ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

Методические указания по выполнению курсовой работы по дисциплине

Сети электросвязи и методы их защиты

(направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи)

Ростов-на-Дону
2019

Методические указания
по выполнению курсовой работы

по дисциплине
Сети электросвязи и методы их защиты

Составители: А.А. Манин, заведующий кафедрой ИТСС.
И.А. Сосновский, доцент кафедры ИТСС.

Рассмотрено и одобрено
на заседании кафедры
Протокол от «26» августа 2019 г. № 1

Общие указания и выбор варианта

Выполнение курсовой работы направлено на закрепление знаний, полученных студентами при изучении дисциплины «Сети электросвязи и методы их защиты», посвященного принципам пакетной коммутации в сетях связи, а также на привитие навыков проектирования и настройки IP-сетей.

Оформление курсовой работы производится в соответствии с требованиями, изложенными в [1].

Каждый студент выполняет проект в одном варианте, номер варианта определяется последней цифрой студенческого билета (СБ) и одной последней цифрой текущего года (Г).

Внешний IP-адрес класса B проектируемой сети выбирается исходя из таблицы 1.

Таблица 1 – Внешний IP-адрес проектируемой сети

СБ	IP-адрес	СБ	IP-адрес
1	135.12.00	6	214.125.0.0
2	128.34.0.0	7	138.234.0.0
3	65.20.0.0	8	85.76.0.0
4	112.38.0.0	9	75.89.0.0
5	94.56.0.0	0	76.94.0.0

Количество виртуальных локальных сетей представлено в таблице 2.

Таблица 2 – Количество виртуальных локальных сетей

СБ	Кол-во VLAN	СБ	Кол-во VLAN
1	5	6	7
2	6	7	8
3	4	8	12
4	9	9	11
5	10	0	3

Внутренняя адресация сети должна использовать частные адреса класса С, до разделения проектируемой сети на подсети адрес сети определяется исходя из значения Г в соответствии с таблицей 3.

Таблица 3 – Внутренняя адресация проектируемой сети

Г				
1,0	2,9	3,6	4,7	8,5
192.168.10.0	192.168.15.0	192.168.20.0	192.168.25.0	192.168.30.0

Количество пользователей каждой VLAN определяется как сумма СБ+5. Например, студент с СБ 12 проектирует сеть, у которой количество пользователей в каждой VLAN должно быть не меньше

$$1+2+5=7.$$

VLAN организуются либо на базе коммутаторов, поддерживающих данную технологию, либо на базе маршрутизаторов, по усмотрению студента. Разделение адресного пространства между VLAN осуществляется с использованием маски переменной длины (VLSM) с учетом таблицы 2 и количества пользователей.

Маршрутизация должна осуществляться между VLAN, номера которых представлены в таблице 4, остальные VLAN должны быть изолированы друг от друга.

Таблица 4 – Номера VLAN, между которыми должна быть настроена маршрутизация.

СБ	Кол-во VLAN	СБ	Кол-во VLAN
1	1,3 4,5	6	4,5 2,7
2	2,6 3,4	7	2,5 3,4
3	1,2 3,4	8	5,10 2,8
4	1,9 2,5	9	2,9 3,7
5	1,2 8,9	0	5,9 3,10

В локальной части сети должно быть установлено не менее двух серверов, доступ к которым должен быть разграничен следующим образом. К серверу 1

должны быть подключены устройства относящиеся к нечётным номерам VLAN, а ко второму - все чётные.

Также должны быть установлены удалённые объекты, один сервер и два компьютера. Они доложены подключаться к проектируемой сети как минимум через три маршрутизатора. Адресацию для этой части сети необходимо разработать самостоятельно.

Между проектируемой сетью и удалённой необходимо настроить статическую маршрутизацию для доступа к серверу и динамическую маршрутизацию для всех остальных устройств. Для настройки динамической маршрутизации можно использовать протокол RIP или OSFP [3,4], на выбор студента.

К данному серверу необходимо обеспечить общий доступ всех компьютеров проектируемой сети. Это может быть как сервер для хранения данных, так и www-сервер.

В пояснительной записке излагается последовательность действий при проектировании и последующей настройке сети. При настройке оборудования необходимо представить скриншоты интерфейса программы. К пояснительной записке прикладывается CD-диск с файлом проекта и электронным вариантом выполненной пояснительной записки. На защите студент запускает свой файл и демонстрирует работу спроектированной и настроенной сети.

Содержание курсовой работы

Студент должен спроектировать корпоративную IP-сеть с учетом исходных данных, соответствующих его варианту. Сеть строится на базе оборудования фирмы Cisco Systems с использованием программного продукта Cisco Packet Tracer, все применяемое оборудование должно быть соответствующим образом настроено и правильно функционировать. В процессе проектирования необходимо произвести следующую работу.

1. С использованием программного продукта Cisco Packet Tracer построить схему проектируемой сети.

2. С учетом исходных данных разделить проектируемую сеть на виртуальные сети (VLAN), разделить между ними адресное пространство.

3. Сконфигурировать коммутаторы и маршрутизаторы проектируемой сети, осуществить проверку работоспособности с использованием утилит ping и tracert.

4. Настроить маршрутизацию между VLAN, указанными в исходных данных.

5. Установить в проектируемой сети сервер, настроить на нем службы DNS и DHCP, произвести автоматическое получение сетевых настроек рабочими станциями.

6. Установить внешний www-сервер, назначить ему доменное имя и IP-адрес, проверить возможность просмотра web-страницы с внутренней рабочей станции проектируемой сети.

Методические указания к выполнению проекта

Проектирование IP-сети производится на базе оборудования фирмы Cisco главным образом потому, что данная фирма разработала программный продукт, позволяющий в виртуальной среде настраивать сетевое оборудование таким же образом, как и реальное.

Настраиваемое оборудование необходимо подсоединить к компьютеру, с которого будет производиться его настройка. Для этих целей используется специальный консольный кабель, поставляемый вместе с приобретенным оборудованием. Распайка разъемов такого кабеля представлена на рисунке 1.

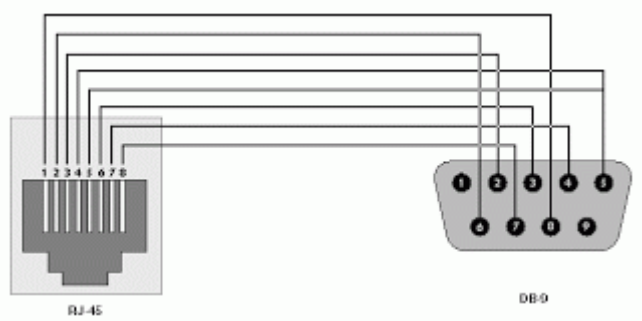

Рисунок 1 – Распайка консольного кабеля

Для связи настраиваемого оборудования с компьютером один конец консольного кабеля (тот, который оснащен сетевым коннектором RJ-45 8P8C) подключается в консольный порт сетевого оборудования (обычно над ним имеется надпись CONSOLE находящаяся в голубой каёмке), другой конец кабеля подключается к COM порту компьютера.

После того, как настраиваемое оборудование фирмы Cisco подключено к компьютеру физически, то есть с помощью кабеля, к нему можно подключиться с помощью специального программного обеспечения и производить его настройку. В качестве такого программного обеспечения можно использовать HyperTerminal, Putty и д.р. При использовании Putty в разделе "Connection Type" необходимо выбрать вариант "Serial", в поле "Serial Line" указать номер COM порта, к которому подключено устройство (если к первому, то COM1, если ко второму, то COM2 и т.д.). Значение поля Speed оставьте без изменений как 9600 (рисунок 2).

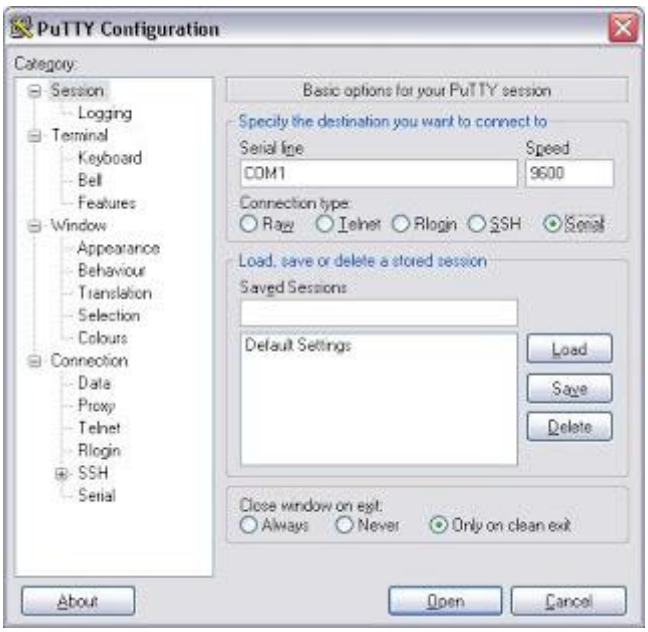

Рисунок 2 – Подключение к оборудованию через последовательный интерфейс

После того, как все параметры выставлены в соответствии с приведенным выше описанием, необходимо нажать на кнопку Open. Откроется окно консоли. Оно будет полностью черным и не будет реагировать на нажатие клавиш клавиатуры. После включения настраиваемого оборудования на экране консоли начнет появляться информация об устройстве, его характеристиках и ходе запуска. Примерный вид консоли в момент запуска устройства приведен на рисунке 3.

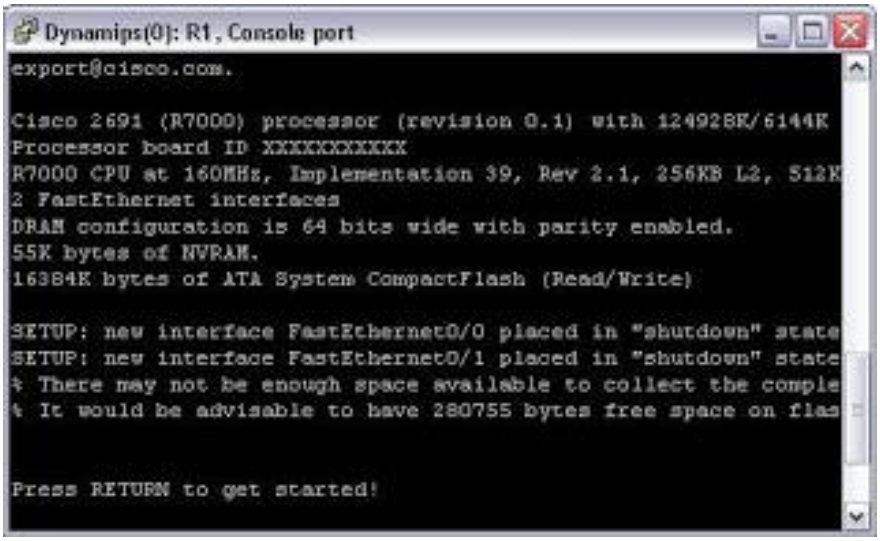

Рисунок 3 – Вид консоли при запуске устройства

Необходимо дождаться, пока завершится процесс запуска оборудования. На экране отобразится надпись Press RETURN to getstarted!, необходимо нажать на клавиатуре клавишу Enter. Указатель ввода перейдет на новую строчку, а в консоли отобразится надпись Router> (данный пример приведен для настройки маршрутизатора, при настройку другого типа устройств надпись Router будет заменена в соответствии с типом настраиваемого устройства).

При настройке оборудования Cisco, необходимо знать, что существует 3 типа доступа к устройству.

Первый режим – непривилегированный (EXEC). В данном режиме нельзя изменять конфигурацию устройства, но можно просмотреть некоторые его характеристики. Присутствие в данном режиме в консоли обозначается значком «>».

Второй режим – привилегированный режим (privilage EXEC). В данном режиме пользователь может просматривать информацию об устройстве, его конфигурацию, сохранять текущую конфигурацию, но не может ее изменять. В данный режим можно перейти из непривилегированного режима путем выполнения команды enable.Присутствие в данном режиме в консоли обозначается значком «#». Например, в данном режиме можно выполнить команду showrunning-config, выводящую текущую рабочую конфигурацию устройства.

Третий режим – режим конфигурации. В данном режиме нельзя просмотреть информацию об устройстве и его конфигурации, но зато можно ее изменять. Для перехода в режим конфигурации необходимо в привилегированном режиме выполнить команду configterminal.Присутствие в данном режиме в консоли обозначается значком «(config)#».

Cisco Packet Tracer (далее просто Packet Tracer) является довольно легким и удобным в использовании симулятором устройств Cisco, идеально подходящим для обучения работе с реальным оборудованием. Конечно, он не позволяет воспроизвести абсолютно все функции реальных сетевых устройств, но способен дать более чем общее представление о принципах их работы, и способах их конфигурации.

Интерфейс программы представлен на рисунке 4.

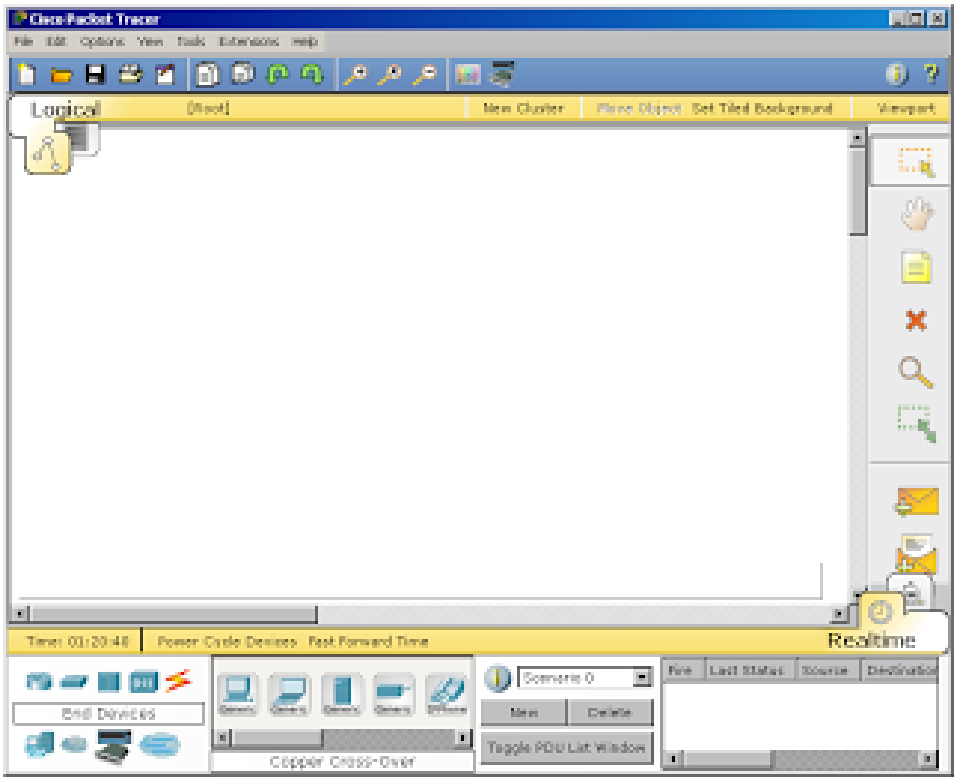

Рисунок 4 – Интерфейс программы Cisco Packet Tracer

Большую часть данного окна занимает рабочая область, в которой можно размещать различные сетевые устройства, соединять их различными способами и как следствие получать самые разные сетевые топологии.

Над рабочей областью расположена главная панель программы и ее меню (рисунок 5). Меню позволяет выполнять сохранение, загрузку сетевых топологий, настройку симуляции, а также много других функций. Главная панель содержит на себе наиболее часто используемые функции меню.

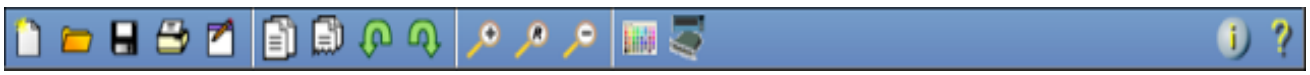

Рисунок 5 – Меню программы

Справа от рабочей области, расположена боковая панель, содержащая ряд кнопок отвечающих за перемещение полотна рабочей области, удаление объектов и т.д.

Снизу, под рабочей областью, расположена панель оборудования (рисунок 6).

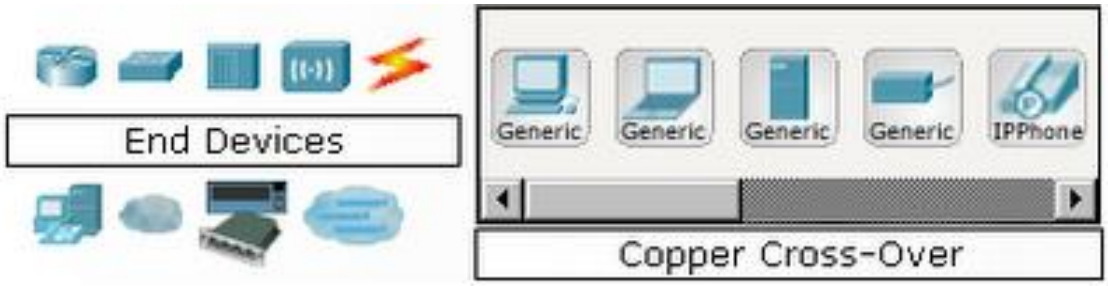

Рисунок 6 – Панель оборудования

Данная панель содержит в своей левой части типы доступных устройств, а в правой части доступные модели. При выполнении проекта эту панель придется использовать намного чаще, чем все остальные. Поэтому рассмотрим ее более подробно.

При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы устройств, наиболее часто используемые в Packet Tracer, представлены на рисунке 7.

Рисунок 7 – Типы устройств

Отдельного рассмотрения заслуживают типы соединений. Перечислим наиболее часто используемые из них (рассмотрение типов подключений идет слева направо, в соответствии с рисунком 8).

Рисунок 9 – Типы соединений

- автоматический тип – при данном типе соединения PacketTracer автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств;

- консоль – консольные соединение;

- медь Прямое – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке. Подойдет для следующих соединений: коммутатор – коммутатор, коммутатор – маршрутизатор, коммутатор – компьютер и др.;

- медь кроссовер – соединение медным кабелем типа витая пара, концы кабеля обжаты как кроссовер. Подойдет для соединения двух компьютеров;

- оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств имеющих оптические интерфейсы;

- телефонный кабель – обыкновенный телефонный кабель, может понадобиться для подключения телефонных аппаратов;

- коаксиальный кабель – соединение устройств с помощью коаксиального кабеля.

В настоящем проекте необходимо в используемых коммутаторах использовать технологию VLAN – виртуальных локальных сетей. VLAN - это технология, позволяющая организовывать несколько независимых виртуальных сетей внутри одной физической сети. С помощью VLAN можно выполнять гибкое разнесение пользователей по различным сегментам сети с разной адресацией, даже если они подключены к единому устройству, а также дробить широковещательные домены.

Принцип организации двух VLAN на одном коммутаторе иллюстрируется рисунком 10.

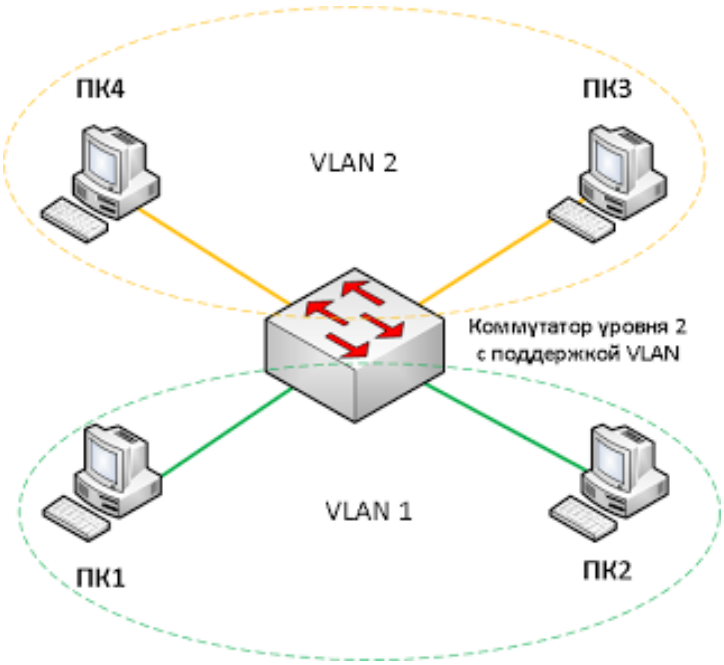

Рисунок 10 – Организация двух VLAN на одном коммутаторе

Компьютеры 1 и 2 объединены в один VLAN, компьютеры 3 и 4 объединены в другой VLAN. Хотя все компьютеры подключены к одному и тому же коммутатору, все они не будут общаться между собой. Компьютер номер 1 сможет общаться только с компьютером 2, компьютер 3 будет видеть только компьютер 4. То есть данная ситуация будет аналогична тому, как если бы мы подключили компьютеры 1 и 2 к одному коммутатору, а компьютеры 3 и 4 к другому коммутатору, и не соединили бы эти коммутаторы между собой. Как легко заметить, в данном случае, технология VLAN помогла нам разделить единую физическую сеть на несколько виртуальных не связанных между собой сетей, при этом компьютеры, находящиеся в этих виртуальных сетях, работают точно так же, как это было бы в обычной сети.

Для взаимодействия устройств в VLAN сетях их порты настраиваются специальным образом. Существует два типа настройки портов: настройка порта в режиме доступа (Access Mode) и настройка порта в режиме магистрали (Trunk Mode).

Порты доступа применяются обычно для подключения оконечных устройств. В простейшем случае, порту доступа задается определенный VLAN, и он

передает весь поступающий на него трафик именно в него. Порты, к которым подключены компьютеры 1,2,3 и 4 на рисунке 10 являются портами доступа.

Магистральные порты предназначены для передачи трафика сразу нескольких VLAN и обычно используются для соединения сетевых устройств между собой. Данный принцип проиллюстрирован на рисунке 11.

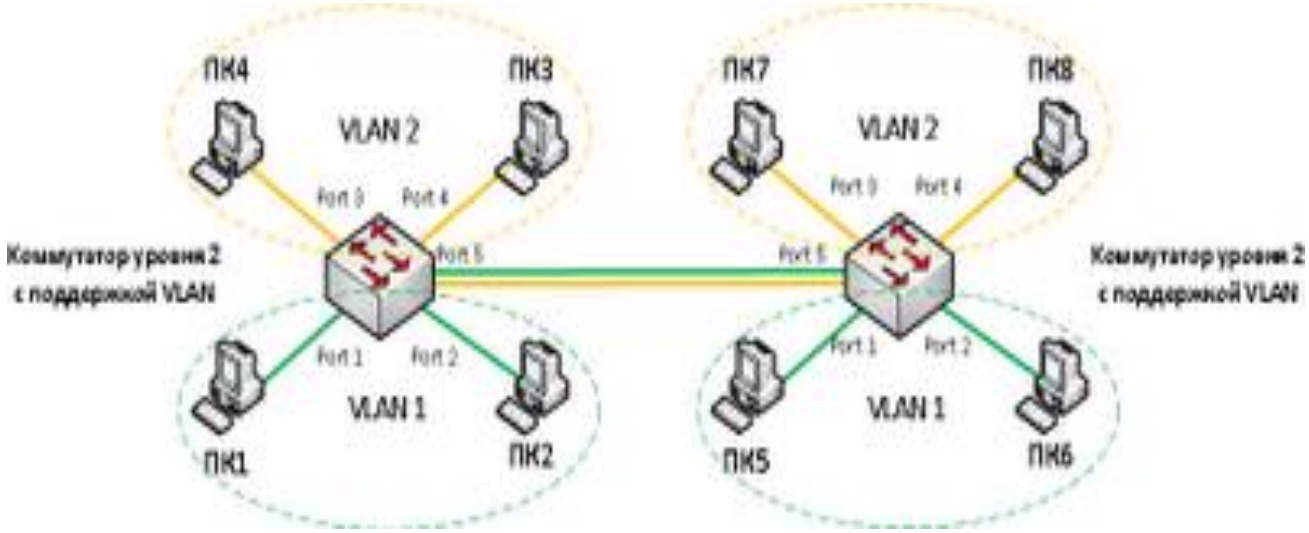

Рисунок 11 – Принцип работы портов доступа и магистральных портов

На данном рисунке порты 1-4 являются портами доступа, и по каждому из этих портов идет трафик только одного VLAN, порты 5 являются магистральными портами, служат для связи коммутаторов между собой и передают через себя трафик сразу двух виртуальных локальных сетей VLAN 1 и VLAN 2.

Передавать трафик VLAN между устройствами можно не только с помощью магистральных портов, но и с помощью портов доступа, но так как порты доступа могут пропускать трафик только одного VLAN, для соединения устройств между собой потребуется выделение портов, количество которых будет равно количеству передаваемых между устройствами VLAN. Данный способ обычно находит применение только в том случае, если между устройствами необходимо передать небольшое число VLAN.

В настоящем курсовом проекте рекомендуется для объединения VLAN использовать магистральные порты, однако это остается на усмотрение студента.

Для настройки VLAN необходимо перейти в привилегированный режим, выполнив команду enable. Информацию о существующих на коммутаторе VLAN можно, выполнив команду ***show vlan brief*** (можно просто ***sh vl br***).

В результате выполнения команды на экране появятся: номера VLAN – первый столбец, название vlan - второй столбец, состояние VLAN (работает он в данный момент или нет) – третий столбец, порты, принадлежащие к данному VLAN – четвертый столбец. Все порты коммутатора по умолчанию принадлежат VLAN 1 [2]. Остальные четыре VLAN являются служебными и используются не очень часто.

При настройке VLAN используются следующие команды:

Switch(config)#vlan 2 – создание VLAN 2;

Switch(config-vlan)#name subnet_192 – присвоение имени VLAN;

Switch(config)#interface range fastEthernet 0/1-2 – вход в режим конфигурирования интерфейсов в заданном диапазоне;

Switch(config-if-range)#switchport mode access - назначение режима работы порта (в данном случае режим доступа);

Switch(config-if-range)#switchport access vlan 2 – присвоение заданного диапазона интерфейсов какой-либо VLAN (в данном случае VLAN 2).

Для передачи трафика сразу нескольких VLAN по одной линии между коммутаторами используются магистральные порты (trunk). Для того, чтобы настроить данные порты на коммутаторах, необходимо выполнить следующие команды в режиме конфигурирования (в роли trunk портов для примера будут выступать интерфейс FastEthernet0/3):

Switch(config)#interface FastEthernet0/3 – вход в режим конфигурирования интерфейса;

Switch(config-if)# switchport mode trunk – назначение режима работы порта (в данном случае магистральный режим).

Для того, чтобы магистральный порт пропускал трафик нужной VLAN, его необходимо правильно сконфигурировать. Для этого используется команда

Switch(config-if)#switchport trunk allowed vlan 2-3

Для того, чтобы обеспечить информационное взаимодействие между различными VLAN, необходимо использовать устройства, способные работать на третьем уровне модели ISO/OSI, то есть маршрутизаторы или коммутаторы третьего уровня. Порты этих устройств должны быть сконфигурированы. В простейшем случае может использоваться статическая маршрутизация, то есть в этом случае надо просто портам задать IP-адреса из диапазона той подсети, к которой они подключены. Конфигурирование маршрутизаторов также производится в привилегированном режиме. Например, если интерфейсу FastEthernet 0/0 необходимо присвоить IP адрес 192.168.1.1 с маской 24, а интерфейсу FastEthernet 0/1 IP адрес 10.10.10.1 с маской 8, на маршрутизаторе в режиме конфигурирования нужно выполнить следующие команды:

Router> enable

Router#config terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 10.10.10.1 255.0.0.0

Router(config-if)#no shutdown

Первый способ объединения VLAN называется «маршрутизатор на привязи». Такой способ иллюстрируется рисунком 12.

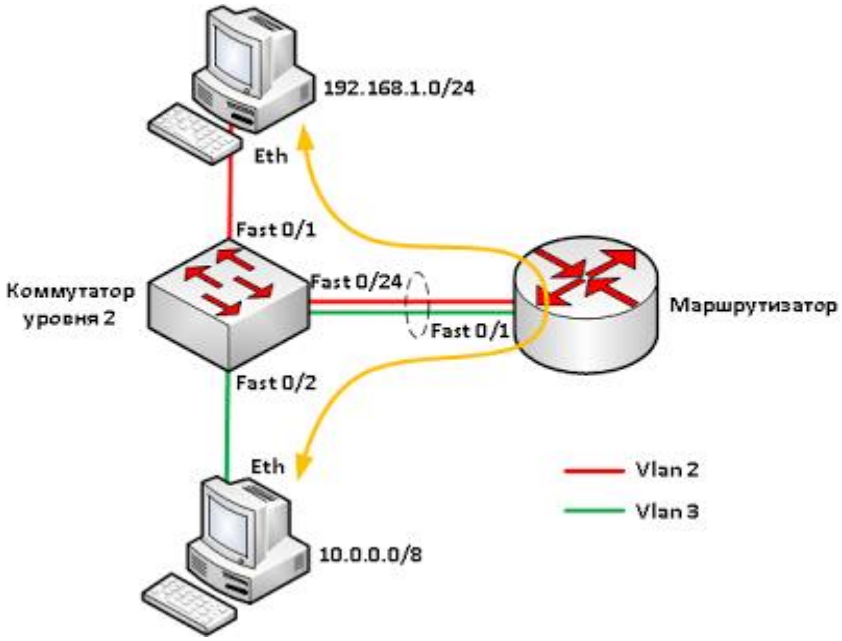

Рисунок 12 – Способ «маршрутизатор на привязи»

Также, необходимо изменить имя маршрутизатора, что можно сделать по команде:

Router(config)#hostname R1

Где R1 – новое имя маршрутизатора.

После установки имени необходимо установить пароль для входа в привилегированный режим. Это делается командой

Router1(config)#enable password parol

Вместо слова «parol» может быть написано любое слово, цифра или набор букв и цифр, которые будут являться парольной фразой.

После установки пароля, любая следующая попытка зайти в привилегированный режим будет начинаться с запроса пароля.

Для тог, чтобы сохранить текущую конфигурацию сети необходимо ввести команду

Router# write memory

или

Router# copy run start

Для тог, чтобы просмотреть сохранённую конфигурацию необходимо воспользоваться командой

Router# Show configuration

или

Router1#show running-config

Для объединения VLAN между собой в данном примере на коммутаторе необходимо выполнить следующие команды.

Switch(config)#vlan 2

Switch(config-vlan)#name vlan_number_2

Switch(config-vlan)#exit

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit

Switch(config)#vlan 3

Switch(config-vlan)#name vlan_number_3

Switch(config-vlan)#exit

Switch(config)#interface fastEthernet 0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 3

Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/24

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 2-3

На маршрутизаторе для начала необходимо включить интерфейс, к которому подключен коммутатор:

Router(config)#interface fastEthernet 0/1

Router(config-if)#no shutdown

Для того, чтобы все же настроить маршрутизацию между данными VLAN, создадим на интерфейсе маршрутизатора субинтерфейсы предназначенные для наших VLAN (по одному субинтерфейсу под каждый VLAN) и присвоим им IP-адреса, которые мы указали на компьютерах в качестве основных шлюзов:

Router(config)#interface fastEthernet 0/1.2

Router(config-subif)#encapsulation dot1Q 2

Router(config-subif)#ip address 192.168.1.1 255.255.255.0

Router(config)#interface fastEthernet 0/1.3

Router(config-subif)#encapsulation dot1Q 3

Router(config-subif)#ip address 10.10.10.1 255.0.0.0

Router(config-subif)#exit

Примечание: номера VLAN на коммутаторе должны соответствовать номерам субинтерфейсов на маршрутизаторе. Например, для VLAN 2 необходимо использовать субинтерфейс fa 0/0.2. Соответственно, команда encapsulation dot1Q тоже должна содержать номер VLAN 2.

Вторым способом является использование коммутатора уровня 3. Этот способ иллюстрирует рисунок 13.

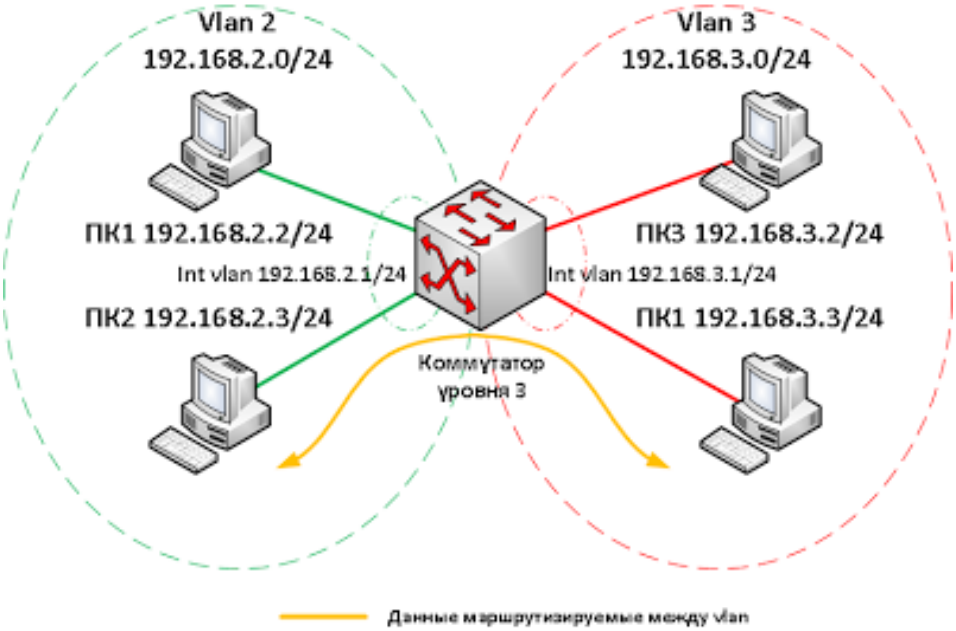

Рисунок 13 – Способ использования коммутатора уровня 3

Сначала необходимо настроить в коммутаторе VLAN таким же образом, как и в предыдущем примере.

Для того, чтобы настроить маршрутизацию между ними, необходимо выполнить следующие команды:

Switch(config)#interface vlan 2

Switch(config-if)#ip address 192.168.2.1 255.255.255.0

Switch(config)#interface vlan 3

Switch(config-if)#ip address 192.168.3.1 255.255.255.0

Switch(config)#ip routing

По сути, эти команды отдают IP-адреса соответствующим VLAN, а последняя команда включает маршрутизацию между ними.

Рассмотрим теперь настройку служб DHCP и DNS.

Название протокола DHCP (Dynamic Host Configuration Protocol) дословно расшифровывается как «Протокол динамической конфигурации хоста». Данный протокол работает на прикладном уровне модели OSI и позволяет компьютерам сети получать ряд настроек (в том числе IP-адрес) от расположенного в сети DHCP сервера. Все устройства в сети при работе с протоколом DHCP можно разделить на два вида: DHCP-серверы и DHCP-клиенты. DHCP-клиенты пытаются получить настройки, а DHCP-серверы выдают их.

Рассмотрим как работает данный протокол на примере топологии сети, показанной на рисунке 14.

Все компьютеры и DHCP-сервер связываются друг с другом через коммутатор. Зная, что в сети существует DHCP-сервер, в настройках компьютеров указывают получать IP-адрес автоматически. После этого каждый компьютер попытается получить IP-адрес от DHCP-сервера. Для этого он выполняет широковещательный запрос на IP-адрес 255.255.255.255, а в качестве своего IP-адреса указывает 0.0.0.0 (так как у него еще нет IP-адреса).

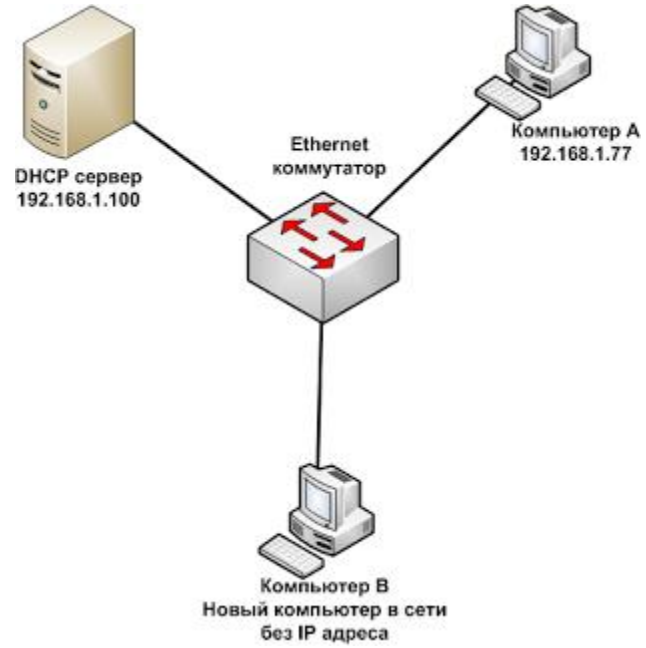

Рисунок 14 – Фрагмент сети

В ходе данного широковещательного запроса рассылается сообщение DHCP DISCOVER, данное сообщение содержит в себе информацию, позволяющую отличить его от других типов запросов/сообщений (то есть указывает на то, что это сообщение предназначено для DHCP-сервера, для получения IP-адреса), MAC-адрес устройства сформировавшего запрос, а также предыдущий IP адрес устройства (если он у него был) (рисунок 15).

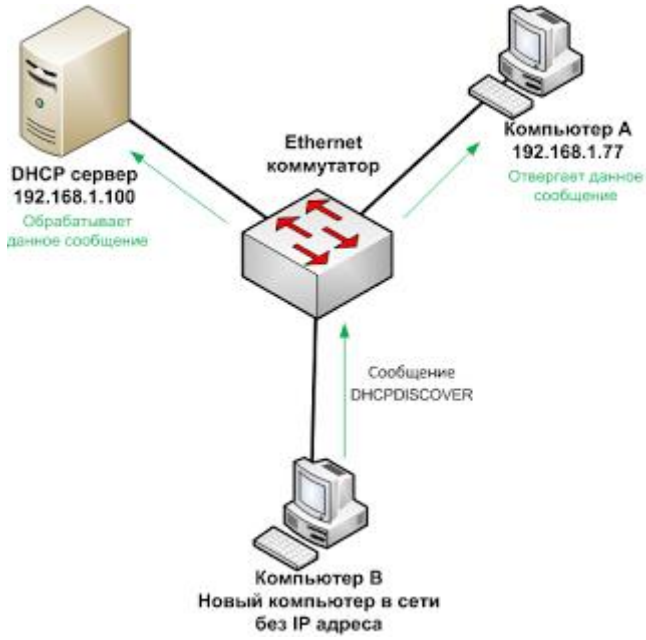

Рисунок 15 – Процесс рассылки сообщения DHCP DISCOVER

Так как сообщение DHCP DISCOVER рассылается широковещательным способом, оно попадает не только на DHCP-сервер, но и на другие устройства данного сегмента сети, но так как в сообщение DHCP DISCOVER указывается, что оно предназначено только для DHCP-сервера, остальные устройства сети отвергают данное сообщение [2].

При получении сообщения DHCP DISCOVER DHCP-сервером, он анализирует его содержание, и в соответствии со своими настройками выбирает подходящую конфигурацию для запросившего компьютера и отправляет ее обратно в сообщении DHCP OFFER. Обычно сообщение DHCP OFFER отсылается только на MAC-адрес компьютера, который был указан в сообщении DHCP DISCOVER, но иногда оно может рассылаться и методом широковещательной рассылки.

В случае если в сети существует несколько DHCP-серверов, компьютер может получить в ответ на сообщение DHCP DISCOVER несколько сообщений DHCP OFFER от разных DHCP-серверов. Из них компьютер выбирает одно, обычно полученное первым. И отвечает на него сообщением DHCP REQUEST, которое содержит в себе всю туже информацию, что и сообщение DHCPDISCOVER + IP адрес выбранного DHCP-сервера. Сообщение DHCP REQUEST рассылается широковещательным методом для того, чтобы его могли получить все DHCP сервера сети, если их несколько.

Все устройства сети, не являющиеся DHCP-серверами игнорируют сообщение DHCP REQUEST. DHCP-сервера, IP-адрес которых не содержится в сообщении DHCP REQUEST понимают, что их не выбрали в качестве DHCP-сервера. DHCP-сервер, IP-адрес которого указан в сообщении DHCP REQUEST, получает его и определяет, что именного его выбрали в качестве DHCP-сервера для нового компьютера, на что он отвечает сообщением DHCP ACK, которое подтверждает данный выбор. Сообщение DHCP ACK отправляется на MAC-адрес компьютера, указанного в сообщении DHCP REQUEST [2].

Компьютер, запрашивающий конфигурацию, получает сообщения DHCP ACK и применяет конфигурацию, которая была получена в сообщении DHCP OFFER.

DHCP-сервер может быть настроен по разному, и в зависимости от его конфигурации он будет выдавать IP-адреса запрашивающим компьютерам разными способами. Например, можно настроить DHCP-сервер так, чтобы он выдавал запросившим компьютерам любые свободные IP-адреса из некоторого диапазона, а можно настроить так, чтобы он выдавал определенные IP-адреса устройствам с заданными MAC-адресами.

В роли DHCP-сервера может выступать сервер под управлением серверной операционной системы семейства Linux или Windows, некоторые модели коммутаторов и даже обычные компьютеры с клиентскими операционными системами в случае, если на них установлено специализированное программное обеспечение. Обычно под DHCP-сервер не отводят отдельного физического сервера или отдельной виртуальной машины, а устанавливают их на одном из уже существующих не сильно загруженных серверов, выполняющих другую роль.

В настоящем проекте рекомендуется выделить в проектируемой сети сервер и настроить на нем службы DNS и DHCP. В настройках DHCP-сервера необходимо указать диапазон выдаваемых адресов, а в настройках DNS-сервера – адрес внешнего www-сервера и его IP-адрес. После этого необходимо установить внешний www-сервер, назначить ему IP-адрес. Соответственно, при наборе в адресной строке браузера на любом компьютере сети должна отображаться Интернет-страница.

Рассмотрим настройку маршрутизаторов сити.

Для создания сети используйте типы и названия устройств, указанные в таблице 5.

Таблица 5 – Используемые устройства

Группа устройств	Название устройства	Дополнительные модули
Маршрутизатор	2811	NM-2FE2W
Коммутаторы	2960-24TT	-
Конечные устройства	PC-PT (компьютер)	-

Название коммутационных устройств произвести по своему усмотрению, можно использовать сокращения.

Поскольку по умолчанию маршрутизатор 2811 имеет всего два порта Fast Ethernet, необходимо произвести установку дополнительных модулей. Это можно произвести следующим образом:

- установите маршрутизатор на рабочее поле и однократным нажатием правой кнопки мыши вызовите форму управления маршрутизатором;

- на вкладке Physical выключите маршрутизатор, область расположения кнопки выделена прямоугольником и помечена номером 1 (рисунок 16);

- выберите необходимый модуль (NM-2FE2W), расположенный на месте 2, нажав на него правой кнопкой мыши, и перетащите его на место его установки - место 3 (рисунок 16).

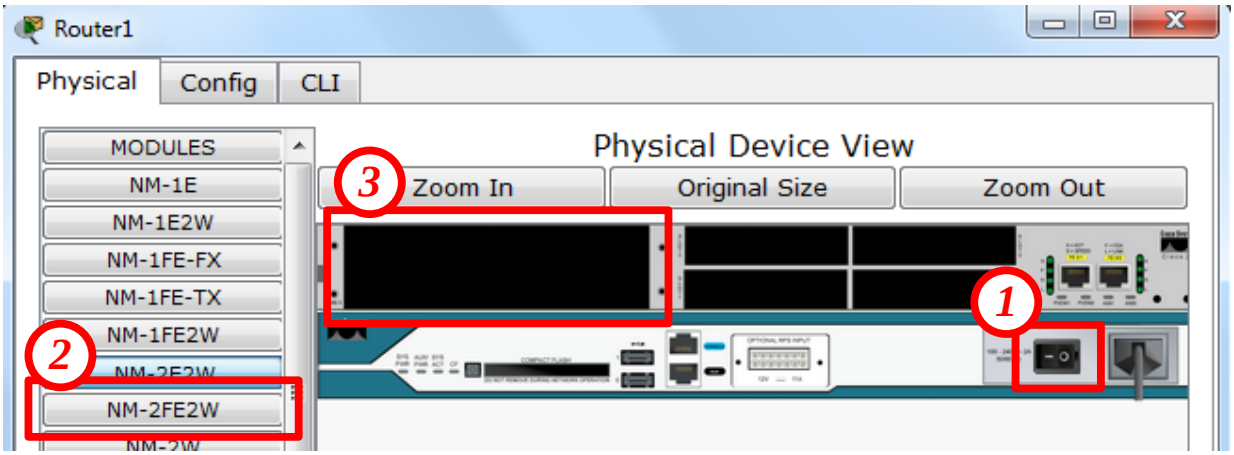

Рисунок 16 – фрагмент формы управления маршрутизатором

Определение подсетей.

На основе исходных данных, определите IP -адреса и маски для всех устройств. Для всех подсетей определите диапазон адресов, доступных для использования, и широковещательный адрес. Портам маршрутизатора присвоите первые адреса, а портам сетевых карт компьютеров – последние адреса подсетей. Результаты расчетов занесите в таблицу 6.

Таблица 6 – Распределение адресов

Название устройства	Интерфейс	Подсеть	IP	Маска	Шлюз
R1	Fa0/0	LAN1			-
R1	Fa1/0	WAN1			-
R2	Fa0/0	LAN2			-
R2	Fa1/0	WAN1			-
R2	Fa1/1	WAN2			-
R3	Fa0/0	LAN3			-
R3	Fa1/0	WAN2			-
R1	Eth0	LAN1			
PC2	Eth0	LAN2			
PC3	Eth0	LAN3			
Все устройства					

После задания портам маршрутизаторов адресации, необходимо произвести настройку статической маршрутизации. В качестве примера рассмотрим случай представленный на рисунке 17.

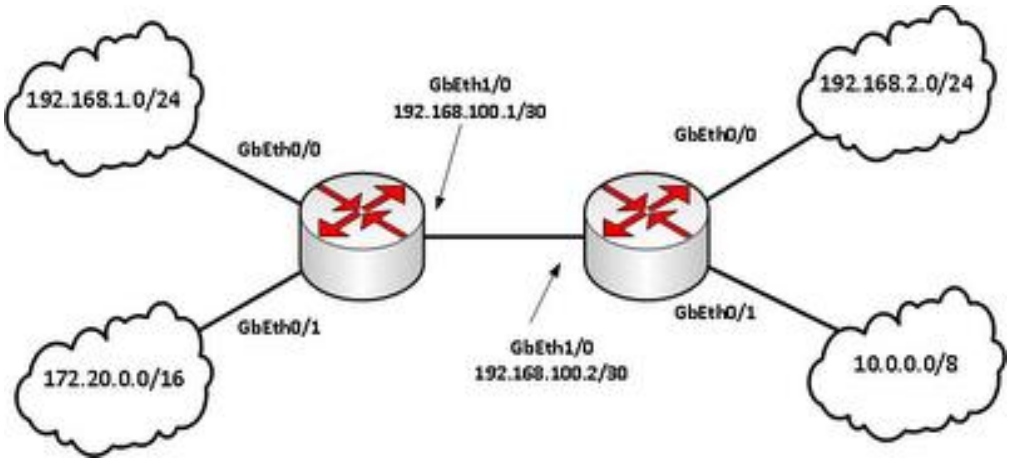

Рисунок 17 – Пример составной сети

Самым простым способом настроить маршрутизацию является добавление маршрута по умолчанию. Для того, чтобы это сделать, нужно выполнить на «левом» маршрутизаторе в режиме конфигурирования следующую команду:

ip route 0.0.0.0 0.0.0.0 192.168.100.2

На «правом» маршрутизаторе:

ip route 0.0.0.0 0.0.0.0 192.168.100.1

В следующих командах первые 4 цифры обозначают IP-адрес сети назначения, следующие 4 цифры обозначают её маску, а последние 4 цифры – это IP-адрес интерфейса, на который необходимо передать пакеты, чтобы попасть в данную сеть. Если мы указываем в качестве адреса сети 0.0.0.0 с маской 0.0.0.0, то данный маршрут становится маршрутом по умолчанию, и все пакеты, адреса назначения которых прямо не указаны в таблице маршрутизации, будут отправлены на адрес, указанный в нем.

К сожалению, далеко не всегда можно обойтись указанием только маршрутов по умолчанию. В более сложных сетевых конфигурациях может потребоваться прописывать маршрут для каждой из сетей в отдельности. Давайте сразу рассмотрим, как это делается. Для этого сначала удалим из таблицы маршрутизации все статически добавленные маршруты, используя команду

no ip route xxxx(адрес сети) yyyy(маска) zzzz(адрес интерфейса)

В конечном итоге таблицы маршрутизации должны содержать только информацию о непосредственно подключенных к ним сетях.

Теперь нам необходимо добавить к каждому из маршрутизаторов маршруты к двум сетям, которые ему неизвестны (к сетям, подключенным к соседнему маршрутизатору).

На «левом» маршрутизаторе выполним:

ip route 192.168.2.0 255.255.255.0 192.168.100.2

ip route 10.0.0.0 255.0.0.0 192.168.100.2

На правом маршрутизаторе выполним:

ip route 192.168.1.0 255.255.255.0 192.168.100.1

ip route 172.20.0.0 255.255.0.0 192.168.100.1

Если все сделано верно, то сети должны будут видеть друг друга.

Для настройки динамической маршрутизации рассмотрим следующий пример.

Создайте схему, представленную на рисунке 18.

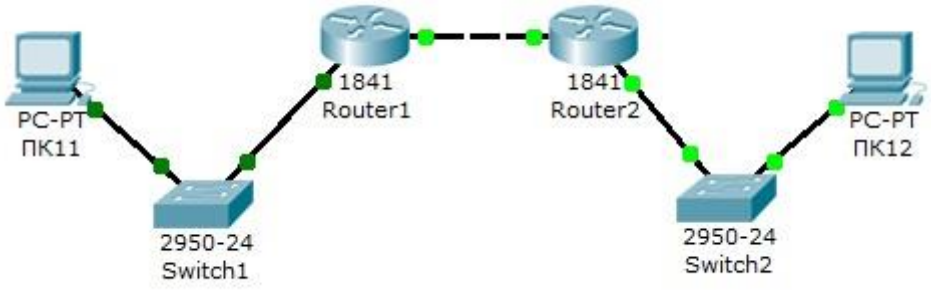

Рисунок 18 - Схема сети

На схеме представлены следующие три сети:

Switch1 – сеть 10.11.0.0/16;

Switch2 – сеть 10.12.0.0/16;

Сеть для роутеров - 10.10.0.0/16.

Введите на устройствах следующую адресацию:

Маршрутизаторы имеют по два интерфейса:

Router1 – 10.11.0.1/16 и 10.10.0.1/16;

Router2 – 10.10.0.2/16 и 10.12.0.1/16.

Компьютеры:

ПК11 - 10.11.0.11/16;

ПК12 - 10.12.0.12/16.

Настройка RIP

Проведем настройку протокола RIP на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

Router1>en

Войдите в режим конфигурации:

Router1>#conf t

Войдите в режим конфигурирования протокола RIP:

Router1(config)#router rip

Подключите клиентскую сеть к роутеру:

Router1(config-router)#network 10.11.0.0

Подключите вторую сеть к роутеру:

Router1(config-router)#network 10.10.0.0

Задайте использование второй версии протокол RIP:

Router1(config-router)#version 2

Выйдите из режима конфигурирования протокола RIP:

Router1(config-router)#exit

Выйдите из консоли настроек:

Router1(config)#exit

Сохраните настройки в память маршрутизатора:

Router1>#write memory

Аналогично проведите настройку протокола RIP на маршрутизаторе Router2.

Проверьте связь между компьютерами ПК11 и ПК12 командой ping.

Если связь есть – все настройки выполнены правильно.

Настройка OSPF.

Возьмите схему сети, представленную на рисунке 18.

Проведем настройку протокола OSPF на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

Switch>en

Войдите в режим конфигурации:

Switch1#conf t

Войдите в режим конфигурирования протокола OSPF:

Router1(config)#router ospf 1

В команде ***router ospf <идентификатор_процесса>*** под идентификатором процесса понимается уникальное числовое значение для каждого процесса роутинга на маршрутизаторе. Данное значение должно быть больше в интервале от 1 до 65535. В OSPF процессам на роутерах одной зоны принято присваивать один и тот же идентификатор.

Подключите клиентскую сеть к роутеру:

Router1(config-router)#network 10.11.0.0

Подключите вторую сеть к роутеру:

Router1(config-router)#network 10.10.0.0

Задайте использование второй версии протокол OSPF:

Router1(config-router)#version 2

Выйдите из режима конфигурирования протокола OSPF:

Router1(config-router)#exit

Выйдите из консоли настроек:

Router1(config)#exit

Сохраните настройки в память маршрутизатора:

Switch1#write memory

Аналогично проведите настройку протокола OSPF на маршрутизаторе Router2 и проверите наличие связи между компьютерами при помощи команды ***ping.***

Библиографический список

1. Жуковский А.Г., и др. Руководство по дипломному проектированию и оформлению результатов курсовых и дипломных проектов. Учебно-методическое пособие. – Ростов-на-Дону: ПЦ СКФ МТУСИ, 2011.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. – СПб: Питер, 2009. – 884 с.

3. Кулябов Д.С., Королькова А.В. Архитектуры и принципы построения современных сетей и систем телекоммуникаций. Учебное пособие. М.: РУДН, 2008. – 281 с.

4. Кольтюков Н.А., Белоусов О.А. Сетевые технологии. – Тамбов: Изд-во Тамб. гос. ун-та, 2009. – 100 с.