кроме того, при использовании детерминированной схемы IP-адресации администраторы смогут более качественно контролировать доступ к ресурсам сети по IP-адресам. Это имеет особенно большое значение для узлов, предоставляющих ресурсы как внутренним сетям, так и внешней сети. Такую роль выполняют веб-серверы или серверы электронной коммерции. Если адреса этих ресурсов не спланированы и не задокументированы, контроль безопасности и доступности устройств существенно усложняется. Если серверу назначен произвольный адрес, этот адрес трудно заблокировать, и клиенты могут столкнуться с определенными трудностями при поиске этого ресурса.

Для таких различных типов устройств необходимо выделить логический блок адресов в пределах диапазона адресов сети.

Другим важным фактором при проектировании сети является обеспечение ее надежности. Даже работа малых предприятий очень часто в большой степени зависит от сети. Сбой в работе сети может повлечь значительные затраты. Чтобы обеспечить высокую степень надежности, при проектировании сети необходимо резервирование. Резервирование позволяет устранить единые точки отказа. Резервирование в сети осуществляется множеством различных способов. Это может быть резервное оборудование или же резервные сетевые каналы на критически важных участках, как показано на рисунке.

В небольших сетях обычно имеется единая точка выхода в Интернет, реализуемая через один или несколько шлюзов по умолчанию. Однако в случае сбоя в работе маршрутизатора без подключения к Интернету остается вся сеть. В связи с этим малым предприятиям можно порекомендовать приобрести в качестве резервного соединения пакет услуг у другого провайдера.

При проектировании сети администратор должен учитывать различные типы трафика и их обработку. Маршрутизаторы и коммутаторы в небольшой сети необходимо настроить так, чтобы поддержка трафика данных, передаваемых в режиме реального времени (например, голоса или видео), осуществлялась отдельно от поддержки трафика других данных. Фактически при качественном проектировании сети трафик четко классифицируется в соответствии с приоритетностью, как показано на рисунке 1. В конечном счете целью нового проекта сети (даже небольшой) являются повышение эффективности работы сотрудников и сведение к минимуму времени простоя сети.

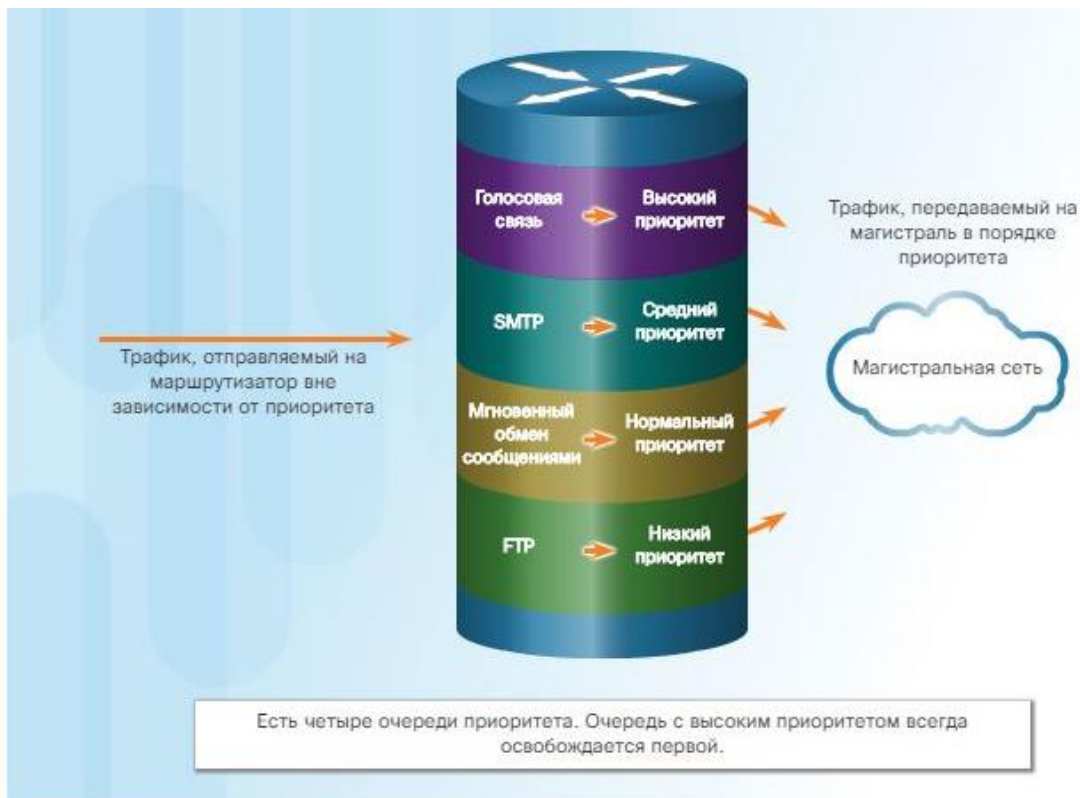


Рисунок 1 – Приоритезация трафика

Большая часть работы технического специалиста в рамках небольшой или большой сети так или иначе связана с сетевыми протоколами. Сетевые протоколы поддерживают приложения и службы, используемые сотрудниками в небольших сетях. Наиболее распространенные сетевые протоколы: DNS, SSH, DHCP, протоколы электронной почты, веб-протоколы, протоколы обмена файлами.

Эти сетевые протоколы содержат основной набор инструментов сетевого специалиста. Политика безопасности многих компаний требует по возможности использовать безопасные версии этих протоколов. К таким протоколам относятся HTTPS, SFTP и SSH.

Расширение - естественный процесс для многих малых предприятий, поэтому используемые в них сети должны расти и развиваться соответственно. Желательно, чтобы у администратора сети было достаточно времени для принятия взвешенных решений относительно расширения сети по мере развития компании:

- для масштабирования сети требуется ряд элементов;
- сетевая документация - физическая и логическая топологии;
- реестр устройств - список устройств, использующих или образующих сеть;
- бюджет - детализированный бюджет на ИТ, включая бюджет на закупку оборудования на финансовый год;
- анализ трафика - протоколы, приложения и службы, а также их требования к трафику; должны быть задокументированы

Эти элементы используются для принятия взвешенных решений в рамках масштабирования небольшой сети.

Разберемся теперь, как будут реализованы конкретные требования в данной ситуации. Требование 200 рабочих мест на этаже по 20 в комнате диктует нам минимальное число портов коммутаторов уровня доступа, которые необходимо разместить в здании, а также размер топологии. При использовании 24-портовых коммутаторов 2960 или 3750 в каждой комнате понадобится 10 таких. Над ними

хорошо бы поставить два коммутатора уровня распределения с перекрестными линками для обеспечения отказоустойчивости. Inter-VLAN маршрутизация может выполняться как на коммутаторах третьего уровня, так и на маршрутизаторах уровня ядра. Для серверов DNS и DHCP можно выделить отдельные серверы, а можно настроить тот же маршрутизатор.

2 ПОСТАНОВКА ЗАДАЧИ И ИСХОДНЫЕ ДАННЫЕ

Постановка задачи в данном случае имеет форму пожеланий директора предприятия по развертыванию инфраструктуры типового филиала. Такая задача ставится техническому директору, однако ее решение трудоемко и не может быть выполнено в рамках одной лабораторной работы. Поэтому к исходным данным добавится уже разработанная документация, а студенту предлагается принять на себя роль помощника технического директора и написать конфигурационные файлы для инициализации оборудования в таких филиалах.

В качестве исходных данных имеются эскизный проект (рисунок 2) и описание реализуемого функционала.

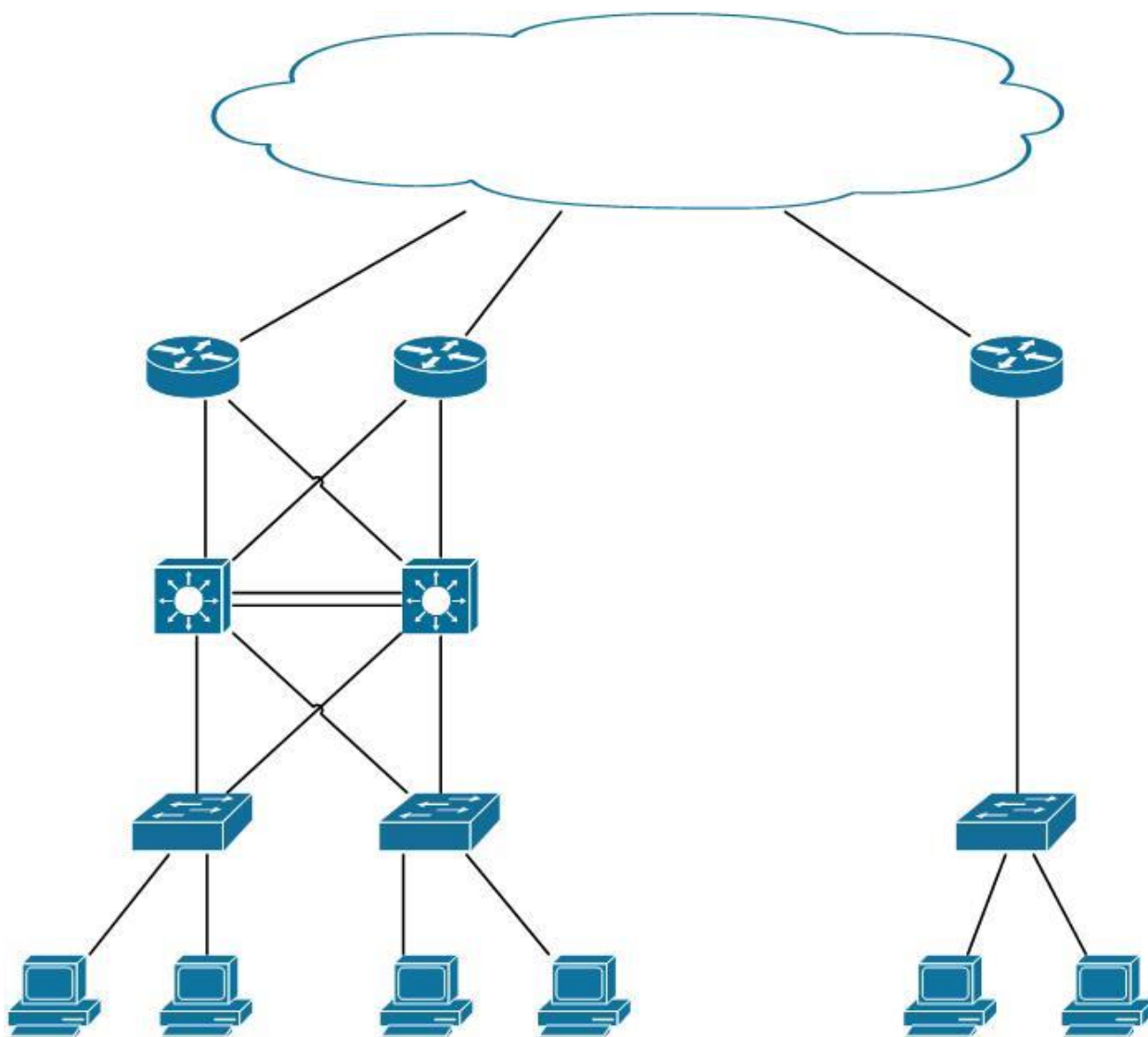


Рисунок 2 – Основа эскизного проекта топологии филиала

Данную топологию необходимо дополнить, обозначив на ней интерфейсы подключения и адресное пространство, а также роли серверов.

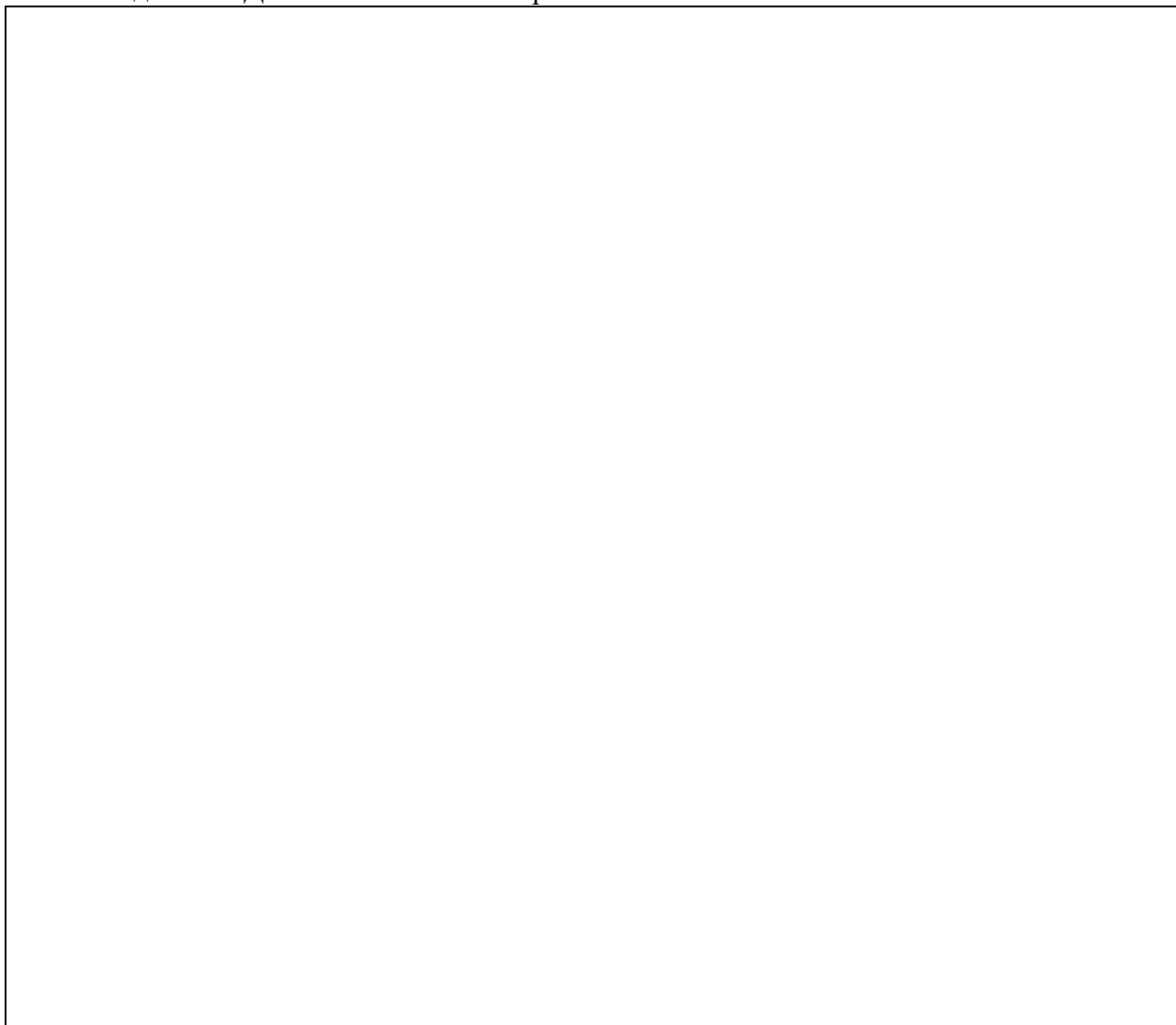
После чего необходимо заполнить таблицу для каждого устройства, указав для каждого устройства адреса и маски подсети на его интерфейсах.

Задание 1. Разработайте логическую адресацию показанных устройств. Адреса необходимо выделить также на интерфейсы управления коммутаторами и на loorback-интерфейсы маршрутизаторов. Номера VLAN выбрать согласно своему варианту (n*10 и n*20, n*30), они должны быть отражены в IP-адресах.

Задание 2. Заполните таблицу для каждого устройства, указав адресацию на их интерфейсах.

Устройство	Интерфейс	Адрес/маска

Задание 3. Дополните эскизный проект.



Команды для создания VLAN, access и trunk портов Вам уже известны. Двойной линк между свитчами можно настроить в режиме Etherchannel, а можно при помощи протокола Rapid PVST+, решение отдается в Ваши руки.

Для создания DHCP пула адресов на маршрутизаторе можно воспользоваться командой `ip dhcp pool pool_name`, после ввода которой Вы попадете в режим редактирования пула DHCP, в котором обязательно должен быть определен диапазон адресов и шлюз по умолчанию. Остальные настройки опциональны. Основные команды настройки пула указаны в таблице 1. Например, IPv4-адрес DNS-сервера, доступный DHCPv4-клиенту, настраивается с помощью команды `dns-server`. Команда `domain-name` домен используется, чтобы задать доменное имя. Продолжительность аренды протокола DHCPv4 изменяется командой `lease`. По умолчанию продолжительность аренды равна одному дню. Чтобы задать сервер NetBIOS WINS, используется команда `netbios-name-server`.

Таблица 1 – команды настройки протокола DHCP

Команда	Описание
<code>(config)# ip dhcp excluded-address</code>	Исключает адреса из пула выдачи
<code>(config)# ip dhcp pool pool-name</code>	Создание адресного пула
<code>(config-pool)# network network_address [mask /prefix]</code>	Определение диапазона адресов пула
<code>(config-pool)# default-router address [address2...address8]</code>	Определение шлюза по умолчанию
<code>dns-server address [address2...address8]</code>	Назначение DNS-сервера
<code>lease {days [hours][minutes] infinity}</code>	Определение срока аренды адреса
<code>domain-name domain</code>	Назначение доменного имени

Служба DHCP включена по умолчанию. Для того чтобы отключить службу, введите команду в режиме глобальной конфигурации по `service dhcp`. Для возобновления работы DHCP-сервера используйте команду в режиме глобальной конфигурации `service dhcp`. В случае, если параметры не настроены, активация службы не имеет эффекта.

Таблица 2 – команды проверки работы протокола DHCP

Команда	Описание
<code>#show running-config section dhcp</code>	Текущая конфигурация DHCP
<code>#show ip dhcp binding</code>	Список всех привязок IP-адресов к MAC-адресам
<code>#show ip dhcp server statistics</code>	Принятые и отправленные DHCP сообщения
<code>#show ip dhcp conflicts</code>	Возникшие конфликты при работе протокола DHCP

Команда `ipconfig /all`, запущенная на PC, отображает параметры TCP/IP. Поскольку PC подключен к сегменту сети, он автоматически получает суффикс DNS, IPv4-адрес, маску подсети, шлюз по умолчанию и адрес сервера DNS из этого пула. Специальная настройка интерфейса маршрутизатора для DHCP не требуется. В случае если компьютер подключен к сегменту сети с доступным пулом DHCPv4, он может получить IPv4-адрес из пула автоматически.

Маршрутизация между VLAN-ами будет осуществляться роутером, расположенным ближе к локальной сети. Для этого на одном физическом интерфейсе, подключенном к коммутатору, необходимо настроить подинтерфейсы (sub-interfaces) для каждого из VLANов, которые будут для этих VLANов шлюзами по умолчанию. Команды для настройки подинтерфейсов предлагается найти самостоятельно.

Задание 4. Разработать файлы инициализации устройств, включающие в себя команды CLI, которые необходимо ввести, чтобы реализовать разработанную топологию.

Задание 5. Настроить NAT на пограничном маршрутизаторе.

Задание 6. Настроить внутри сети протокол маршрутизации.

Разработанные файлы инициализации прикрепить к журналу лабораторных работ.

Контрольные вопросы:

1. Что необходимо учитывать при планировании адресного пространства?
2. Что такое PAT и PAT overload?
3. Что такое проброс портов?
4. Что такое router-on-a-stick?
5. Какова сходимость сети в случае применения различных версий протокола STP?