

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Оренбургский государственный университет»

# **КОМПЬЮТЕРНЫЕ СЕТИ**

Практикум

Рекомендован ученым советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательным программам высшего образования по направлениям подготовки, входящим в образовательные области «Инженерное дело, технологии и технические науки», «Математические и естественные науки»

Оренбург  
2020

УДК 004.42(075.8)

ББК 39.973я73

У93

Рецензент – доцент, кандидат педагогических наук А. Е. Шухман

Авторы: Ю.А. Ушаков, М.В. Ушакова, А.Л. Коннов, Д.А. Муслимов

У93 Компьютерные сети [Электронный ресурс] : практикум для обучающихся по образовательным программам высшего образования по направлениям подготовки, входящим в образовательные области "Инженерное дело, технологии и технические науки", "Математические и естественные науки" / Ю.А. Ушаков [и др.]; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2020. - 130 с-  
Загл. с тит. экрана.  
ISBN 978-5-7410-2499-7

В издании рассмотрены принципы построения и функционирования компьютерных сетей, а также представлены алгоритмы работы сетевых протоколов и устройств.

Практикум предназначен для обучающихся по программам высшего образования по направлениям подготовки, входящим в образовательные области «Инженерное дело, технологии и технические науки», «Математические и естественные науки».

УДК 004.42(075.8)

ББК 39.973я73

ISBN 978-5-7410-2499-7

© Ушаков Ю.А.,  
Ушакова М.В.,  
Коннов А.Л.,  
Муслимов Д.А., 2020  
© ОГУ, 2020

## Содержание

Введение .....	5
1 Лабораторная работа №1. Проектирование схемы IP адресации корпоративной сети.....	10
1.1 Общие сведения.....	10
1.2 Рабочее задание .....	14
1.3 Контрольные вопросы .....	15
2 Лабораторная работа №2. Изучение системы моделирования Cisco Packet Tracer	16
2.1 Общие сведения.....	16
2.2 Рабочее задание .....	26
2.3 Контрольные вопросы .....	28
3 Лабораторная работа №3. Создание логической схемы сети в Cisco Packet Tracer	28
3.1 Общие сведения.....	29
3.2 Рабочее задание .....	36
3.3 Контрольные вопросы .....	37
4 Лабораторная работа №4. Протокол OSPF.....	37
4.1 Основные теоретические положения .....	37
4.2 Рабочее задание .....	49
4.3 Контрольные вопросы .....	52
5 Лабораторная работа №5. Протокол BGP.....	54
5.1 Основные теоретические положения .....	54
5.2 Рабочее задание .....	58
5.3 Контрольные вопросы .....	61
6 Лабораторная работа №6. Настройка интерфейсов IPv4 и IPv6 .....	61
6.1 Основные теоретические положения .....	61
6.2 Рабочее задание .....	66
7 Лабораторная работа №7. Проектирование беспроводной сети, выбор оптимальных мест для базовых станций, настройка оборудования. ....	70
7.1 Основные теоретические положения .....	70
7.2 Выбор расположения оборудования .....	73
7.3 Настройка оборудования .....	75
7.4 Рабочее задание .....	81
8 Лабораторная работа №8. Проектирование физической схемы сети, расчет комплектующих и расходных материалов .....	83
8.1 Общие сведения.....	83
8.2 Рабочее задание .....	86
8.3 Контрольные вопросы .....	88
9 Лабораторная работа №9. Настройка VLAN.....	88
9.1 Общие сведения.....	88
9.1.1 Настройка VLAN на коммутаторах.....	90
9.1.2 Настройка маршрутизации между VLAN .....	93
9.1.3 Пример базовой настройки VLAN, без настройки маршрутизации .....	96
9.1.4 Пример конфигураций с настройкой маршрутизации между VLAN .....	98

9.1.5 Настройка VLAN на маршрутизаторах Cisco .....	100
9.2 Рабочее задание .....	101
10 Лабораторная работа №10. Общие сведения об VoIP .....	104
10.1 Краткие теоретические положения .....	104
10.2 Рабочее задание .....	109
11 Лабораторная работа №11. Добавление устройств IoT в умную домашнюю сеть .....	121
11.1 Краткие теоретические положения .....	121
11.2 Рабочее задание .....	122
11.2.1 Изучение возможностей Packet Tracer для построения схемы интеллектуальной домашней сети .....	122
11.2.4 Согласование работы датчика движения и веб-камеры.....	124
Список использованных источников .....	130

## Введение

В настоящее время вычислительная сеть является неотъемлемой частью любой организации, а её отсутствие рассматривается как анахронизм, существенно снижающий эффективность работы персонала. Особенно важно наличие вычислительной сети в учебном заведении, так как без использования информационных и компьютерных технологий давно стало невозможно обеспечивать учебный процесс и проводить научную работу [1].

Главным требованием, предъявляемым к сетям, является выполнение их основной функции: обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам сети. Все остальные требования связаны с качеством выполнения основной задачи. Для разных логических типов сетей приоритетными параметрами могут быть производительность, надежность, совместимость, управляемость, защищенность, расширяемость, масштабируемость и их совокупность.

На сегодняшний день практически все средние и крупные потребители услуг сетей передачи данных (СПД) не ограничиваются только локальными сетями и услугами. Все больше растет потребность в корпоративных, распределенных сетях передачи данных.

Корпоративные сети передачи данных (КСПД) представляют собой территориально распределенные, соединенные между собой сегменты единой сети, использующие выделенные централизованные ресурсы и сервисы. Цель построения корпоративных сетей передачи данных – обеспечение транспорта для территориально распределенных бизнес-приложений. К таким приложениям обычно относят сетевые базы данных, информационные порталы, электронную почту, традиционный файловый обмен, IP телефонию, видеоконференцсвязь и дистанционное обучение. КСПД – один из важнейших инструментов развития бизнеса. Качественную и надежную корпоративную сеть имеют, в первую очередь, географически распределенные компании, бизнес которых зависит от надежности и гибкости совместной работы ее подразделений [2].

Построение КСПД в общем – это организация связности по протоколу IP между рабочими станциями и серверами предприятия. Сеть образуется совокупностью узлов связи, располагаемых на территории офисов или других точек присутствия предприятия. В основе построения корпоративных сетей передачи данных положена методология проектирования компании Cisco Systems на основе композитной сетевой модели предприятия. Данное решение – это модульный подход к построению структуры сети. Методология решения позволяет строить как небольшие сети, объединяющие несколько офисов, так и крупные, включающие сотни узлов.

Развивая сеть путем добавления новых модулей или узлов, подход обеспечивает предсказуемость качественных характеристик сети и требует минимальных усилий и средств для поиска и устранения неисправностей [3].

В основе композитной модели лежит принцип разделения сети на модули (декомпозиции). Каждый характеризуется свойственными только ему функциями и особенностями реализации. Ключевым компонентом, связующим узлы КСПД, является услуга связи, которая обеспечивает передачу трафика между узлами. Виды услуг связи, используемые при организации каналов между узлами, делятся на следующие группы:

1) выделенные линии связи – оптические или медные кабели, соединяющие узлы сети заказчика (это могут быть как свои, так и арендуемые линии связи);

2) выделенные каналы данных – каналы данных предоставляемые оператором связи поверх своей сети передачи данных: Frame Relay (PVC), ATM (PVC), E1/E3/STM-1, Ethernet VLAN;

3) услуги по соединению на базе «группового» доступа: IP VPN, VPLS – Virtual Private LAN Service, сеть «Интернет».

Принципиальная разница между этими типами услуг заключается в различном механизме передачи трафика между сетевыми узлами клиента. В первом случае используются выделенные каналы связи, то есть трафик проходит строго по определенным направлениям. В случае группового доступа трафик может проходить произвольно между любыми офисами. Второй способ обеспечивает

лучшие скоростные характеристики передачи трафика и оптимальное «дешевое» использование полосы пропускания.

Узлы сетей передачи данных можно классифицировать в три группы: центральный узел, отделение/крупный узел, конечный узел [4].

Центральные узлы – это наиболее крупные узлы сети. На данных узлах осуществляется консолидация информационных ресурсов, размещается основная масса серверов приложений, развертываются выделенные подсистемы безопасности и осуществляется стыковка с внешними сетями.

Отделение/крупные узлы – "основная масса" сети. Здесь размещаются информационные ресурсы, имеющие только локальное значение и предоставляющие сервисы только локально – абонентам данного узла.

Конечный узел – данный тип узла является самым маломощным. В его составе нет никаких информационных ресурсов и серверов приложений. Данные узлы предназначены только для подключения пользователей.

Для образования подсистемы КСПД всех типов узлов обычно предлагается использовать интеллектуальное оборудование – маршрутизаторы с интеграцией сервисов, которые обеспечивают решение следующих задач:

1) традиционных для маршрутизатора – передача IP трафика и обеспечение связности по протоколу IP;

2) обеспечения безопасности:

- межсетевое экранирование и обнаружение атак – защита от возможных сетевых атак злоумышленника, нацеленных на перебой штатного функционирования сети;

- шифрование данных – обеспечение конфиденциальности передаваемой по сети информации;

- контроль целостности данных – обеспечение невозможности манипуляции данными при передаче через сеть;

3) бесперебойного функционирования приложений IP телефонии:

- маршрутизация вызовов;

- голосовая почта;

- стыковка с традиционной телефонией.

Классификация типов узлов, конечно, весьма условная, но она помогает добиться большей легкости при первичной декомпозиции проекта.

Сеть конечного узла строится на базе одного устройства, возможно совмещение маршрутизатора и коммутатора в одном устройстве, также возможно построение только на базе беспроводной связи. Сеть отделений в большинстве случаев может быть построена на базе «плоской» архитектуры, при построении обычно используют наиболее «слабые» или «средние» коммутаторы с функциями мониторинга [5].

Сеть центральных узлов строится по всем правилам построения крупных сетей, с декомпозицией сети по функциям.

К центральным узлам применяют правила построения кампусных сетей, т.е. многоуровневую архитектуру, базирующуюся на следующих принципах:

- иерархичность – сеть разделяется на несколько уровней, каждый уровень выполняет определенные функции;
- модульность – уровни строятся на основе модулей, каждый модуль представляет собой функционально законченную единицу, выполняющую функции соответственно уровня.

Сеть должна быть максимально универсальной, то есть допускать интеграцию уже существующих и будущих приложений с минимально возможными затратами и ограничениями. Часто узлы корпоративной сети оказываются расположенными в различных городах, а иногда и странах [6].

Если при создании локальной сети основные затраты приходится на закупку оборудования и прокладку кабеля, то в территориально-распределенных сетях наиболее существенным элементом стоимости оказывается арендная плата за использование каналов. Это ограничение является принципиальным, и при проектировании корпоративной сети следует предпринимать все меры для минимизации объемов передаваемых данных. В остальном же корпоративная сеть не должна вносить ограничений на то, какие именно приложения и каким образом обрабатывают переносимую по ней информацию. Под приложениями мы здесь



понимаем как системное программное обеспечение (базы данных, почтовые системы, вычислительные ресурсы, файловый сервис), так и средства, с которыми работает конечный пользователь.

# **1 Лабораторная работа №1. Проектирование схемы IP адресации корпоративной сети**

*Цель работы.* Изучение процесса формирования IP-пространства крупных сетей, получение навыков вычисления подсетей.

## **1.1 Общие сведения**

Процесс построения сети обычно включает в себя следующие глобальные этапы:

1) Анализ задач, для решения которых создается сеть, а также определение объема финансирования проекта.

2) Проектирование физической структуры – этап, на котором анализируются начальные условия (планировка здания, имеющиеся технические средства и т.п.) и создается детальный проект физической организации сети.

3) Проектирование инфраструктуры – этап, на котором определяются протоколы взаимодействия, используемые службы, политика безопасности и т.п. – т.е. логическая организация сети.

4) Развертывание – этап, связанный с прокладкой линий связи, установкой и настройкой оборудования.

Этап анализа является одним из важнейших, поскольку определяет все остальные решаемые задачи: как физическую структуру сети (например, места расположения компьютеров), так и логическую – используемые протоколы, службы и т.п. На этом этапе необходимо собрать как можно больше информации, чтобы упростить выполнение следующих этапов.

На этапе планирования IP-сетей необходимо каждому узлу сети назначить IP-адрес. Далее показан один из вариантов планирования сетей.

1) Для узлов создаваемой сети резервируется диапазон уникальных для Интернета IP-адресов (общие адреса). Этот способ наиболее дорогой, поскольку требуется нужно платить за аренду каждого IP-адреса. Кроме того, при подключении сети к Интернету вряд ли удастся получить необходимое количество

IP-адресов – в настоящее время наметился их дефицит, поэтому в лучшем случае, можно получить несколько, а зачастую – всего один.

2) Для узлов создаваемой сети адреса назначаются из диапазона так называемых частных сетей. Такие адреса не используются в Интернете, поэтому нет необходимости соблюдать их уникальность. Однако чтобы узлы, обладающие такими адресами, имели доступ к ресурсам Интернета, на шлюзе, через который сеть подключена к Интернету, необходимо настроить службу трансляции адресов (Network Address Translation, NAT).

Второй подход – наиболее распространенный и простой с точки зрения администрирования. При планировании IP-адресов необходимо выполнить следующие действия:

1) Определить по числу физических подсетей количество планируемых IP-сетей. Каждая физическая подсеть должна быть представлена хотя бы одной IP-сетью.

2) Определить количество узлов в каждой IP-сети и число адресов, необходимое каждому из них.

3) Определить для каждой сети диапазоны IP-адресов и маски подсети. Если не предполагается, что IP-сетей в сети будет более чем 254, и каждая из них будут содержать более 254 узлов, проще всего закреплять адреса из частного диапазона 192.168.X.0 (где X – уникальное число для каждой IP-сети) и маску 255.255.255.0.

4) Закрепить для каждой сети IP-адреса за интерфейсами маршрутизаторов. Обычно для этого используют начальные номера диапазона адресов IP-сети (например, 192.168.X.1).

5) Закрепить за каждым узлом IP-адрес(а).

6) При использовании статической маршрутизации определить таблицы маршрутизации для каждого маршрутизатора.

7) Определить параметры для настройки службы трансляции адресов.

Так как в базовом IP-адресе фиксированные биты должны располагаться в одной непрерывной группе, начинающейся с самого старшего бита адреса, маска должна содержать непрерывную последовательность единичных битов,

соответствующую фиксированной части адреса, за которой следует непрерывная последовательность нулевых битов, обозначающая переменную часть адреса.

Базовый IP-адрес, маска и диапазон адресов связаны друг с другом математической операцией, называемой побитовым логическим «И». При побитовом логическом «И» 32 бита IP-адреса выравниваются с 32 битами маски. Для каждой пары битов выполняется логическое «И». Результат логического «И» равен единице, если оба бита-операнда равны единице; во всех остальных случаях результат операции равен нулю.

Так как переменные биты адреса в маске обозначены нулями, то побитовое логическое «И», выполненное над любым IP-адресом из диапазона (включая базовый IP-адрес) и маской, всегда дает один и тот же результат: базовый IP-адрес.

В последнее время поле номера сети в адресе принято называть сетевым префиксом, так как первая порция каждого IP-адреса идентифицирует номер сети. Все хосты в определенной сети имеют один и тот же сетевой префикс, но при этом они должны иметь уникальные номера хостов. Аналогично, два любых расположенных в разных сетях хоста должны иметь различные сетевые префиксы, но они могут иметь одинаковые номера хостов. Длиной префикса называется количество бит в маске.

Первым шагом в процессе планирования является определение максимального количества требуемых подсетей. Данное число округляется до ближайшей степени двойки. При выполнении этой оценки важно учесть возможное увеличение числа подсетей в будущем.

На втором шаге проверяется факт существования достаточного количества адресов хостов в наибольшей подсети организации.

Предположим, что организация получила сеть 193.1.1.0/24, и ей необходимо сформировать шесть подсетей. Наибольшая подсеть должна поддерживать 25 хостов. На первом шаге определяется число битов, требуемых для определения необходимых шести подсетей ( $2^n \geq 6$ ). В данном примере администратор должен определить восемь подсетей ( $2^3 = 8 \geq 6$ ), т. е. для выделения подсетей будут использованы три бита из выделенного адреса. Полученный после выделения

подсетей сетевой префикс будет записан как /27 (24 бита базовой маски + 3 бита на подсети = 27). Это расширенный сетевой префикс и он имеет эквивалентное значение маски подсети 255.255.255.224.

Используемый 27-разрядный расширенный сетевой префикс оставляет 5 бит для задания номеров хостов в каждой из подсетей. Это означает, что в каждой подсети может быть определено до 32 ( $2^5 = 32$ ) индивидуальных адресов хостов. Однако адреса, у которых все биты равны или нулю, или единице, являются зарезервированными, так что общее число адресов хостов в каждой подсети становится равным 30 ( $2^5 - 2 = 30$ ). Пример расчета всех подсетей представлен в таблице 1.1.

Таблица 1.1 – Варианты подсетей для сети 193.1.1.0/24

Сеть	Точечно-десятичная нотация	Двоичное представление адреса
1	2	3
Базовая сеть	193.1.1.0 /24	11000001.00000001.00000001. <u>00000000</u>
Подсеть #0	193.1.1.0 /27	11000001.00000001.00000001. <b>000</b> <u>00000</u>
Подсеть #1	193.1.1.32 /27	11000001.00000001.00000001. <b>001</b> <u>00000</u>
Подсеть #2	193.1.1.64 /27	11000001.00000001.00000001. <b>010</b> <u>00000</u>
Подсеть #3	193.1.1.96 /27	11000001.00000001.00000001. <b>011</b> <u>00000</u>
Подсеть #4	193.1.1.128 /27	11000001.00000001.00000001. <b>100</b> <u>00000</u>
Подсеть #5	193.1.1.160 /27	11000001.00000001.00000001. <b>101</b> <u>00000</u>
Подсеть #6	193.1.1.192 /27	11000001.00000001.00000001. <b>110</b> <u>00000</u>
Подсеть #7	193.1.1.224 /27	11000001.00000001.00000001. <b>111</b> <u>00000</u>

Выделенные жирным биты определяют номер подсети, выделенные курсивом биты используются для задания конкретных адресов.

## 1.2 Рабочее задание

1) Разработайте план IP-адресации для корпоративной сети JVI (рисунок 1.1) с учетом таких показателей, как масштабирование, агрегирование и следующих требований заказчика:

- число хостов в каждой сети, исключая филиалы, в будущем может увеличиться в 1,5 раза, но в данный момент нет необходимости создавать сети увеличенного размера. Следует предусмотреть возможность их будущего расширения за счет временно неиспользуемого адресного пространства;

- может быть добавлен третий отдел (15 хостов) или же эти хосты волеются в сеть первого отдела (решение будет принято по мере развития бизнеса). Дизайн сети должен быть рассчитан на безболезненное слияние и разделение отделов 1 и 3;

- число филиалов может быть увеличено до 4, размер филиала – 9-12 хостов;

- сеть отделов и серверов включаются в сеть Core каждая через свой маршрутизатор.

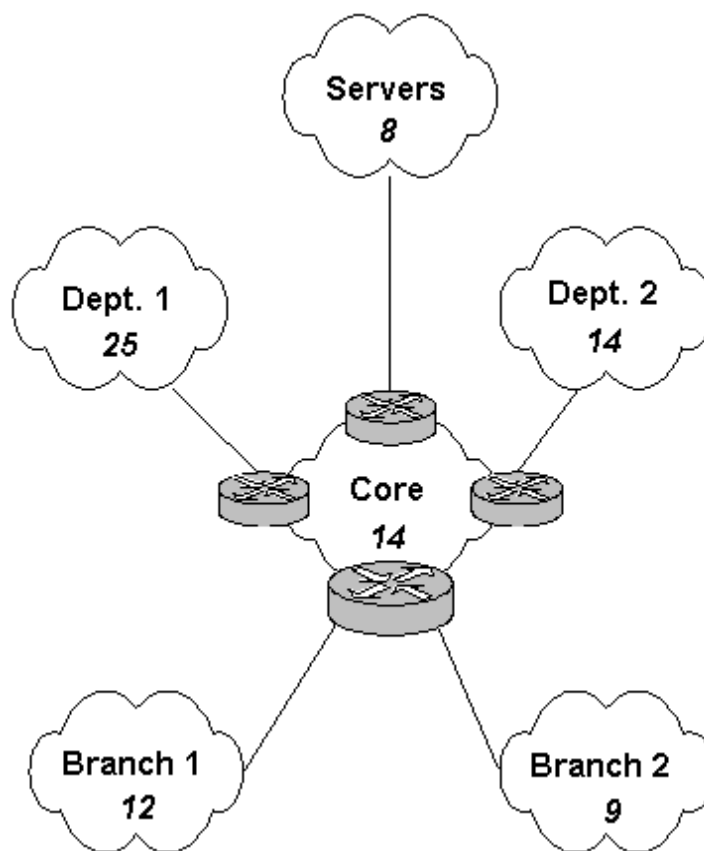


Рисунок 1.1 – Сеть компании

2) По заданным IP-адресу и маске для всей сети компании (таблица 1.2) определите базовый адрес сети, диапазон адресов сети, широковещательный адрес, а также длину префикса.

3) По заданному числу хостов (рисунок 1.1) и базовому адресу сети найдите IP-сети для каждого существующего отдела, филиала, и планируемых подразделений, в которых можно разместить указанное число хостов, (сети указывать в виде "адрес сети/длина префикса (маска)").

4) Заполните таблицу 1.2, записывая подсети в порядке убывания количества хостов

Таблица 1.2

Название подсети	Количество хостов	n	Адрес подсети	Диапазон адресов сети	Широковещательный адрес

Таблица 1.3 – Задание для лабораторной работы 2

Вариант	IP адрес	Маска
1	10.129.56.48	255.255.252.0
2	172.16.25.58	255.254.0.0
3	192.168.52.14	255.255.248.0
4	10.129.56.38	255.255.224.0
5	172.16.25.28	255.255.192.0
6	192.168.52.19	255.255.128.0
7	10.129.56.52	255.255.254.0
8	172.16.25.75	255.252.0.0
9	192.168.52.21	255.248.0.0
10	11.25.36.54	255.224.0.0

### 1.3 Контрольные вопросы

- 1) Назовите основные этапы построения сети.
- 2) Как происходит планирование IP-адресов?

3) Как по заданному числу хостов в сети и заданному диапазону IP-адресов найти все возможные IP-сети внутри данного диапазона, в которых можно разместить указанное число хостов?

4) Как по заданным IP-адресу и маске определить адрес сети, номер хоста, широковещательный адрес, а также длину префикса?

5) Как по заданным IP-адресу длине префикса определить адрес сети, номер хоста, широковещательный адрес, а также маску?

6) Как рассчитать количество подсетей при известной маске и количеству хостов?

7) Как рассчитать количество подсетей при известном количестве хостов?

8) Как рассчитать количество хостов при известной маске?

9) Как рассчитать количество подсетей при известной базовой маске и маске подсети?

10) Как рассчитать маску по известной длине префикса?

## **2 Лабораторная работа №2. Изучение системы моделирования Cisco Packet Tracer**

*Цель работы.* Изучить систему моделирования корпоративных сетей Cisco Packet Tracer. Получить навыки настройки сетевого оборудования, создания сложных сетевых топологий.

### **2.1 Общие сведения**

Packet Tracer (PT) – бесплатный эмулятор сетевой среды, выпускаемый фирмой Cisco, который:

- позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS и визуально) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями;

- включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650; серверы DHCP, HTTP, TFTP, FTP, TIME, рабочие



станции, различные модули к компьютерам и маршрутизаторам, устройства WiFi, различные кабели;

– успешно позволяет создавать сложные макеты сетей, проверять на работоспособность топологии. Внешний вид рабочего окна Packet Tracer показан на рисунке 2.1.

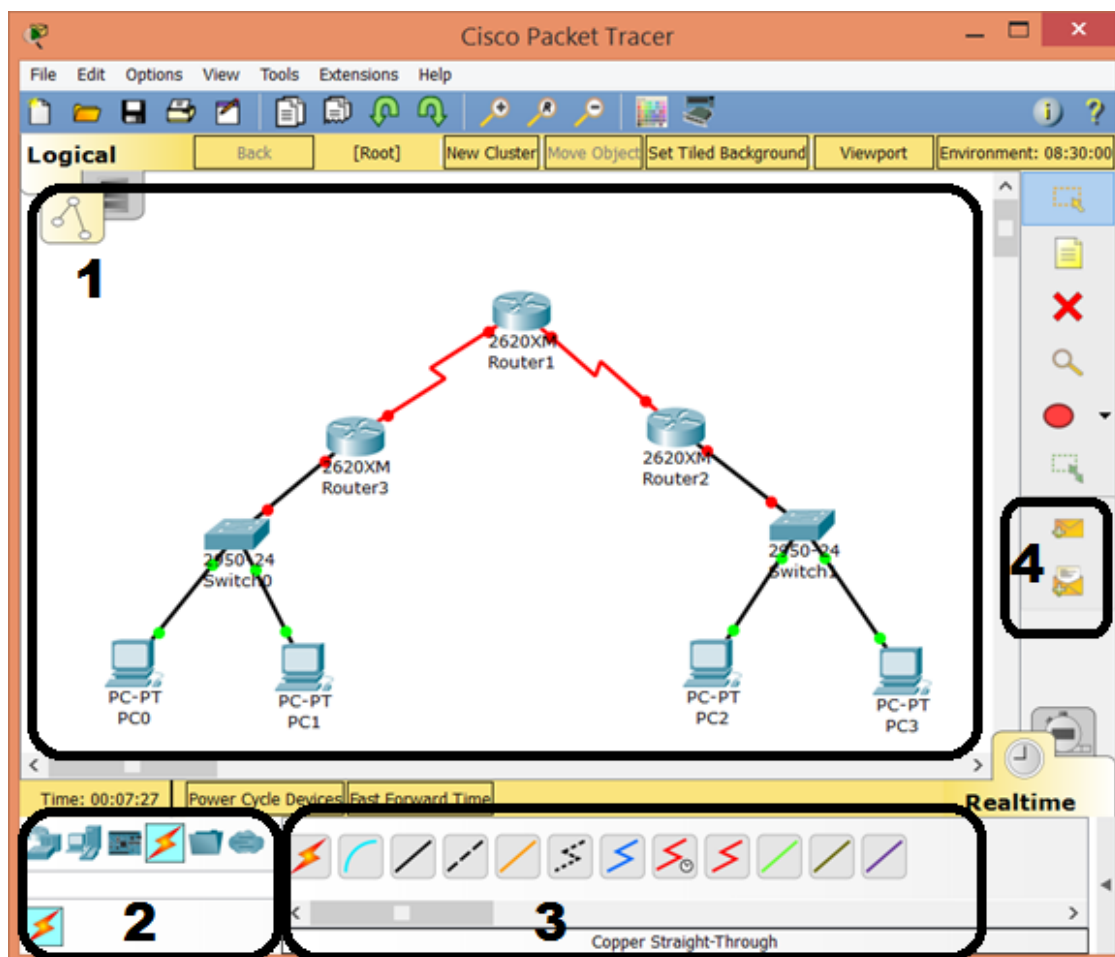


Рисунок 2.1 – Главное окно программы Packet Tracer

Основные области главного окна программы Packet Tracer следующие:

- 1 – рабочая область программы, в этой области можно собирать виртуальные сети, видеть трафик, запускать настройку устройств;
- 2 – область, используемая для выбора типа устройств, которые будут добавляться в рабочую область;
- 3 – область для выбора конкретного устройства для добавления;

– 4 – область, необходимая для визуального запуска сетевого пакета с одного устройства на другое.

В рабочей области отображается *логическая диаграмма сети*. Работа с объектами на логической диаграмме происходит мышью. Чтобы войти в режим настройки оборудования надо кликнуть на нужной картинке оборудования. Откроется окно настройки (рисунок 2.2).

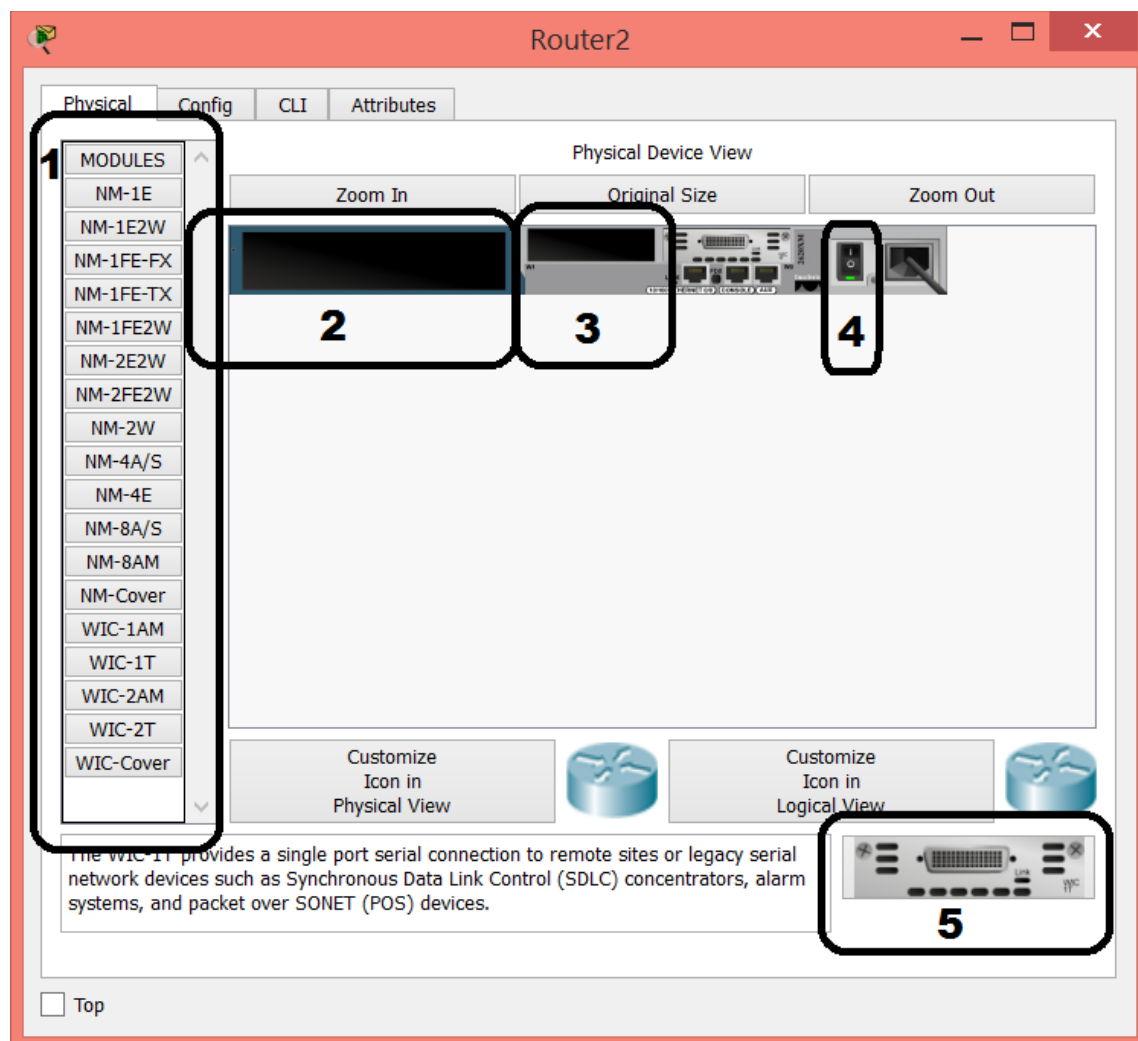


Рисунок 2.2 – Окно настройки

В первой вкладке окна настройки есть следующие элементы:

1) Модули, которые можно вставить в роутер. Чтобы вставить модуль, необходимо сначала выключить устройство (элемент 4), выбрать в списке нужный модуль, он появится в элементе 5. Перетащить мышью изображение модуля в пустой слот для модулей (элемент 2 или 3) и включить устройство.

- 2) Слот для модуля 1.
- 3) Слот для модуля 2.
- 4) Кнопка выключения питания.
- 5) Изображение выбранного модуля.

В маршрутизаторах представлены следующие модули:

- HWIC-4ESW – модуль-коммутатор с 4 портами Ethernet;
- HWIC-AP-AG-B – модуль точки доступа 802.11B/G;
- WIC-1AM – 1 аналоговый порт модема V.90;
- WIC-1ENET – 1 маршрутизируемый порт Ethernet;
- WIC-2AM – 1 аналоговых порта модема V.90;
- WIC-2T – 2 последовательных порта serial;
- WIC-Cover – заглушка.

В каждом маршрутизаторе есть как минимум 2 порта Ethernet. Обычно для модульных маршрутизаторов они называются FastEthernet 0/0 и FastEthernet 0/1. Для немодульных устройств это будет FastEthernet0 и FastEthernet1.

Если в пустой слот вставлена карта расширения, например WIC-1ENET с 1 портом Ethernet в слоте №1, порт в маршрутизаторе будет обозначаться Ethernet0/0/0, где первая цифра 1 – это номер слота. Если карта будет вставлена в слот №2, то порт будет обозначаться Ethernet0/1/0. Последовательные (serial) порты обозначаются в маршрутизаторе аналогично, например, Serial0/0/0. Лучший способ проверить названия интерфейсов – зайти на вкладку «Config» окна настройки (рисунок 2.3).

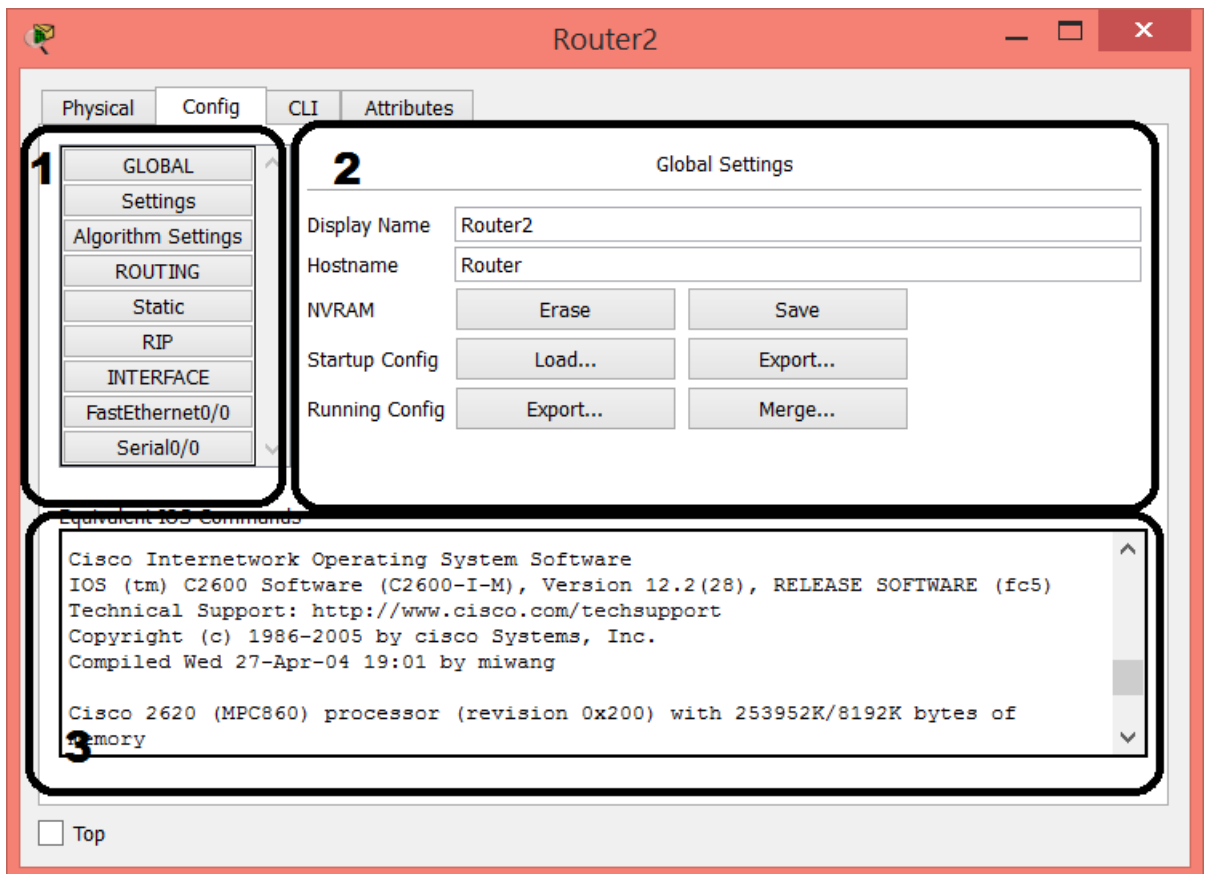


Рисунок 2.3 – Вкладка «Config» окна настройки

В окне настройки маршрутизатора есть следующие элементы:

- 1) Выбор типа настройки, имеет четыре вкладки, выделенные жирным шрифтом:
  - а) GLOBAL – для общих настроек (рисунок 3.4).
  - б) ROUTING – для статической и динамической маршрутизации.
  - в) SWITCHING – для внутренней коммутации между виртуальными подсетями VLAN.
  - г) INTERFACE – настройка конкретных интерфейсов.
- 2) Область «2» предназначена для задания настроек.
- 3) В области «3» показываются эквиваленты команд для настройки маршрутизатора через командную строку (CLI, command line interface). На рисунке 2.4 показана настройка интерфейса.

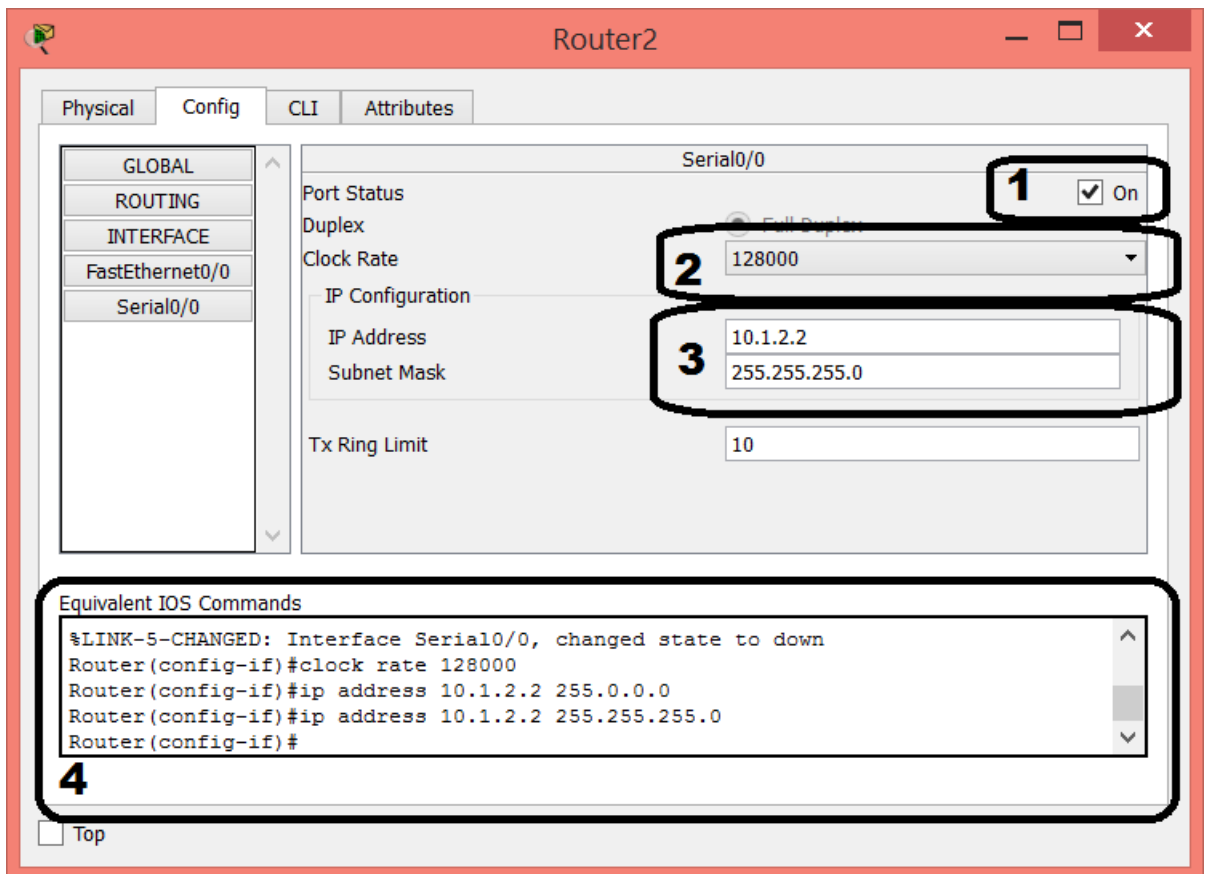


Рисунок 2.4 – Настройка интерфейса

Первое, что необходимо сделать – включить интерфейс (элемент 1). Затем можно задать IP адрес и маску (элемент 3). Для Serial интерфейсов необходимо заполнить еще скорость передачи данных Clock gate (элемент 2). В нижней части окна (элемент 4) будет показано, как сделать то же самое, только без использования графических инструментов, в командной строке.

Для конечных устройств, таких как компьютер, ноутбук, сервер, используется третья вкладка “Desktop”, которая выглядит, как показано на рисунке 2.5.

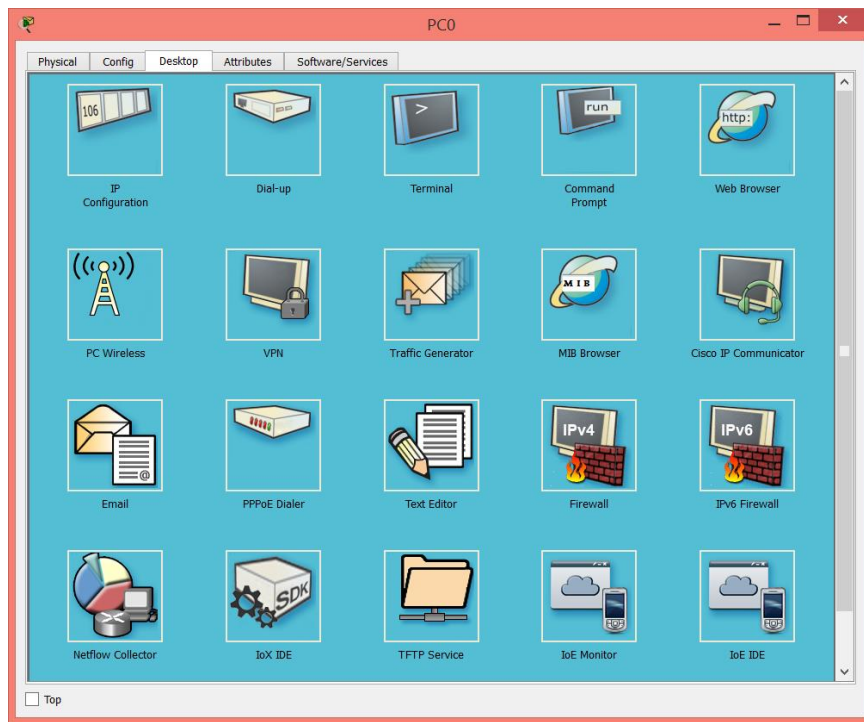


Рисунок 2.5 – Вкладка “Desktop” компьютера

Для настройки IP адреса, маски, шлюза по умолчанию и DNS лучше всего воспользоваться пунктом IP Configuration (рисунок 2.6).

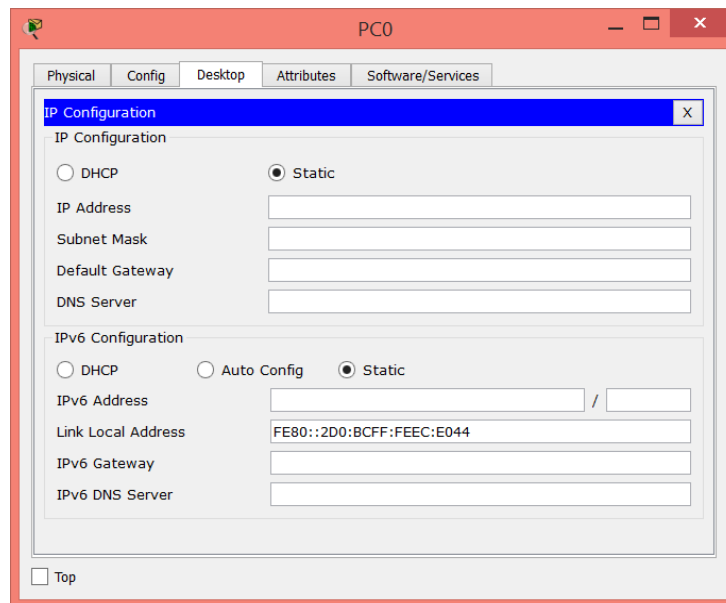


Рисунок 2.6 – Настройка IP параметров компьютера и сервера

Также часто используется пункт Command Prompt (рисунок 2.7). Командная строка поддерживает основные команды для тестирования сети – *ping*, *tracert*, *arp*, *telnet*.

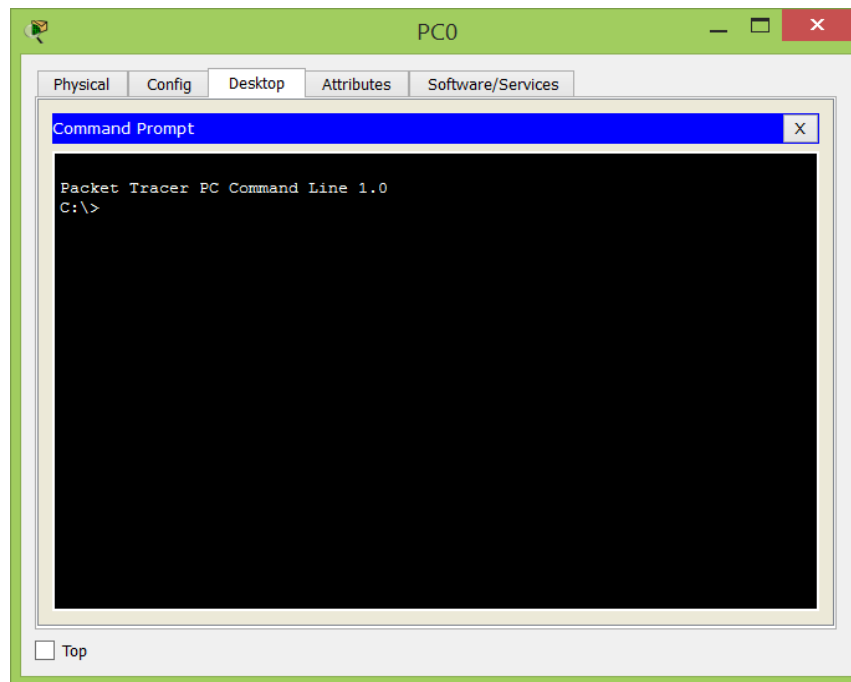


Рисунок 2.7 – Командная строка компьютера

Для проверки Web-серверов можно использовать браузер из пункта Web Browser (рисунок 2.8).

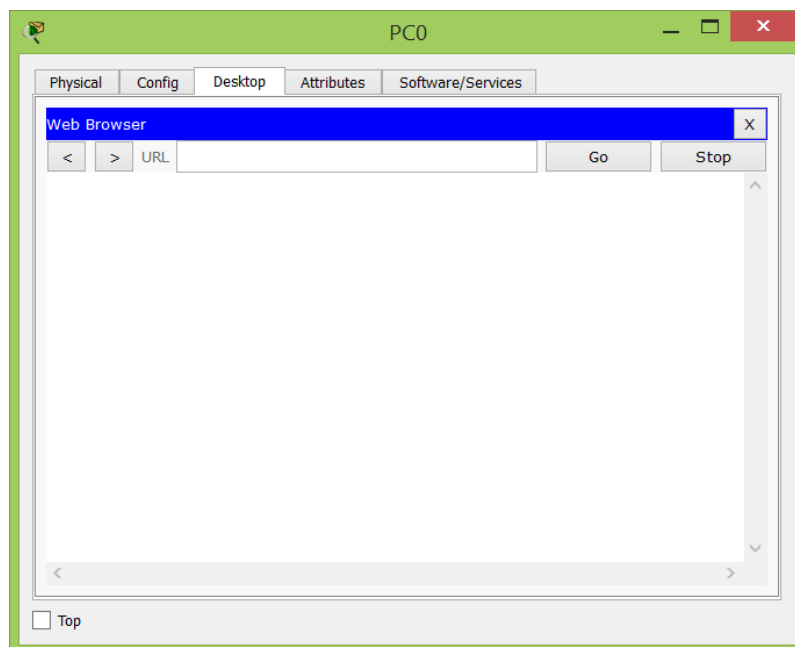


Рисунок 2.8 – Браузер компьютера

Сервер в Packet Tracer имеет также вкладку «Services», показанную на рисунке 2.9.

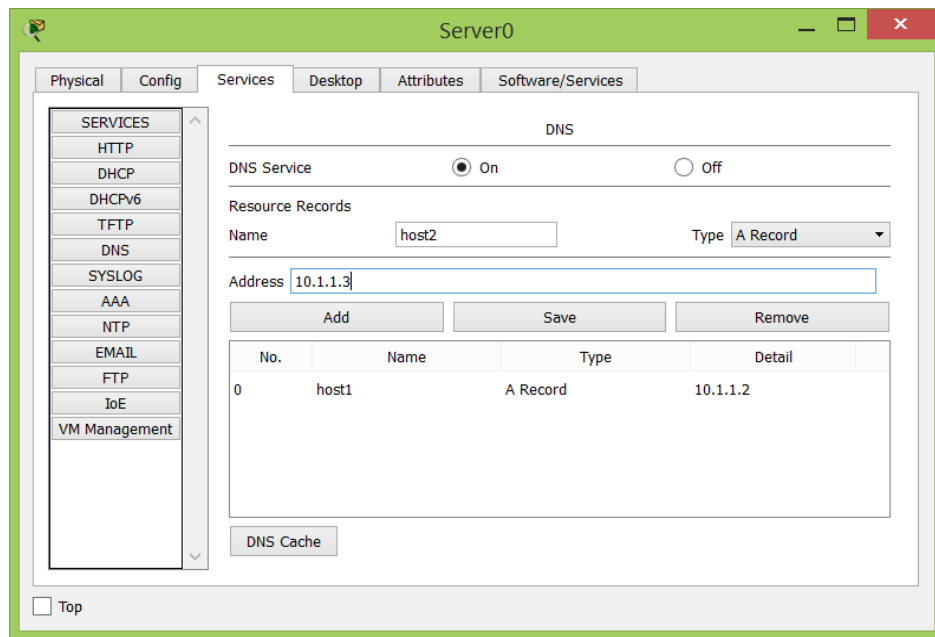


Рисунок 2.9 – Настройка сервисов в сервере

На этой вкладке расположены элементы настройки для сервисов, например DNS. Каждый сервис имеет переключатель On/Off и настройки. Например, в DNS сервере можно вручную задать соответствие IP адреса и доменного имени.

При настройке второго по популярности сервиса – DHCP – необходимо задать такие параметры, как шлюз по умолчанию (default gateway), DNS сервер (обычно это адрес текущего сервера), начальный адрес для раздачи адресов (Start IP address), маску для всех раздаваемых адресов (Subnet mask), количество адресов для резервирования (Maximum number of Users) и имя пула (Pool Name). Пример можно увидеть на рисунке 2.10.



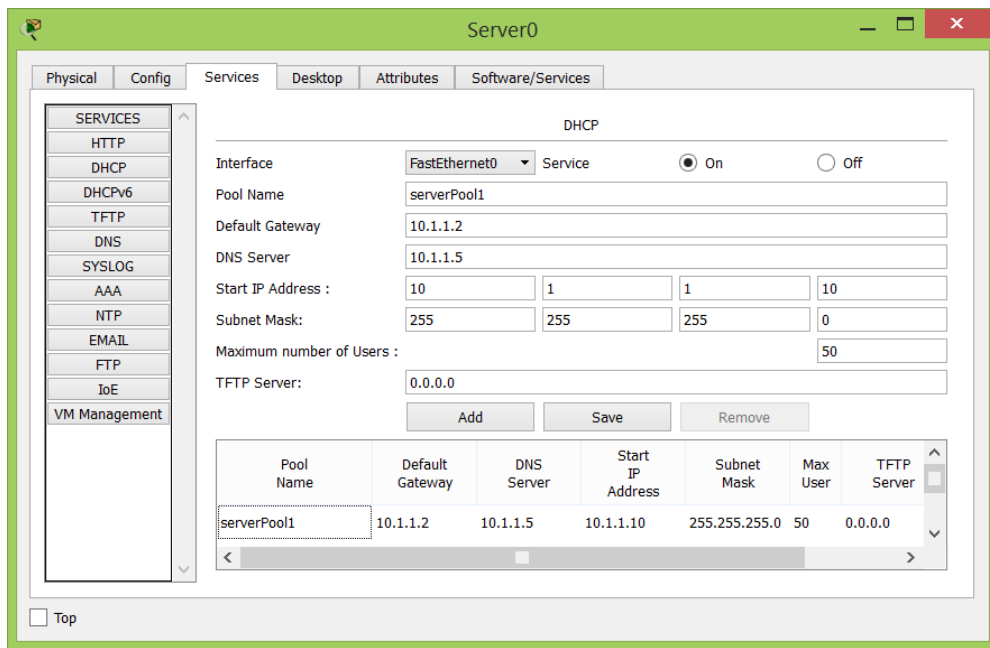


Рисунок 2.10 – Настройка DHCP сервера

В Packet Tracer дополнительно есть множество различных устройств. Символическое изображение показано на рисунке 2.11.

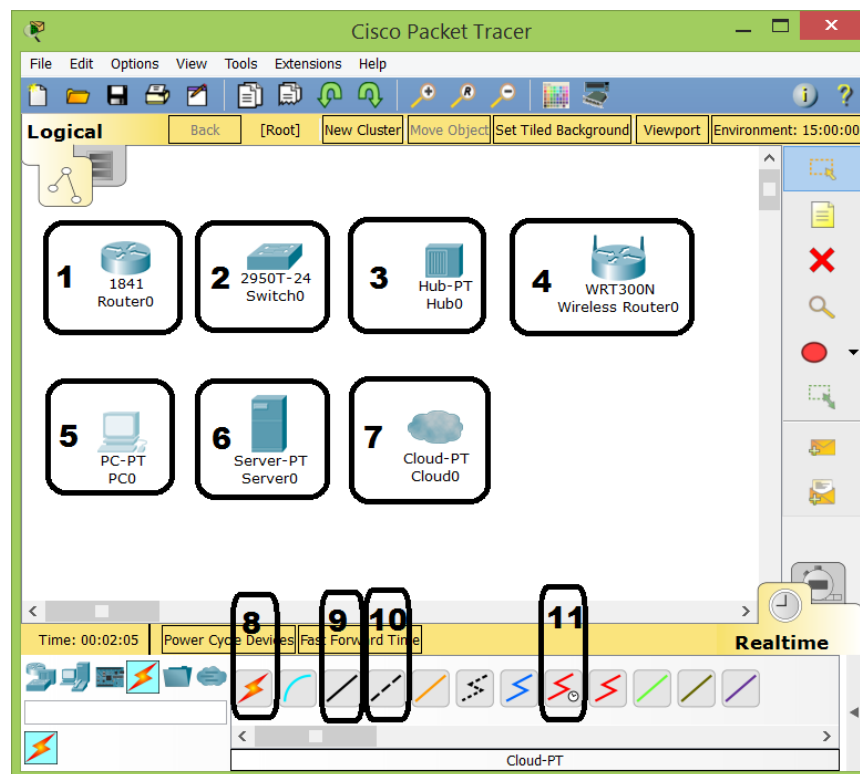


Рисунок 2.11 – Устройства и связи в Packet Tracer

Устройства обозначаются следующим образом:

1 – маршрутизатор, он же «роутер». Используется для передачи данных между сетями;

2 – коммутатор, он же «свич». Используется для объединения компьютеров в одну сеть;

3 – концентратор, он же «хаб». Используется с той же целью, что и коммутатор, но менее интеллектуален, поэтому уже несколько лет не выпускается;

4 – беспроводной маршрутизатор. Обычный маршрутизатор, оснащенный беспроводным модулем. Изображенный на рисунке маршрутизатор относится к серии домашних, поэтому имеет только Веб-интерфейс для настройки;

5 – персональный компьютер;

6 – сервер;

7 – облако, изображает провайдера Интернет;

Кроме устройств сеть состоит еще из соединительных носителей, например, из кабелей. На рисунке они обозначены как:

8 – автоматический определитель типа кабеля. Используется для быстрого соединения устройств. Имеет существенный недостаток: нельзя проконтролировать, в какой порт устройства будет присоединен кабель. Это очень неудобно, когда надо знать интерфейс, например, при соединении двух маршрутизаторов;

9 – прямой кабель, он же «патч-корд». Используется для соединения разных классов устройств, например компьютер-коммутатор, коммутатор-маршрутизатор;

10 – обратный кабель, он же «кроссовер». Используется для соединения одинакового класса устройств, например компьютер-компьютер, коммутатор-коммутатор, компьютер-маршрутизатор;

11 – последовательный кабель, он же «серийный». Используется исключительно для соединения портов типа Serial между маршрутизаторами.

## **2.2 Рабочее задание**

1) Создайте в Packet Tracer простейшую сеть, состоящую из двух компьютеров. Соедините их подходящим кабелем. Настройте IP адресацию и проведите тестирование соединения.

2) Создайте в Packet Tracer топологию, состоящую из двух компьютеров, коммутатора и сервера. Настройте на сервере DHCP сервис и IP параметры. Обновите на компьютерах IP параметры для проверки работы DHCP. Протестируйте связь от компьютеров к серверу.

3) Создайте в Packet Tracer топологию, состоящую из двух компьютеров и маршрутизатора cisco 1841. Соедините компьютеры с маршрутизатором соответствующим кабелем. Настройте параметры IP на маршрутизаторе, затем на компьютерах. Протестируйте соединений с помощью утилиты *tracert*.

IP параметры необходимо взять из таблиц 2.1 – 2.2.

Таблица 2.1 – Параметры IP для заданий 1 и 2

Вариант	IP сеть для компьютеров
1	2
1	192.168.100.128/26
2	192.168.100.64/27
3	10.14.2.192/26
4	10.18.22.16/28
5	172.16.32.32/27
6	192.168.100.128/26
7	192.168.100.64/27
8	10.14.2.192/26
9	10.18.22.16/28
10	172.16.32.32/27

Таблица 2.3 – Параметры IP для задания 3

Вариант	IP сеть для компьютера 1	IP сеть для компьютера 2
1	2	3
1	172.16.32.32/27	10.14.2.192/26

2	10.18.22.16/28	192.168.100.128/26
3	192.168.100.64/27	10.18.22.16/28
4	10.14.2.192/26	172.16.32.32/27
5	192.168.100.128/26	192.168.100.64/27
6	172.16.32.32/27	10.14.2.192/26
7	10.18.22.16/28	192.168.100.128/26
8	192.168.100.64/27	10.18.22.16/28
9	10.14.2.192/26	172.16.32.32/27
10	192.168.100.128/26	192.168.100.64/27

### 2.3 Контрольные вопросы

- 1) Каким типом кабеля соединяется маршрутизатор и компьютер?
- 2) Чем отличается настройка Serial интерфейса от остальных?
- 3) Какие данные требуются для настройки DHCP сервера?
- 4) Назовите основные сетевые устройства.
- 5) Назовите основные типы интерфейсов на маршрутизаторе.
- 6) Опишите процесс настройки IP адресации на маршрутизаторе.
- 7) Опишите процесс проверки соединений между устройствами.
- 8) Чем кроссовер отличается от прямого кабеля?
- 9) Чем отличается концентратор от коммутатора?
- 10) Какие существуют дополнительные инструменты на конечных устройствах?

## 3 Лабораторная работа №3. Создание логической схемы сети в Cisco Packet Tracer

*Цель работы.* Изучить принципы построения сложных сетей. Изучить работу динамической маршрутизации. Получить навыки тестирования сложных сетей.

### 3.1 Общие сведения

Работа будет проводиться в эмуляторе сетей Cisco Packet Tracer. Логическая схема сети показана на рисунке 3.1.

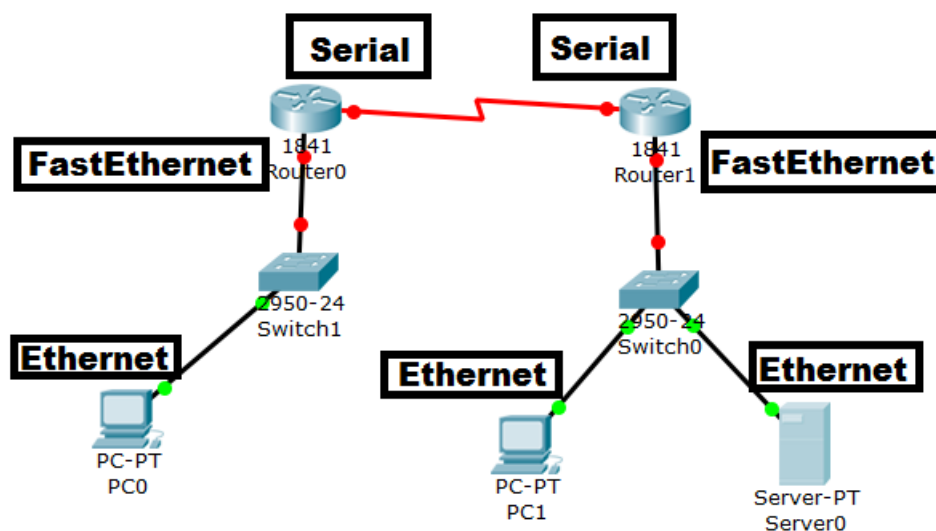


Рисунок 3.1 – Схема сети

Для реализации корректной работы сети необходимо, во-первых, рассчитать IP адреса для каждой из сетей. Для сети 1 (слева) возьмем адрес 10.1.1.0/24, для сети 2 (справа) – адрес 10.1.3.0/24, для связи между маршрутизаторами адрес 10.2.1.0/30.

Возьмем первый адрес сети 1 и 2 в качестве адреса интерфейса маршрутизатора, второй адрес – в качестве адреса конечных устройств. Общая адресация показана в таблице 3.1.

Таблица 3.1 – Конечные адреса для сети

Устройство	Адрес/маска	Шлюз	DNS
1	2	3	4
PC1	10.1.1.2/255.255.255.0	10.1.1.1	10.1.3.2
Router1 - FastEthernet0/0	10.1.1.1/255.255.255.0	-	-
Router1 - Serial0/0/0	10.1.2.1/255.255.255.252	-	-

Router2 - FastEthernet0/0	10.1.3.1/255.255.255.0	-	-
Router2 - Serial0/0/0	10.1.2.2/255.255.255.252	-	-
PC2	10.1.3.3/255.255.255.0	10.1.3.1	10.1.3.2
Server1	10.1.3.2/255.255.255.0	10.1.3.1	10.1.3.2

Затем необходимо настроить IP адреса на компьютерах и сервере (рисунок 4.2). Шлюзом указывается ближайший интерфейс ближайшего маршрутизатора, DNS-сервер находится на сервере в сети 2.

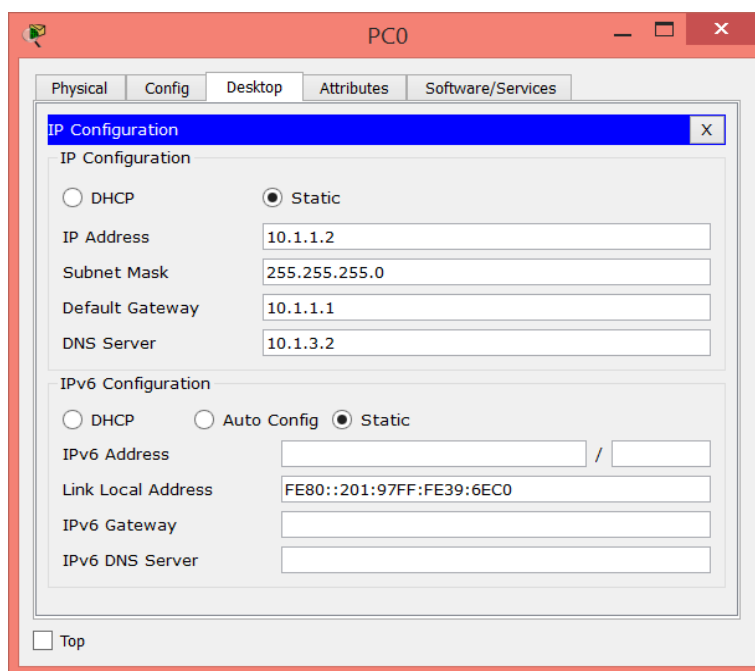


Рисунок 3.2 – Настройка параметров IP конечных устройств

Настройка IP адреса на интерфейсе маршрутизатора ничем не отличается от настройки компьютера, кроме того, что указывать шлюз и DNS сервер не надо (рисунок 3.3).

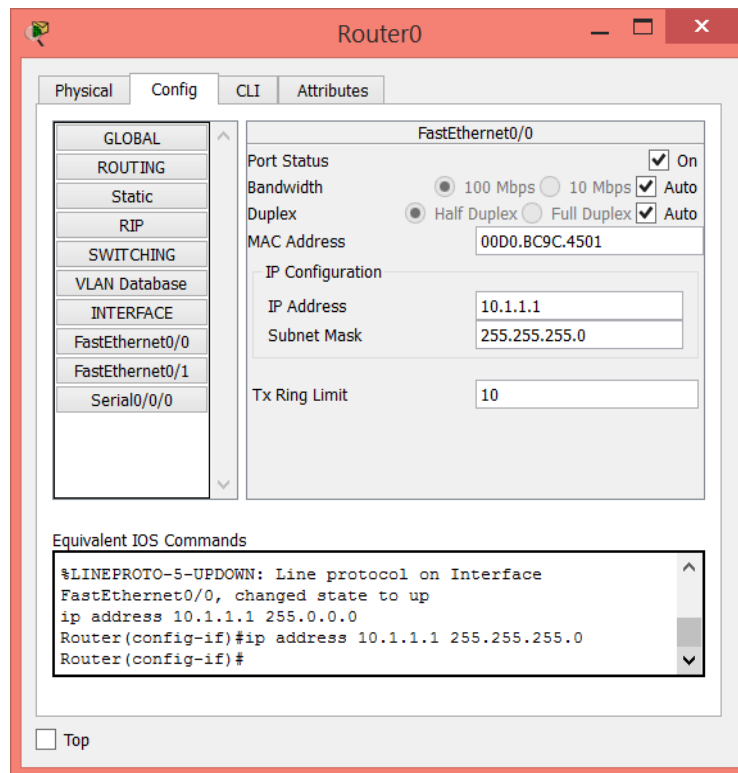


Рисунок 3.3 – Настройка FastEthernet на маршрутизаторах

Настройка интерфейса Serial отличается тем, что дополнительно необходимо указать скорость интерфейса «Clock Rate» (рисунок 3.4).

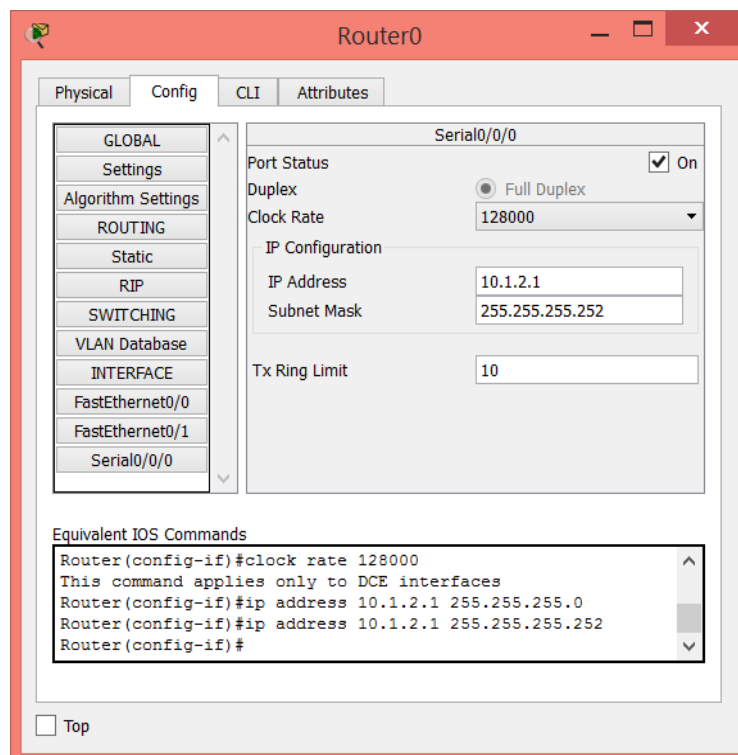


Рисунок 3.4 – Настройка Serial на маршрутизаторах

Затем необходимо настроить динамическую маршрутизацию на маршрутизаторе. В качестве протокола был выбран RIPv2 (Routing Internet Protocol Version 2) как самый простой в настройке (рисунок 3.5). Необходимо на вкладке RIP задать адрес всех сетей, которые есть на данном маршрутизаторе (ни в коем случае не на соседнем). При добавлении сетей (кнопка «ADD») они могут агрегироваться из-за недостатков протокола.

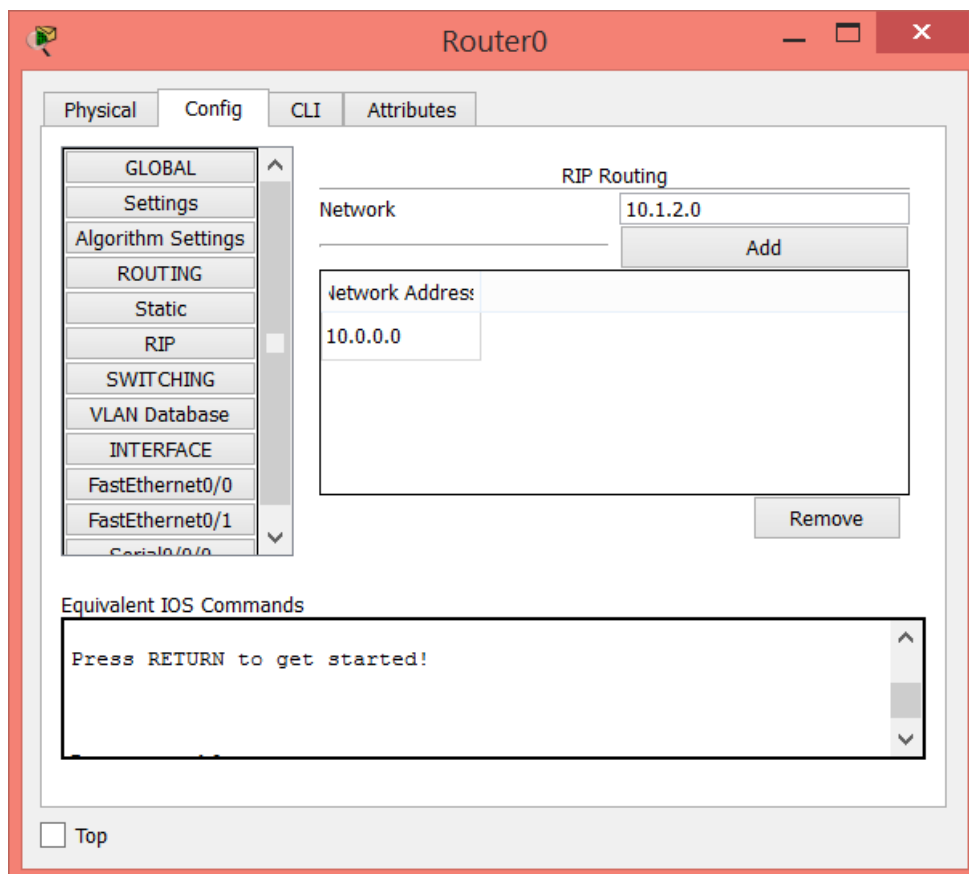


Рисунок 3.5 – Настройка RIP на маршрутизаторе

После добавления сетей необходимо переключить RIP на вторую версию протокола. Для этого необходимо сразу после добавления сетей переключиться на вкладку «CLI» и набрать команду «*version 2*», после чего нажать Ctrl-Z (рисунок 3.6).



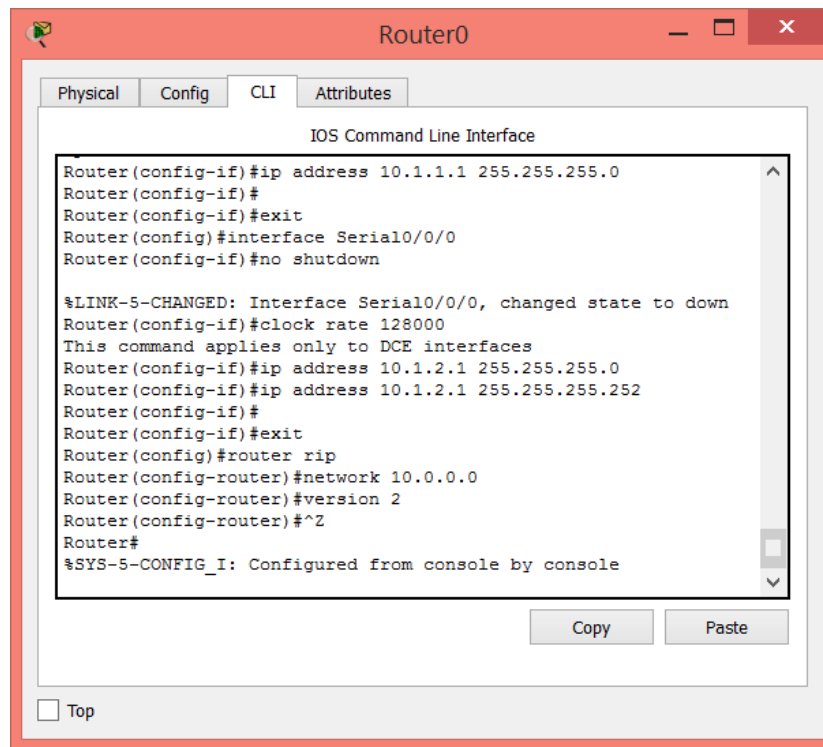
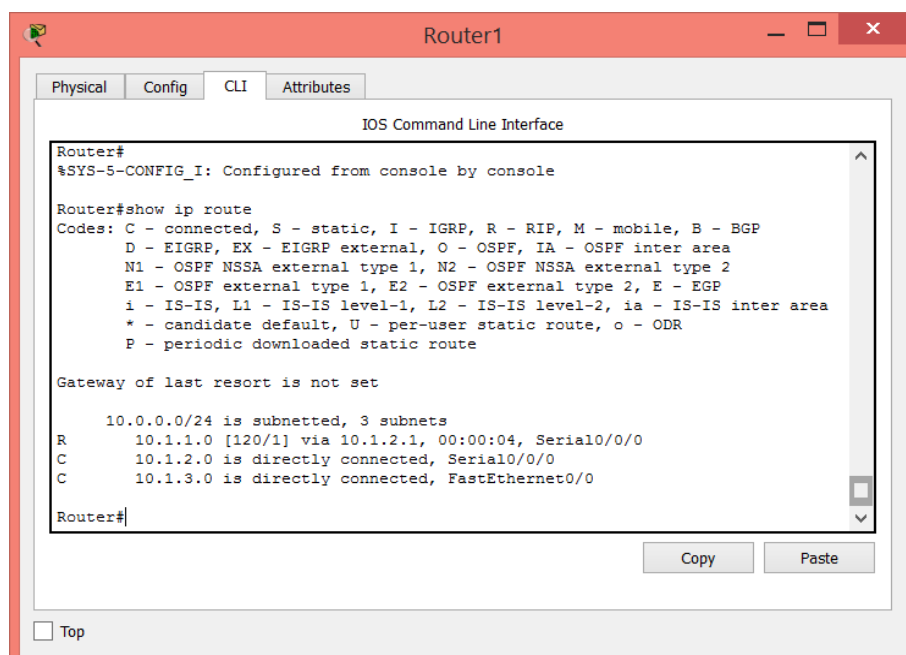


Рисунок 3.6 – Настройка версии RIP на маршрутизаторе

После настройки обоих маршрутизаторов необходимо проверить корректность работы. Для этого необходимо набрать в командной строке команду «*show ip route*» и нажать «Enter». В выводе команды должна быть строка, начинающаяся буквой «R», что значит RIP (рисунок 3.7). Если такой строки нет, значит, неправильно произведена настройка.



### Рисунок 3.7 – Проверка работы RIP на маршрутизаторах

Затем необходимо настроить DNS сервер. Для этого на вкладке «DNS» сервера Server1 нужно добавить имя будущего сервера (например, server или yandex.ru) и добавить IP адрес текущего сервера и нажать кнопку «Add».

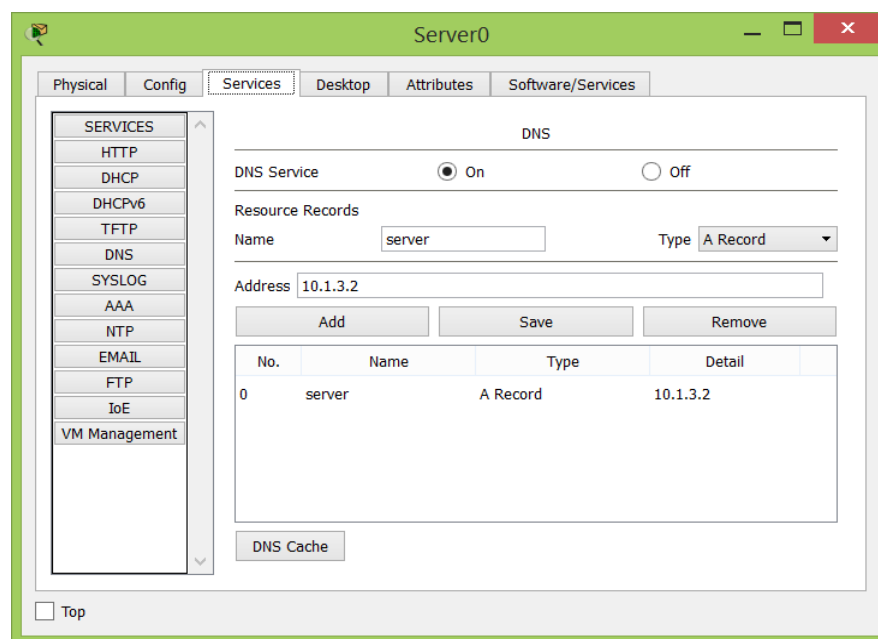


Рисунок 4.7 – Настройка DNS службы на сервере

После окончания всех настроек необходимо проверить работу сети командой *ping*. Сначала проверим связь по IP протоколу. Для этого используем IP адрес сервера в команде *Ping* на компьютере PC1. Если связь работает (первый пакет может потеряться, это нормально), будет выведена информация о задержках пакетов и статистическая информация. После этого необходимо проверить работу DNS службы командой *ping ИМЯ*, где *ИМЯ* – это доменное имя, заданное в DNS сервере.

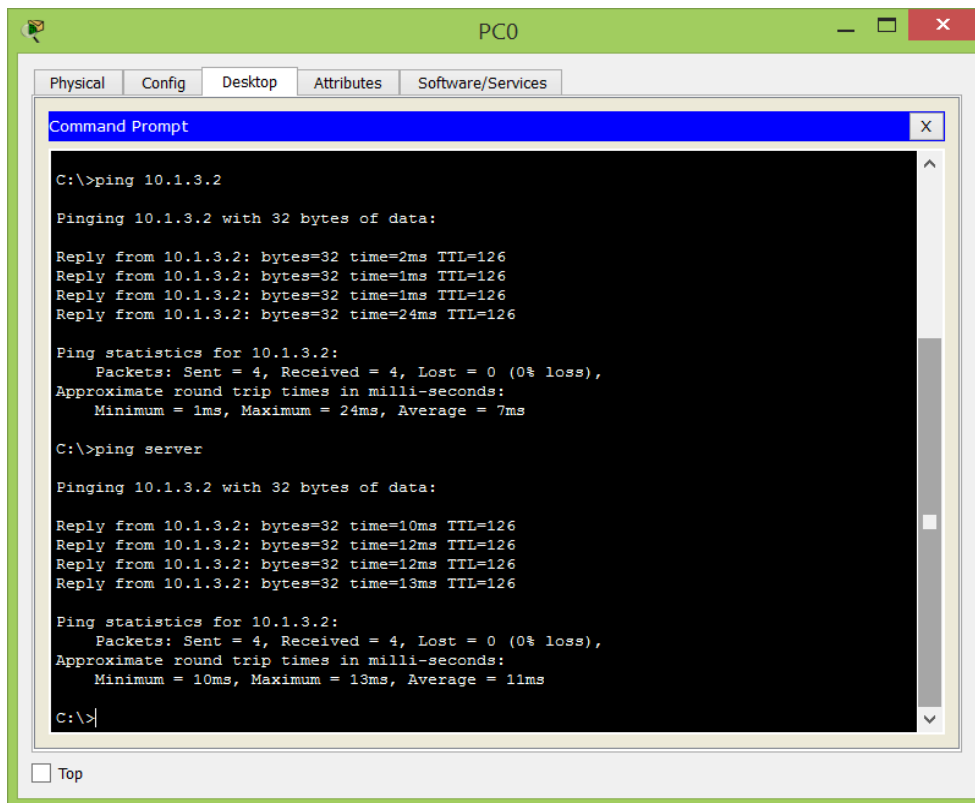


Рисунок 3.8 – Проверка с помощью PING по IP адресу и доменному имени

Если проверка Ping завершилась успешно, необходимо проверить работу Web-сервера. Для этого на компьютере PC1 нужно на вкладке «Desktop» выбрать «Web Browser» и в строке адреса набрать доменное имя сервера (рисунок 3.9).

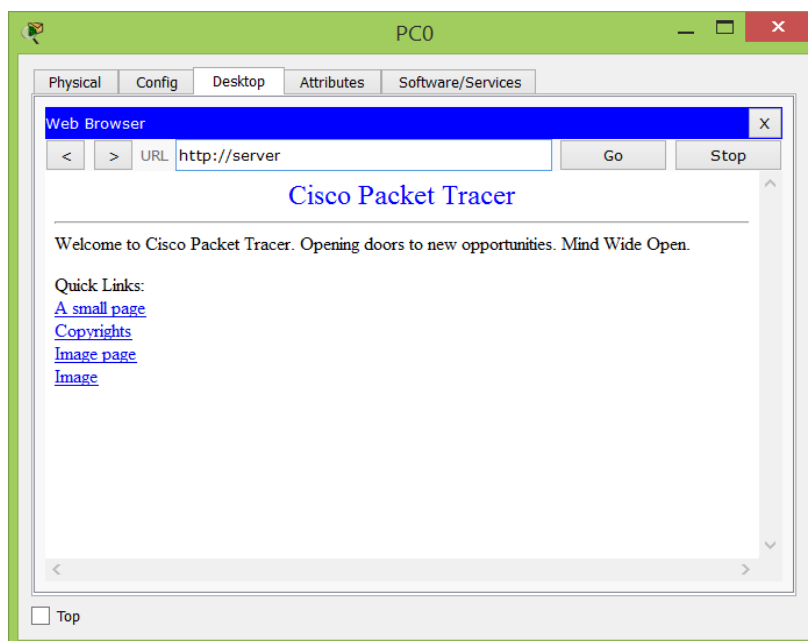


Рисунок 3.9 – Проверка через Веб-браузер

Если все тесты пройдены успешно, значит, сеть работает корректно.

### 3.2 Рабочее задание

1) Собрать схему сети (рисунок 3.1) в программе Packet Tracer. После сборки сети следует перерисовать (или распечатать) эту схему и подписать ВСЕ интерфейсы ВСЕХ устройств, в том числе интерфейсы присоединения кабелей.

2) Провести проектирование IP адресации, подписать все IP адреса всех интерфейсов оборудования.

3) Настроить компьютеры и сервер. Задать им IP адреса и маски в соответствии с п.2. Подписать эти адреса и маски в схеме. Настроить DNS службу.

4) Сконфигурировать маршрутизаторы. В настройках включить нужные интерфейсы (по схеме), задать IP адрес, маску для каждого из интерфейсов.

5) Использовать *ping*-запросы из командной строки для проверки доступности или недоступности связи.

6) Настроить динамическую маршрутизацию в настройках маршрутизаторов.

7) Использовать *ping*-запросы из командной строки для проверки связи.

8) Использовать трассировку маршрута (*tracert*, *tracert*) для проверки пути следования пакетов.

9) Использовать Веб-браузер для проверки работы сервера.

Варианты заданий показаны в таблице 3.1

Таблица 3.1 – Параметры IP

Вариант	IP сеть для сети 1	IP сеть для сети 2	IP сеть для связи между маршрутизаторами
1	2	3	4
1	172.16.32.32/27	10.14.2.192/26	10.18.22.16/30
2	10.18.22.16/28	192.168.100.128/26	172.16.32.32/30
3	192.168.100.64/27	10.18.22.16/28	10.14.2.192/30
4	10.14.2.192/26	172.16.32.32/27	192.168.100.128/30
5	192.168.100.128/26	192.168.100.64/27	10.0.0.0/30

6	172.16.32.32/27	10.14.2.192/26	10.18.22.16/30
7	10.18.22.16/28	192.168.100.128/26	172.16.32.32/30
8	192.168.100.64/27	10.18.22.16/28	10.14.2.192/30
9	10.14.2.192/26	172.16.32.32/27	192.168.100.128/30
10	192.168.100.128/26	192.168.100.64/27	10.0.0.0/30

### 3.3 Контрольные вопросы

- 1) Что такое RIP?
- 2) Как настроить RIP на поддержку двух сетей?
- 3) Опишите настройку маршрутизации с помощью командной строки.
- 4) На каком уровне модели OSI происходит проверка связи с помощью протокола NTTP?
- 5) На каком уровне модели OSI происходит проверка связи с помощью команды ping?
- 6) Каким образом работает команда *ping ИМЯ*?
- 7) Что необходимо настроить для поддержки второй версии RIP?
- 8) IP адреса на последовательных интерфейсах маршрутизатора должны располагаться в разных подсетях или в одной?
- 9) IP адреса на Ethernet интерфейсах маршрутизатора должны располагаться в разных подсетях или в одной?
- 10) При проверке Web-браузером, какие уровни модели OSI проверяются?

## 4 Лабораторная работа №4. Протокол OSPF

*Цель работы.* Научиться настраивать динамическую маршрутизацию на основе протокола OSPF.

### 4.1 Основные теоретические положения

Протокол маршрутизации OSPF (Open Shortest Path First) – динамический, внутридоменный, распределенный, иерархический, многопутевой и каналный. OSPF-маршрутизаторы обмениваются обновлениями при изменении таблицы состояния канала. Чтобы выявить сбой, маршрутизатор рассылает сообщения “еще жив”. Протокол OSPF поддерживает запросы QoS (quality of service), когда

приложение сообщает о срочности некоторых данных. В этом случае OSPF может по своему усмотрению использовать имеющиеся каналы, чтобы максимально быстро отправить данные.

Протокол OSPF является протоколом внутреннего шлюза (Interior Gateway Protocol – IGP). Он распространяет данные о доступных маршрутах между маршрутизаторами одной автономной системы.

Преимуществами протокола OSPF являются:

- отсутствие ограничений на размер сети;
- высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- рассылка обновлений маршрутов только при изменении топологии;
- поддержка сетевых масок переменной длины (VLSM);
- передача обновлений маршрутов с использованием адресов типа multicast;
- оптимальное использование пропускной способности;
- использование алгоритма SPF для расчета пути к месту назначения с наименьшей стоимостью;
- периодическая рассылка полной таблицы маршрутизации не производится;
- аутентификация маршрутов.

OSPF-маршрутизаторы обмениваются сообщениями о состоянии каналов связи, информируя друг друга о:

- добавлении нового соседнего маршрутизатора;
- выходе из строя канала;
- восстановлении канала.

В случае изменения топологии сети (например, при выходе из строя одного из каналов или при добавлении нового маршрутизатора) все маршрутизаторы, на которые влияет данное изменение, рассылают извещения LSA для обновления маршрутов остальным маршрутизаторам сети. Все маршрутизаторы вносят нужные изменения в базы данных топологий, перестраивают деревья SPF для поиска кратчайшего пути к каждой сети и обновляют маршруты в своих таблицах маршрутизации.

Протокол OSPF альтернативен протоколу RIP в качестве внутреннего протокола маршрутизации. OSPF является протоколом состояния маршрута, причем в качестве метрики используется коэффициент качества обслуживания. Каждый маршрутизатор имеет полную информацию о состоянии всех интерфейсов всех маршрутизаторов автономной системы.

Автономную систему можно разделить на несколько областей, куда могут входить отдельные ЭВМ или целые сети. В этом случае внутренние маршрутизаторы области могут не иметь информации о топологии остальной части автономной системы. Сеть чаще всего имеет выделенный маршрутизатор, являющийся источником маршрутной информации для остальных маршрутизаторов AS.

Каждый маршрутизатор сам решает задачу оптимизации маршрутов. В случае, когда к месту назначения ведут несколько эквивалентных маршрутов, информационный поток делится между ними поровну. Переходные процессы в OSPF завершаются быстрее, чем в RIP. В процессе выбора оптимального маршрута анализируется ориентированный граф сети.

Распределение нагрузки между параллельными каналами (Load balancing) заключается в следующем. При использовании протокола маршрутизации OSPF допускается существование нескольких маршрутов в направлении некоторого узла сети. В том случае, если эти маршруты обеспечивают одинаковое качество передачи данных, информационный поток в адрес данного узла может быть направлен по всем этим каналам одновременно, что обеспечит существенное увеличение скорости передачи данных.

Использование процедуры установления подлинности целесообразно в тех информационных системах, в которых большое внимание уделяется информационной безопасности. В таких системах маршрутизаторы, которые участвуют в процессе определения маршрута, должны выполнить совокупность действий, которая необходима для установления приемником подлинности источника передаваемых данных (authentication procedure). Только в том случае, если источник передаваемых данных успешно выполнил процедуру

аутентификации, те данные о маршрутах, которые были от него получены, принимаются для обработки.

Существуют следующие способы организации обмена информацией о маршрутах.

1. Использование адресов типа multicast для информационного обмена между маршрутизаторами в процессе определения маршрута. Использование таких адресов позволяет отказаться от использования адресов типа broadcast, что в свою очередь приводит к повышению эффективности использования вычислительных ресурсов сети.

2. Использование аппарата «назначенных» (designated) маршрутизаторов. Использование этой возможности позволяет существенно сократить объем служебного трафика в том случае, когда несколько маршрутизаторов подключены к одной сети.

В отличие от протокола маршрутизации RIP, который для сравнения маршрутов может использовать только их длину, выраженную в числе переходов, протокол маршрутизации OSPF использует для этой же цели специальный критерий, который называется метрика. Метрика маршрута в протоколе OSPF формируется по специальному алгоритму и учитывает следующие параметры:

- пропускная способность канала;
- величина задержки распространения сигнала в канале;
- надежность канала;
- загруженность канала;
- размер максимального блока данных, который может быть передан через данный канал.

Использование такой метрики позволяет более объективно оценивать маршруты и, при наличии выбора, принимать эффективное и целесообразное решение.

Для обеспечения формирования и обслуживания этих баз данных маршрутизаторы OSPF должны обмениваться специальными сообщениями. В частности такие сообщения формируются в том случае, если в сети появился новый



маршрутизатор или изменилось состояние канала передачи данных. При получении сообщения об изменениях в структуре сети, каждый маршрутизатор вносит соответствующие изменения в свою копию базы данных. Таким образом, в каждый момент времени все базы данных маршрутизаторов, которые находятся внутри одной автономной системы, являются идентичными и адекватно отображают структуру информационного взаимодействия внутри автономной системы. Для того, чтобы определить маршрут по которому должен быть передана дейтаграмма, каждый маршрутизатор, на основании своей копии базы данных, строит дерево кратчайших путей. В вершине своего дерева каждый из маршрутизаторов размещает себя самого.

При описании алгоритма OSPF используются несколько следующих специальных терминов и понятий.

1. Autonomous System (AS), автономной системой называется группа маршрутизаторов, которая для обеспечения взаимного обмена информацией о маршрутах использует единый протокол маршрутизации.

2. Neighboring Routers – маршрутизаторы, которые подключены к одной и той же сети называются соседними маршрутизаторами.

3. Adjacency – два маршрутизатора из числа соседних могут быть выбраны для установления близких отношений, которые предполагают обмен информацией о маршрутах. Близкие отношения устанавливаются не в каждой паре соседствующих маршрутизаторов.

4. Link State Advertisement (LSA) – блок данных, который содержит информацию о состоянии маршрутизатора или сети называется объявлением о состоянии канала. В том случае, если данное объявление представляет состояние маршрутизатора, оно должно содержать информацию о статусе его интерфейсов и близких ему маршрутизаторов. Каждое такое объявление распространяется по всей автономной системе. Совокупность таких LSA формирует базу данных маршрутизации в каждом из маршрутизаторов.

5. Flooding – процесс распространения LSA в пределах автономной системы называется затоплением.

Одним из компонентов протокола OSPF является Hello протокол, с помощью которого маршрутизаторы устанавливают и обслуживают соседские отношения. С помощью этого протокола в частности производится выбор назначенного маршрутизатора для некоторых сетей.

Возможно возникновение ситуации, когда к одной сети типа broadcast окажутся подключенными несколько входящих в один домен маршрутизации OSPF маршрутизаторов. Для того чтобы избежать дублирования представления сети типа broadcast несколькими маршрутизаторами в протоколе OSPF используется специальный алгоритм, с помощью которого выбирается Designated Router (назначенный маршрутизатор, DR). В этом случае только один маршрутизатор обеспечивает передачу информации о маршрутах в сегменте сети.

В сетях с множественным доступом отношения соседства устанавливаются между всеми маршрутизаторами. Если бы все маршрутизаторы в состоянии соседства обменивались топологической информацией, это привело бы к рассылке большого количества копий LSA. Если, к примеру, количество маршрутизаторов в сети с множественным доступом равно  $n$ , то будет установлено  $n(n-1)/2$  отношений соседства. Каждый маршрутизатор будет рассылать  $n-1$  LSA своим соседям, плюс одно LSA для сети, в результате сеть сгенерирует  $nI$  LSA.

Для предотвращения проблемы рассылки копий LSA в сетях с множественным доступом выбираются выделенный маршрутизатор (DR) и запасной выделенный маршрутизатор (BDR).

Выделенный маршрутизатор управляет процессом рассылки LSA в сети. Каждый маршрутизатор сети устанавливает отношения смежности с DR. Информация об изменениях в сети отправляется DR маршрутизатором, обнаружившим это изменение, а DR отвечает за то, чтобы эта информация была отправлена остальным маршрутизаторам сети.

Недостатком в схеме работы с DR маршрутизатором является то, что при выходе его из строя должен быть выбран новый DR. Новые отношения соседства должны быть сформированы и, пока базы данных маршрутизаторов не

синхронизируются с базой данных нового DR, сеть будет недоступна для пересылки пакетов. Для устранения этого недостатка выбирается BDR.

Существует также резервный выделенный маршрутизатор (backup designated router, BDR). Каждый маршрутизатор сети устанавливает отношения соседства не только с DR, но и BDR. DR и BDR также устанавливают отношения соседства и между собой. При выходе из строя DR, BDR становится DR и выполняет все его функции. Так как маршрутизаторы сети установили отношения соседства с BDR, время недоступности сети минимизируется.

Маршрутизатор, выбранный DR или BDR в одной присоединённой к нему сети с множественным доступом, может не быть DR (BDR) в другой присоединённой сети. Роль DR (BDR) является свойством интерфейса, а не свойством всего маршрутизатора.

Протокол OSPF относится к протоколам, которые обеспечивают иерархическую маршрутизацию. При использовании протоколов данного типа информационная система разбивается на независимые области по функциональному принципу. Как уже было выше отмечено, область №0 играет роль backbone и используется для обеспечения информационного взаимодействия между остальными областями.

В зависимости от того, к какой области принадлежит маршрутизатор, и какие информационные потоки через него проходят, различают четыре типа маршрутизаторов OSPF:

- Internal Router – IR;
- Area Border Router – ABR;
- Backbone Router – BR;
- AS Boundary Router – ASBR.

Маршрутизаторы типа Internal Router – внутренний маршрутизатор – размещаются внутри автономной системы и не имеют интерфейсов, которые выходят за пределы этой автономной системы.

К маршрутизаторам Backbone Router относятся все маршрутизаторы, которые имеют интерфейсы в нулевую область.

Маршрутизаторы типа Area Border Router (пограничный маршрутизатор области) – размещаются на границе между несколькими областями в пределах автономной системы. Такие маршрутизаторы имеют интерфейсы, которые связывают их с маршрутизаторами, находящимися в других областях. Маршрутизаторы данного типа предназначены для того, чтобы передавать информацию о маршрутах между различными областями.

Маршрутизаторы типа AS Boundary Router (пограничный маршрутизатор автономной системы) обеспечивают информационный обмен с маршрутизаторами, которые расположены в других автономных системах.

База данных Link-State Database отображает текущую структуру информационных связей в рассматриваемой области маршрутизации. Эти базы данных должны быть идентичными у всех маршрутизаторов, которые расположены в пределах одной области. Базы данных состоят из сообщений, которые называются Link – State Advertisement и формируются всеми активными маршрутизаторами данной области. Активным в данном случае считается маршрутизатор, который имеет хотя бы один подключенный канал в данной области.

Сообщения, в которых содержатся LSA, формируются при каждом изменении состояния канала и передаются всеми маршрутизаторами данной области методом затопления. Для формирования базы данных используются различные типы LSA:

- LSA типа 1 - router link advertisement;
- LSA типа 2 - network link advertisement;
- LSA типа 3, 4 - summary link advertisement;
- LSA типа 5 - external link advertisement;
- LSA типа 6 - multicast OSPF LSA;
- LSA типа 7 - AS external LSA for NSSA;
- LSA типа 8 - link LSA.

Сообщения типа 1 – router link advertisement (состояния каналов маршрутизатора) формируются каждым маршрутизатором для каждой области, в которой он имеет активные интерфейсы. Сообщения LSA типа 1 содержат объединенную информацию о состоянии каналов, которые имеет маршрутизатор в

данной области. Сообщения этого типа распространяются только в пределах одной области.

Сообщения LSA типа 2 – network link advertisement (состояние сети) формируется только в сетях, которые могут быть отнесены к классу broadcast (Ethernet) или NBMA (Non Broadcast Multi Access). В сообщении LSA типа 2 указываются идентификаторы всех маршрутизаторов, подключенных к данной сети. Формирование сообщений данного типа выполняется маршрутизатором, который называется Designated Router. Выбор этого маршрутизатора выполняется по специальному алгоритму среди всех маршрутизаторов, которые подключены к данной сети.

Сообщения LSA типа 3, 4 – summary link advertisement формируются Area Border Router – маршрутизаторами и направляются за пределы области, в которой они сформированы. Каждое сообщение данного типа содержит маршрут, который может быть использован для информационного обмена между различными областями в пределах одной автономной системы. В частности, LSA типа 3 описывают маршруты к сетям, LSA типа 4 описывают маршруты к AS Boundary Router – маршрутизаторам.

Сообщения LSA типа 5 – external link advertisement формируются AS Boundary Router – маршрутизаторами и содержат информацию о маршрутах, которые являются внешними по отношению к данной автономной системе. Сообщения данного типа распространяются по всем областям автономной системы за исключением отдельных специально сконфигурированных областей, которые называются stubareas.

Сообщения LSA типа 6 – Multicast OSPF LSA, специализированный LSA, который используют мультикаст OSPF приложения.

Сообщения LSA типа 7 Type – AS external LSA for NSSA это объявления о состоянии внешних каналов автономной системы в NSSA зоне. Оно может передаваться только в NSSA зоне. На границе зоны пограничный маршрутизатор преобразует type 7 LSA в type 5 LSA.

Сообщения LSA типа 8 – link LSA, анонсирует link-local адрес и префикс(ы) маршрутизатора всем маршрутизаторам разделяющим канал (link). Отправляется только если на канале присутствует более чем один маршрутизатор. Распространяются только в пределах канала (link).

Помимо установления партнерских отношений данный протокол используется для регулярного подтверждения наличия двустороннего обмена между маршрутизаторами. Для этого пакеты Hello периодически отправляются через все интерфейсы маршрутизатора. В пакете Hello маршрутизатор размещает IP адреса соседей, от которых он получил сообщения Hello. Двусторонний характер обмена заключается в том, что маршрутизатор должен обнаружить в принятом от партнера пакете Hello свой собственный идентификатор.

В broadcast и NBMA сетях данный протокол используется для выбора назначенного маршрутизатора. Процедуры, которые маршрутизатор выполняет в рамках протокола Hello, являются различными в сетях различного типа. В broadcast сетях маршрутизатор периодически заявляет о себе путем передачи пакетов адресованных в адрес типа multicast. В данном случае эти пакеты Hello содержат представления данного маршрутизатора по поводу кандидатуры назначенного маршрутизатора, а также, список маршрутизаторов, от которых были получены пакеты Hello в течение установленного интервала времени.

При разделении автономной системы на зоны, маршрутизаторам принадлежащим к одной зоне, не известна информация о детальной топологии других зон. Разделение на зоны позволяет:

- снизить нагрузку на ЦП маршрутизаторов за счёт уменьшения количества перерасчётов по алгоритму OSPF;
- уменьшить размер таблиц маршрутизации;
- уменьшить количество пакетов обновлений состояния канала.

Каждой зоне присваивается идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Однако идентификаторы зон не являются IP-адресами и могут совпадать с любым назначенным IP-адресом.

Существует несколько типов зон, приведенных далее.

1. Магистральная зона или backbone area (известная также как нулевая зона или зона 0.0.0.0) формирует ядро сети OSPF. Все остальные зоны соединены с ней, и межзональная маршрутизация происходит через маршрутизатор, соединенный с магистральной зоной. Магистральная зона ответственна за распространение маршрутизирующей информации между немагистральными зонами. Магистральная зона должна быть смежной с другими зонами, но она не обязательно должна быть физически смежной; соединение с магистральной зоной может быть установлено и с помощью виртуальных каналов.

2. Стандартная зона (standard area) – обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты.

3. Тупиковая зона (stub area) не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. Исключение из этого правила – ABR может быть и ASBR.

Totally stubby area не принимает информацию о внешних маршрутах для автономной системы и маршруты из других зон. Если маршрутизаторам необходимо передавать информацию за пределы зоны, то они используют маршрут по умолчанию.

Not-so-stubby area (NSSA) определяет дополнительный тип LSA – LSA type 7. В NSSA зоне может находиться ASBR. Сообщения об изменениях маршрутов могут быть вызваны следующими причинами:

- возраст маршрута достиг предельного значения (lsrefreshtime);
- изменилось состояние интерфейса;
- произошли изменения в маршрутизаторе сети;
- произошло изменение состояния одного из соседних маршрутизаторов;

- изменилось состояние одного из внутренних маршрутов (появление нового, исчезновение старого и т.д.);
- произошло изменение состояния межзонного маршрута;
- появление нового маршрутизатора, подключенного к сети;
- вариация виртуального маршрута одним из маршрутизаторов;
- возникли изменения одного из внешних маршрутов;
- маршрутизатор перестал быть пограничным для данной as (например, перезагрузился).

Маршрутная таблица OSPF содержит в себе:

- IP-адрес места назначения и маску;
- тип места назначения (сеть, граничный маршрутизатор и т.д.);
- тип функции (возможен набор маршрутизаторов для каждой из функций TOS);
- область (описывает область, связь с которой ведет к цели, возможно несколько записей данного типа, если области действия граничных маршрутизаторов перекрываются);
- тип пути (характеризует путь как внутренний, межобластной или внешний, ведущий к AS);
- цена маршрута до цели;
- очередной маршрутизатор, куда следует послать дейтограмму;
- объявляющий маршрутизатор (используется для межобластных обменов и для связей автономных систем друг с другом).

Преимущества OSPF приведены далее.

1. Для каждого адреса может быть несколько маршрутных таблиц, по одной на каждый вид IP-операции (TOS).
2. Каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения. Для каждой IP-операции может быть присвоена своя цена (коэффициент качества).
3. При существовании эквивалентных маршрутов OSFP распределяет поток равномерно по этим маршрутам.



4. Поддерживается адресация субсетей (разные маски для разных маршрутов).

5. При связи точка-точка не требуется IP-адрес для каждого из концов, что экономит адреса.

6. Применение мультикастинга вместо широковещательных сообщений снижает загрузку не вовлеченных сегментов.

К недостаткам OSPF относят:

- трудности в получении информации о предпочтительности каналов для узлов, поддерживающих другие протоколы, или со статической маршрутизацией;

- OSPF является лишь внутренним протоколом.

#### **4.2 Рабочее задание**

1. Собрать схему сети в соответствии с рисунком 3.1 (лабораторная работа №3) в программе Packet Tracer, настроить компьютеры и сервер и задать им IP адреса и маски в соответствии с таблицей 3.1.

2. Сконфигурировать маршрутизаторы. В настройках включить нужные интерфейсы (по схеме), задать IP адрес, маску для каждого из интерфейсов.

3. Настроить динамическую маршрутизацию в настройках маршрутизаторов на основе протокола OSPF в соответствии с вариантом указанным в таблице 3.1.

4. Использовать *ping*-запросы из командной строки для проверки связи.

5. Использовать трассировку маршрута (*traceroute*, *tracert*) для проверки пути следования пакетов.

Перед настройкой протокола OSPF на маршрутизаторах необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую частоту главного маршрутизатора.

Настройка базового протокола OSPF не является сложной задачей и состоит только из двух шагов. Первый шаг - включение процесса маршрутизации OSPF. Второй шаг - определение сетей, которые должны быть объявлены:

- Router(config)#router ospf [id процесса];

- Router(config-router)#network [адрес сети] [групповая маска] area [id области].

Первая команда используется для включения протокола OSPF на маршрутизаторе. Эту команду необходимо ввести в глобальном режиме настройки.

Также для включения протокола OSPF необходимо указать идентификатор процесса, который выбирается администратором, он может представлять собой любое число в диапазоне от 1 до 65535. Идентификатор процесса имеет только локальное значение и необязательно должен совпадать с идентификатором других маршрутизаторов OSPF.

Команда `network` имеет такую же функцию, как в других протоколах маршрутизации IGP. Этой командой определяются интерфейсы, которые могут посылать и принимать пакеты OSPF. Данная инструкция определяет сети, включаемые в обновления маршрутизации OSPF.

В команде OSPF `network` используется сочетание сетевого адреса и групповой маски. Групповая маска (Wildcard mask, перевернутая маска, или как ее еще называют – инверсная) показывает, какая часть (сколько бит) IP адреса могут меняться. Она может применяться при объявлении сетей в протоколах маршрутизации, таких как IGRP, EIGRP, OSPF, в списках доступа. Принцип работы маски тоже такой же, как у обычной маской, за исключением того, что вместо единиц ставятся нули, а вместо нулей единицы. Для расчёта групповой маски подсети нужно вычесть маску подсети из 255.255.255.255. Например, для маски 255.255.255.252 инверсной будет маска 0.0.0.3.

Сетевой адрес, наряду с групповой маской, указывает адрес интерфейса, или диапазон адресов, который будет включен для OSPF.

Идентификатор области определяет область OSPF, которой принадлежит сеть. Даже если никакие области не указаны, должна присутствовать какая-либо область 0. В окружении OSPF с одной областью область всегда имеет идентификатор 0. По завершении настройки необходимо сравнить рабочую конфигурацию с точной схемой топологии для сверки номеров сетей и IP-адресов интерфейсов для обнаружения возможных механических ошибок, допущенных при вводе IP-адресов. Пример настройки протокола OSPF показан на рисунке 4.1.

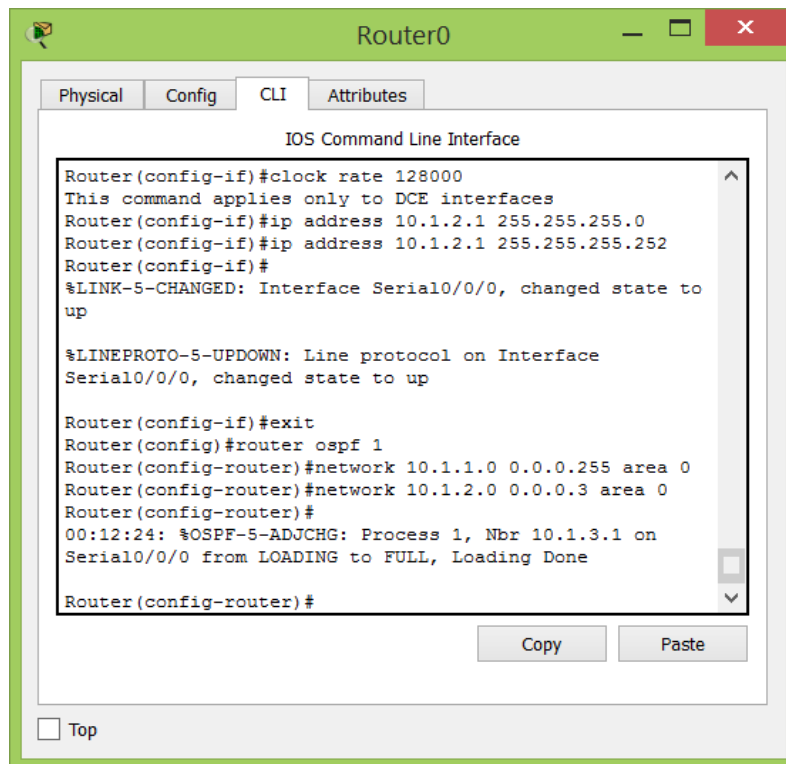


Рисунок 4.1 – Настройка OSPF на маршрутизаторе

Проверить функционирование протокола OSPF в сети можно несколькими способами.

Если конфигурация верна, то для проверки работоспособности маршрутизации можно отправить эхо-запросы командой ping на устройства в удаленных сетях. Успешное выполнение команды ping будет свидетельством работоспособности маршрутизации.

Выполните команды для проверки IP-маршрутизации show ip protocols и show ip route в приглашении командной строки. Команда show ip protocols позволяет убедиться в верности настройки маршрутизации OSPF, использовании соответствующих интерфейсов для отправки и приема обновлений OSPF, а также правильном составе сетей в оповещениях. Команда show ip route выводит таблицу маршрутизации, по которой можно проверить присутствие маршрутов, полученных соседними маршрутизаторами (рисунок 4.2).

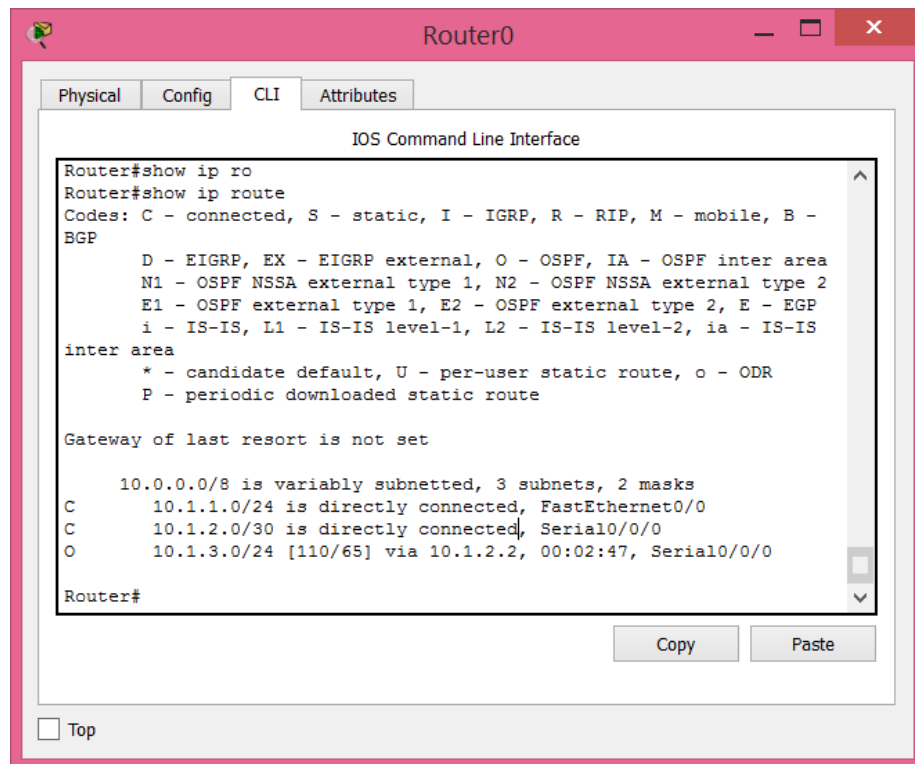


Рисунок 4.2 – Проверка работы OSPF на маршрутизаторе

### 4.3 Контрольные вопросы

1. Дайте понятие протокола маршрутизации OSPF.
2. Назовите основные преимущества протокола OSPF.
3. О каких изменениях в состоянии каналов маршрутизаторы обмениваются извещениями?
4. Дайте понятие выделенного (designated) маршрутизатора.
5. Дайте понятие распределения нагрузки между параллельными каналами.
6. В каких информационных системах целесообразно использование процедуры установления подлинности?
7. Перечислите способы организации обмена информацией о маршрутах.
8. Какие параметры учитывает метрика маршрута в протоколе OSPF?
9. Дайте понятие автономной системы (Autonomous System).
10. Какие маршрутизаторы называются соседними?
11. Какие маршрутизаторы называются смежными?
12. Дайте понятие объявления о состоянии канала (Link State Advertisement).
13. Как называется процесс распространения LSA в пределах автономной системы?

14. Дайте понятие выделенного маршрутизатора (DR) и запасного выделенного маршрутизатора (BDR).
15. С какой целью в сетях с множественным доступом выбираются выделенный маршрутизатор (DR) и запасной выделенный маршрутизатор (BDR)?
16. Назовите и опишите типы маршрутизаторов OSPF?
17. Какие типы LSA используются для формирования базы данных?
18. Какие преимущества дает разделение автономной системы на зоны?
19. Какие типов зон существуют в автономных системах?
20. Какие причины вызывают сообщения об изменениях маршрутов?
21. Какие данные содержит в себе маршрутная таблица OSPF?
22. Перечислите преимущества и недостатки протокола OSPF.

## 5 Лабораторная работа №5. Протокол BGP

*Цель работы.* Научиться настраивать динамическую маршрутизацию на основе протокола BGP. Выполнить задание в соответствии с вариантом.

### 5.1 Основные теоретические положения

Протокол маршрутизации BGP (Border Gateway Protocol) является динамическим, междоменным, распределенным, одноуровневым, многопутевым и управляется маршрутизатором. Он разработан с целью устранения недостатков протокола EGP (Exterior Gateway Protocol), считается его приемником и уже скоро полностью вытеснит его с просторов Интернета.

Изначально маршрутизаторы, использующие протокол BGP, обмениваются полными таблицами маршрутизации. Далее, по мере их изменения, рассылаются обновления – последовательные и отражающие только изменения. В таблицах протокола BGP возможно несколько маршрутов к одному месту назначения, но другим маршрутизаторам сообщаются только оптимальные. Естественно, для выбора таких маршрутов необходима какая-то метрика. В BGP она предусмотрена и представляет собой просто число, которое назначено администратором сети. При этом администратор должен сам учитывать такие факторы, как число переходов, скорость канала и его стабильность.

BGP, в отличие от других протоколов динамической маршрутизации, предназначен для обмена информацией о маршрутах не между отдельными маршрутизаторами, а между целыми автономными системами, и поэтому, помимо информации о маршрутах в сети, переносит также информацию о маршрутах на автономные системы. BGP не использует технические метрики, а осуществляет выбор наилучшего маршрута исходя из правил, принятых в сети. Обновления таблиц BGP рассылаются при помощи протокола TCP. Они содержат информацию о том, какие домены достижимы с конкретного узла.

Существует способ выявить сбои в работе узлов и маршрутизаторов посредством сообщений “еще жив” (keep-alive), которые генерируются примерно каждые 30 секунд. Также BGP называют протоколом, поддерживающим

бесклассовую междоменную маршрутизацию (Classless Interdomain Routing, CIDR). Это означает, что в таблицах маршрутизации используются 32-разрядные IP-адреса и маски подсетей, значения которых при выборе маршрутов трактуются как “сплошные”. Протокол BGP использует суммирование маршрутов для уменьшения таблиц маршрутизации.

Сейчас используется новая версия протокола BGP – BGP-4. Помимо других возможностей, в ней можно применять маски подсетей произвольной длины. Протокол BGP используется для передачи информации о внутренних маршрутах между автономными системами. Протокол BGP может быть использован для определения различных типов маршрутов:

- Inter-autonomous system routing маршруты которые соединяют данную автономную систему с одной или несколькими другими автономными системами;

- Intra-autonomous system routing – протокол может быть использован для определения маршрута внутри автономной системы, в том случае, когда несколько маршрутизаторов участвуют в процессе определения маршрута BGP;

- Pass-through autonomous system – протокол может быть использован для определения маршрутов, которые проходят через автономную систему, которая не участвует в процессе BGP.

Пара BGP-соседей устанавливает между собой соединение по протоколу TCP, порт 179. Соседи, принадлежащие разным АС, должны быть доступны друг другу непосредственно; для соседей из одной АС такого ограничения нет, поскольку протокол внутренней маршрутизации обеспечит наличие всех необходимых маршрутов между узлами одной автономной системы.

Поток информации, которым обмениваются BGP-соседи по протоколу TCP, состоит из последовательности BGP-сообщений. Максимальная длина сообщения 4096 октетов, минимальная – 19. Имеется 4 типа сообщений.

1. OPEN – посылается после установления TCP-соединения. Ответом на OPEN является сообщение KEEPALIVE, если вторая сторона согласна стать BGP-соседом; иначе посылается сообщение NOTIFICATION с кодом, поясняющим причину отказа, и соединение разрывается.

2. KEEPALIVE – сообщение предназначено для подтверждения согласия установить соседские отношения, а также для мониторинга активности открытого соединения: для этого BGP-соседи обмениваются KEEPALIVE-сообщениями через определенные интервалы времени.

3. UPDATE – сообщение предназначено для анонсирования и отзыва маршрутов. После установления соединения с помощью сообщений UPDATE пересылаются все маршруты, которые маршрутизатор хочет объявить соседу (full update), после чего пересылаются только данные о добавленных или удаленных маршрутах по мере их появления (partial update).

4. NOTIFICATION – сообщение этого типа используется для информирования соседа о причине закрытия соединения. После отправления этого сообщения BGP-соединение закрывается. Вся маршрутная информация хранится в специальной базе данных RIB (routing information base). Маршрутная база данных BGP состоит из трех частей.

1. ADJ-RIBS-IN: Запоминает маршрутную информацию, которая получена из update-сообщений. Это список маршрутов, из которого можно выбирать. (policy information base – PIB).

2. LOC-RIB: Содержит локальную маршрутную информацию, которую BGP-маршрутизатор отобрал, руководствуясь маршрутной политикой, из ADJ-RIBS-IN.

3. ADJ-RIBS-OUT: Содержит информацию, которую локальный BGP-маршрутизатор отобрал для рассылки соседям с помощью UPDATE-сообщений.

Так как разные BGP-партнеры могут иметь разную политику маршрутизации, возможны колебания маршрутов. Для исключения этого необходимо выполнять следующее правило: если используемый маршрут объявлен не рабочим (в процессе корректировки получено сообщение с соответствующим атрибутом), до переключения на новый маршрут необходимо ретранслировать сообщение о недоступности старого всем соседним узлам.

Протокол BGP позволяет реализовать маршрутную политику, определяемую администратором AS. Политика отражается в конфигурационных файлах BGP. Маршрутная политика это не часть протокола, она определяет решения, когда место



назначения достижимо несколькими путями, политика отражает соображения безопасности, экономические интересы и пр. Количество сетей в пределах одной AS не лимитировано. Один маршрутизатор на много сетей позволяет минимизировать таблицу маршрутов.

BGP использует три таймера:

- connectretry (сбрасывается при инициализации и коррекции; 120 сек);
- holdtime (запускается при получении команд Update или Keepalive; 90сек);
- keepalive (запускается при посылке сообщения Keepalive; 30сек).

BGP отличается от RIP и OSPF тем, что использует TCP в качестве транспортного протокола. Две системы, использующие BGP, связываются друг с другом и пересылают посредством TCP полные таблицы маршрутизации. В дальнейшем обмен идет только в случае каких-то изменений. ЭВМ, использующая BGP, не обязательно является маршрутизатором. Сообщения обрабатываются только после того, как они полностью получены.

В BGP в качестве метрики используется число шагов до цели, и время распространения маршрутной информации велико, у разных маршрутизаторов может быть прописана разная маршрутная политика. Допустим, какой-то маршрутизатор на основании анализа ситуации принял решение об изменении маршрута с варианта 1 на вариант 2 и сразу реализовал это решение. Эти данные дойдут до соседей спустя несколько минут. Они на основе новых данных могут также принять определенные решения, уведомив об этом своих соседей. Может так получиться, что после того как наш маршрутизатор получит данные от своих соседей, метрика для варианта маршрута 1 окажется меньше метрики маршрута 2 и придется вернуться к пути, от которого он только что отказался. Чтобы такого не происходило, нужно сначала уведомлять соседние маршрутизаторы о принятом решении, но на новый маршрут не переключаться, пока от соседей не придут данные об их намерениях. (Для этого нужно задать соответствующие таймерные переменные). Может так случиться, что переключение на новый маршрут придется отменить, так как это ведет к осцилляции маршрута. Кто-то может сказать, что ему все равно, по какому маршруту доставляется пакет (по пути 1 или 2), и пусть себе

маршруты осциллируют. Эта точка зрения ошибочна, так как при осцилляции маршрутов их установление происходит в маршрутизаторах не одновременно и заметное число пакетов не будет доставлено адресату вообще.

Важным свойством протокола является возможность декларации резервного (backup) маршрута. Так, если основной маршрут автономной системы стал недоступен, маршрутизатор переключит поток на этот резервный канал. При этом пользователи сети не должны ожидать момента, когда администратор сети вернется из отпуска, проснется или вернется из кафетерия и сам внесет необходимые коррективы.

## **5.2 Рабочее задание**

Необходимо настроить динамическую маршрутизацию на основе протокола BGP в соответствии с вариантом, указанным в таблице 3.2 лабораторной работы №3.

При правильной настройке маршрутизации все компьютеры должны иметь возможность успешно отправлять icmp запросы друг другу.

Перед настройкой протокола BGP на маршрутизаторах необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую частоту главного маршрутизатора.

Когда Интернет-провайдер размещает граничный маршрутизатор на объекте клиента, в качестве маршрута по умолчанию обычно настраивается статический маршрут к Интернет-провайдеру. Однако иногда Интернет-провайдеру требуется включить маршрутизатор в свою автономную систему и сделать его участником BGP. В этих случаях необходимо настроить маршрутизатор в помещении клиента, введя необходимые команды для активации BGP.

Первый шаг в активации BGP на маршрутизаторе состоит в настройке номера автономной системы [7]. Это делается с помощью следующей команды:

```
router bgp [номер AS].
```

Следующий шаг – идентификация маршрутизатора провайдера, который будет выступать соседним узлом BGP для обмена информацией с маршрутизатором

в помещении клиента (CPE). Соседний маршрутизатор идентифицируется следующей командой:

```
neighbor [IP-адрес] remote-as [номер AS].
```

Клиентам Интернет-провайдера, имеющим собственные зарегистрированные блоки IP-адресов, может быть необходима возможность объявления маршрутов к своим внутренним сетям в Интернете. Объявление внутренних маршрутов посредством BGP осуществляется по команде "network". Формат команды "network":

```
network [адрес сети]
```

На рисунках 5.1 и 5.2 показана настройка двух соседних маршрутизаторов сети, находящихся в разных автономных системах.

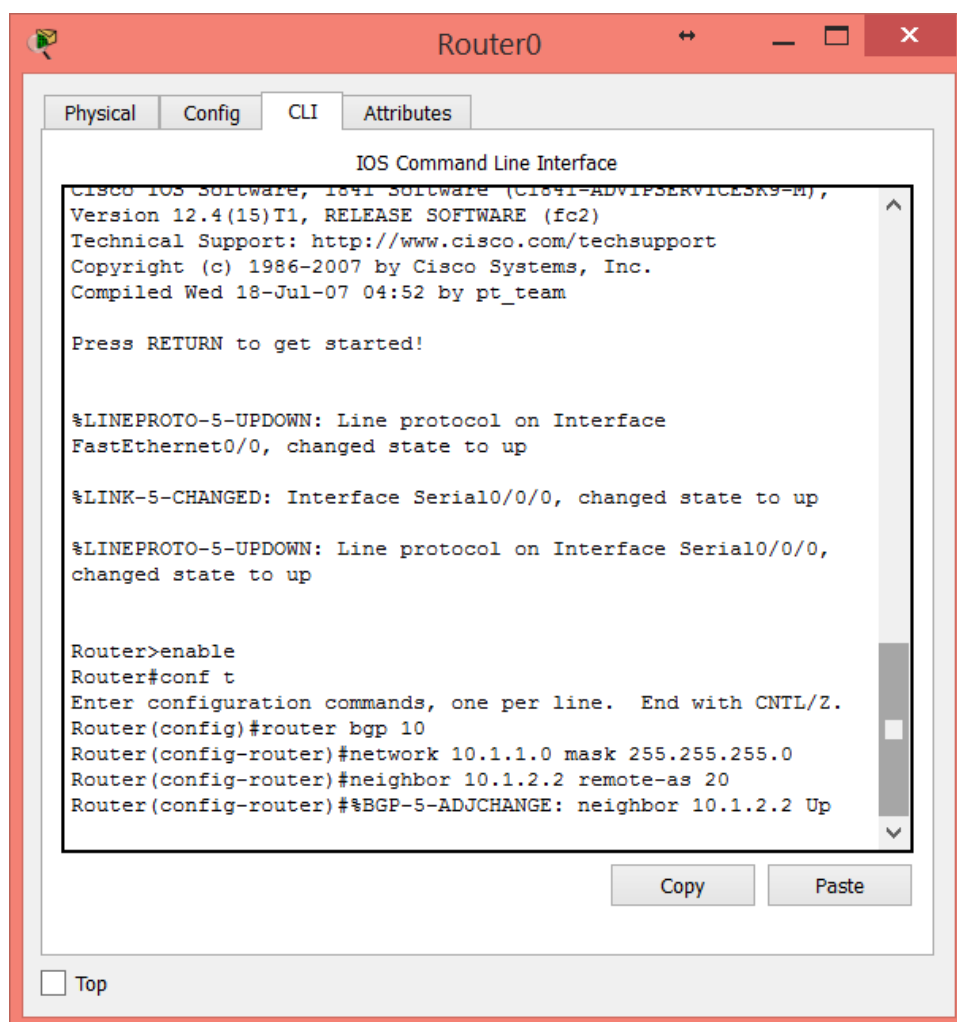


Рисунок 5.1 – Настройка маршрутизатора Router0

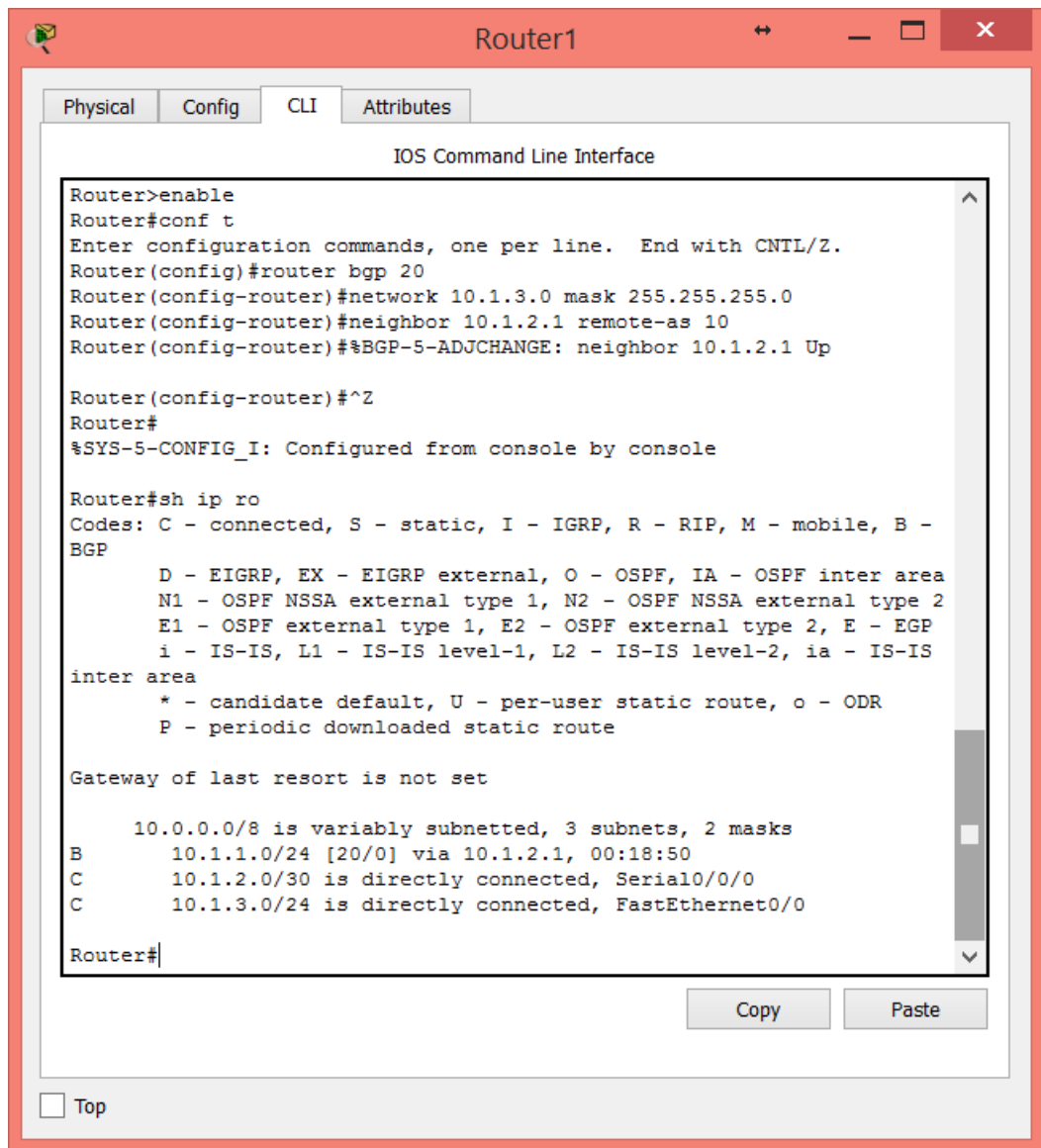


Рисунок 5.2 – Настройка маршрутизатора Router1

После установки оборудования в помещениях клиента и настройки протоколов маршрутизации клиент получает работающую локальную сеть и подключение к Интернету. Клиент становится полноправным участником других сервисов, предлагаемых провайдером.

Для BGP обычно используются зарегистрированные IP-адреса, которые могут использоваться в маршрутизации и однозначно идентифицируют организацию. В очень крупных организациях для процессов BGP могут применяться частные адреса, как показано на рисунке. В Интернете запрещается применять BGP для объявления адресов частных сетей.

### **5.3 Контрольные вопросы**

1. Дайте понятие протокола маршрутизации BGP.
2. Назовите основные особенности протокола BGP.
3. Для определения каких типов маршрутов может быть использован протокол BGP?
4. Какие типы сообщений содержит поток информации, которым обмениваются BGP-соседи по протоколу TCP?
5. Какие таймеры использует BGP?
6. В чем заключается отличие BGP от RIP и OSPF?
7. Опишите важное свойство протокола BGP – возможность декларации резервного (backup) маршрута.

## **6 Лабораторная работа №6. Настройка интерфейсов IPv4 и IPv6**

### **6.1 Основные теоретические положения**

Протокол IPv6 разработан как преемник протокола IPv4. В протоколе IPv6 больше 128-битного адресного пространства, что достаточно для 340 ундециллионов адресов. (Это число 340, за которым следует 36 нулей.) Однако IPv6 – не просто большие адреса. Когда специалисты IETF начали разработку преемника IPv4, они использовали эту возможность для устранения ограничений протокола IPv4 и внесения дополнительных улучшений. Среди таких улучшений – протокол управляющих сообщений версии 6 (ICMPv6), который включает в себя разрешение адресов и автонастройку адресов, что отсутствовало в протоколе ICMP для IPv4 (ICMPv4).

Сокращение адресного пространства протокола IPv4 – основной стимулирующий фактор для перехода к использованию IPv6. По мере того как Африка, Азия и другие регионы планеты всё больше нуждаются в подключении к сети Интернет, остается всё меньше IPv4-адресов для поддержки таких темпов развития. 31 января 2011 г. Администрация адресного пространства Интернет IANA

назначила последние 2 блока IPv4-адресов /8 региональным интернет-регистраторам (RIR).

Теоретическое максимальное количество IPv4-адресов – 4,3 миллиарда. Частные адреса RFC 1918 в сочетании с преобразованием сетевых адресов (NAT) служат для замедления истощения адресного пространства IPv4. Преобразование сетевых адресов (NAT) имеет ограничения, которые препятствуют одноранговой связи.

Современная сеть Интернет значительно отличается от Интернета последних десятилетий. Сегодня это не просто электронная почта, веб-страницы и передача файлов между компьютерами. Интернет развивается и становится неотъемлемой частью нашей жизни. Скоро можно будет получить доступ к Интернету не только через компьютеры, планшеты и смартфоны. В будущем Интернет станет неотделим от многих устройств и технического оборудования, в том числе автомобилей и биомедицинских аппаратов, домашней техники и экосистемы.

В связи с распространением Интернета ограниченным адресным пространством IPv4, проблемами с преобразованием сетевых адресов и проникновением Интернета в нашу жизнь пришло время для перехода на протокол IPv6.

Точно неизвестно, когда мы перейдем на протокол IPv6. В ближайшем будущем протоколы IPv4 и IPv6 будут существовать совместно. Полный переход может занять многие годы. Специалисты IETF создали различные протоколы и инструменты, которые позволяют сетевым администраторам постепенно переводить свои сети на протокол IPv6. Методы перехода можно разделить на 3 категории:

- Двойной стек: двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одной сети. Устройства с двойным стекком одновременно работают с протокольными стеками IPv4 и IPv6.

- Туннелирование: это способ транспортировки IPv6-пакетов через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных.

- Преобразование: преобразование сетевых адресов 64 (NAT64) позволяет устройствам под управлением IPv6 обмениваться данными с устройствами под

управлением IPv4 с помощью метода преобразования, похожего на метод преобразования из NAT для IPv4. IPv6-пакет преобразовывается в пакет IPv4-пакет и наоборот.

Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представлены одной шестнадцатеричной цифрой, причём общее количество шестнадцатеричных значений равно 32. IPv6-адреса не чувствительны к регистру, их можно записывать как строчными, так и прописными буквами.

В предпочтительном формате IPv6-адрес записан с помощью 32 шестнадцатеричных цифр. Тем не менее, это не самый оптимальный способ представления IPv6-адреса. Существуют два правила, которые помогут сократить количество цифр, необходимых для представления IPv6-адреса.

Первое правило для сокращения записи IPv6-адресов – пропуск всех ведущих 0 (нулей) в шестнадцатеричной записи. Например:

- 01AB можно представить как 1AB
- 09F0 можно представить как 9F0
- 0A00 можно представить как A00
- 00AB можно представить как AB

Это правило применяется только к ведущим нулям, а НЕ к последующим, иначе адрес будет записан неясно. Например, шестнадцатеричное число «ABC» может быть представлено как «0ABC» или «ABC0».

Второе правило для сокращения записи адресов IPv6 заключается в том, что двойное двоеточие (::) может заменить любую единую, смежную строку одного или нескольких 16-битных сегментов (хекстетов), состоящих из нулей.

Двойное двоеточие (::) может использоваться в адресе только один раз, в противном случае в результате может возникнуть несколько адресов. Сочетание этого правила с методом пропуска нулей помогает значительно сократить запись IPv6-адреса. Это называется сжатым форматом.

Существует три типа IPv6-адресов.

- **Индивидуальный:** служит для определения интерфейса на устройстве под управлением протокола IPv6. Как показано на рисунке, IPv6-адрес источника должен быть индивидуальным.

- **Групповой:** используется для отправки IPv6-пакетов по нескольким адресам назначения.

- **Произвольный:** любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к ближайшему устройству с этим адресом.

В отличие от протокола IPv4, IPv6 не использует адрес широковещательной рассылки. Однако есть групповой IPv6-адрес для всех узлов, который даёт аналогичный результат.

Префикс, или сетевая часть адреса IPv4, может быть обозначен маской подсети в десятичном формате с разделительными точками или длиной префикса (запись с наклонной чертой). Например, IP-адрес 192.168.1.10 с маской подсети в десятичном формате с разделительными точками 255.255.255.0 эквивалентен записи 192.168.1.10/24.

Протокол IPv6 использует длину префикса для обозначения части префикса адреса. IPv6 не использует для маски подсети десятичное представление с разделительными точками. Длина префикса обозначает сетевую часть IPv6-адреса с помощью адреса или длины IPv6-префикса.

Диапазон длины префикса может составлять от 0 до 128. Традиционная длина IPv6-префикса для локальных и других типов сетей – /64. Это означает, что длина префикса, или сетевая часть адреса, составляет 64 бита, а оставшиеся 64 бита остаются для идентификатора интерфейса (узловой части) адреса.

Индивидуальный адрес служит для определения интерфейса устройства под управлением протокола IPv6. Пакет, который отправляется на индивидуальный адрес, будет получен интерфейсом, присвоенным для этого адреса. Как и в случае с протоколом IPv4, IPv6-адрес должен быть индивидуальным. IPv6-адрес назначения может быть как индивидуальным, так и групповым.

Существует шесть типов индивидуальных IPv6-адресов:



### 1) Глобальный индивидуальный адрес

Глобальный индивидуальный адрес мало чем отличается от публичного IPv4-адреса. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. В динамическом назначении IPv6-адреса устройством имеются некоторые важные отличия по сравнению с динамическим назначением IPv4-адреса.

### 2) Локальный адрес канала

Локальные адреса канала используются для обмена данными с другими устройствами по одному локальному каналу. В протоколе IPv6 термин «канал» означает подсеть. Локальные адреса каналов ограничены одним каналом. Они должны быть уникальны только в рамках этого канала, поскольку вне канала к ним нельзя проложить маршрут. Другими словами, маршрутизаторы не смогут пересылать пакеты, имея локальный адрес канала источника или назначения.

### 3) Логический интерфейс loopback

Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, который выглядит как ::1/128 или просто ::1 в сжатом формате.

### 4) Неопределённый адрес

Неопределённый адрес состоит из нулей и в сжатом формате представлен как ::/128 или просто ::. Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес или когда источник пакета не относится к месту назначения.

### 5) Уникальный локальный адрес

Уникальные локальные IPv6-адреса имеют некоторые общие особенности с частными адресами RFC 1918 для IPv4, но при этом между ними имеются и значительные различия. Уникальные локальные адреса используются для локальной

адресации в пределах узла или между ограниченным количеством узлов. Эти адреса не следует маршрутизировать в глобальном протоколе IPv6. Уникальные локальные адреса находятся в диапазоне от FC00::/7 до FDFE::/7.

### б) Встроенный IPv4

Последними из рассматриваемых типов индивидуальных адресов являются встроенные IPv4-адреса. Использование этих адресов способствует переходу с протокола IPv4 на IPv6.

## 6.2 Рабочее задание

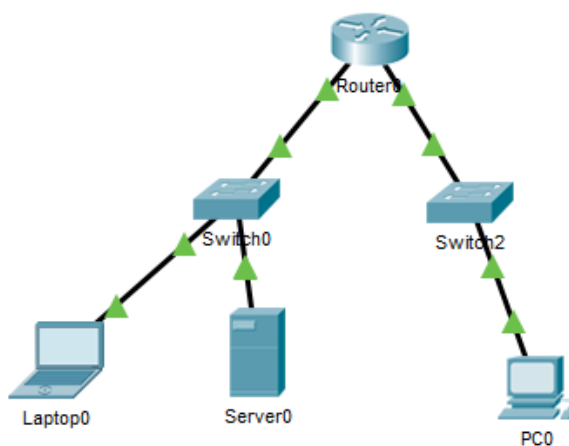


Рисунок 6.1 – Топология сети

Соберите схему сети в соответствии с рисунком 6.1.

Таблица 6.1 – Таблица адресации, используемая в примере настройки

Устройство	Интерфейс	IPv6-адрес/префикс	Шлюз по умолчанию
Router0	G0/0	2001:DB8:1:1::1/64	Недоступно
	G0/1	2001:DB8:1:2::1/64	Недоступно
	Локальный адрес канала	FE80::1	Недоступно
Laptop0	Сетевой адаптер	2001:DB8:1:1::3/64	FE80::1
Server0	Сетевой адаптер	2001:DB8:1:1::4/64	FE80::1
PC0	Сетевой адаптер	2001:DB8:1:2::3/64	FE80::1

Настройте маршрутизатор Router0:

1) Включите пересылку пакетов IPv6 на маршрутизаторе. Для этого введите команду глобальной настройки маршрутизации одноадресной передачи IPv6. Данная команда нужна для включения пересылки пакетов IPv6 на маршрутизаторе [8].

```
R1(config)# ipv6 unicast-routing
```

2) В соответствии с таблицей вариантов настройте интерфейс GigabitEthernet0/0 (рисунок 6.2)

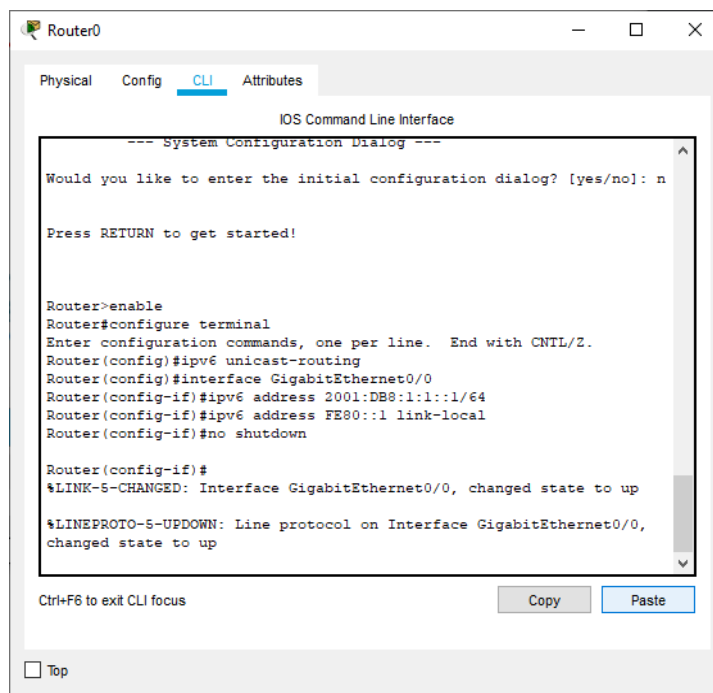


Рисунок 6.2 – Настройка маршрутизатора

Аналогично настройте второй интерфейс GigabitEthernet.

Настройте адресацию IPv6 на сервере Server0. Для этого на вкладке Desktop (Рабочий стол) выберите IP Configuration (Настройка IP) и установите для адреса IPv6 соответствующее значение. Установите для шлюза IPv6 локальный адрес канала.

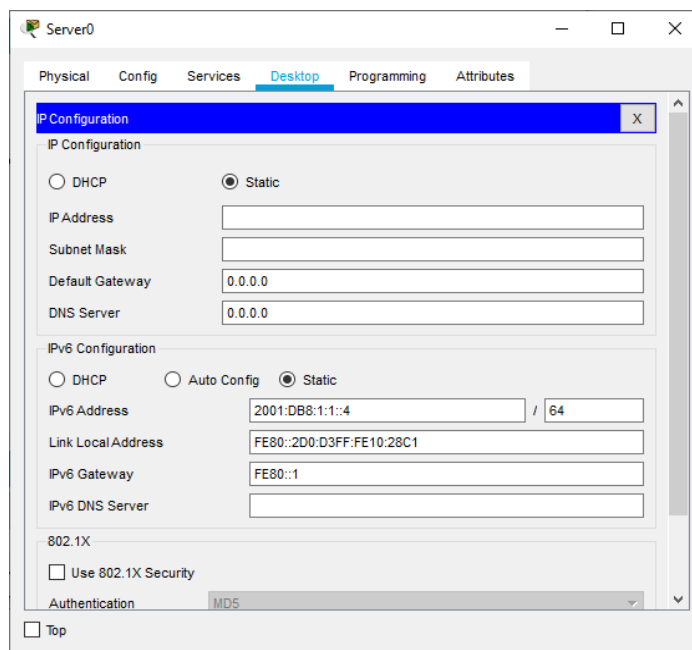


Рисунок 6.3 – Настройка адресации сервера

Настройте адресацию IPv6 на клиентских узлах Laptop0 и PC0. Для этого выберите IP Configuration на вкладке Desktop, установите значение адреса IPv6 и локального адреса канала для шлюза IPv6 в соответствии с таблицей вариантов.

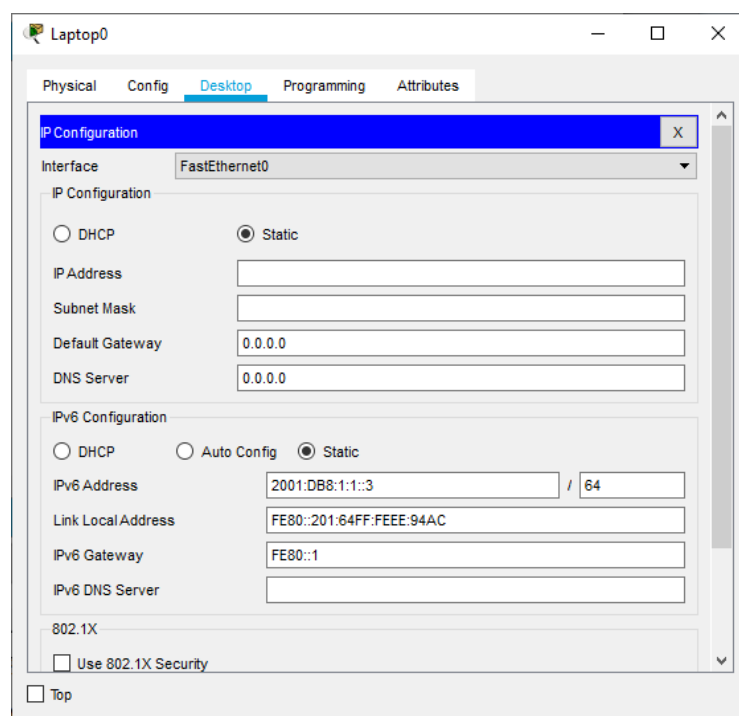


Рисунок 6.4 – Настройка клиентских устройств

Вариант	Router0	Laptop0	Server0	PC0
1	интерфейс G0/0 2001:DB8:C0DE:12::1/64  интерфейс G0/1 2001:DB8:C0DE:13::1/64  Локальный адрес канала FE80::2	2001:DB8:C0DE:12::A/ 64	2001:DB8:C0DE:12::B/ 64	2001:DB8:C0DE:13::A/ 64
2	интерфейс G0/0 2001:DB8:12:12::1/64  интерфейс G0/1 2001:DB8:12:13::1/64  Локальный адрес канала FE80::2	2001:DB8:12:12::A/64	2001:DB8:12:12::B/64	2001:DB8:12:13::A/64
3	интерфейс G0/0 2001:DB8:C0DE:11::1/64  интерфейс G0/1 2001:DB8:C0DE:12::1/64  Локальный адрес канала FE80::2	2001:DB8:C0DE:11::A/ 64	2001:DB8:C0DE:11::B/ 64	2001:DB8:C0DE:12::A/ 64
4	интерфейс G0/0 2001:DB8:C0DE:12::1/64  интерфейс G0/1 2001:DB8:C0DE:13::1/64  Локальный адрес канала FE80::2	2001:DB8:C0DE:12::3/ 64	2001:DB8:C0DE:12::4/ 64	2001:DB8:C0DE:13::3/ 64
5	интерфейс G0/0 2001:DB8:1:1::1/64  интерфейс G0/1 2001:DB8:1:2::1/64  Локальный адрес канала FE80::2	2001:DB8:1:1::A/64	2001:DB8:1:1::B/64	2001:DB8:1:2::A/64
6	интерфейс G0/0 2001:DB8:C0DE:12::1/64  интерфейс G0/1 2001:DB8:C0DE:13::1/64  Локальный адрес канала FE80::2	2001:DB8:C0DE:12::3/ 64	2001:DB8:C0DE:12::4/ 64	2001:DB8:C0DE:13::3/ 64
7	интерфейс G0/0 2001:DB8:1:1::1/64  интерфейс G0/1 2001:DB8:1:2::1/64  Локальный адрес канала FE80::2	2001:DB8:1:1::A/64	2001:DB8:1:1::B/64	2001:DB8:1:2::A/64

8	интерфейс G0/0 2001:DB8:C0DE:12::1/64  интерфейс G0/1 2001:DB8:C0DE:13::1/64  Локальный адрес канала FE80::2	2001:DB8:C0DE:12::3/ 64	2001:DB8:C0DE:12::4/ 64	2001:DB8:C0DE:13::3/ 64
9	интерфейс G0/0 2001:DB8:1:1::1/64  интерфейс G0/1 2001:DB8:1:2::1/64  Локальный адрес канала FE80::2	2001:DB8:1:1::A/64	2001:DB8:1:1::B/64	2001:DB8:1:2::A/64
10	интерфейс G0/0 2001:DB8:C0DE:12::1/64  интерфейс G0/1 2001:DB8:C0DE:13::1/64  Локальный адрес канала FE80::2	2001:DB8:C0DE:12::3/ 64	2001:DB8:C0DE:12::4/ 64	2001:DB8:C0DE:13::3/ 64

## **7 Лабораторная работа №7. Проектирование беспроводной сети, выбор оптимальных мест для базовых станций, настройка оборудования.**

### **7.1 Основные теоретические положения**

Для выбора конфигурации беспроводной сети в первую очередь необходимо произвести замеры уровня сигнала и с учетом уже существующей сетевой инфраструктуры составить проект будущей сети.

При составлении проекта можно задействовать имеющийся проводной сегмент с добавлением беспроводной части, либо исключительно беспроводную сеть, от этого зависит выбор оборудования и его физическое расположение.

Радиус покрытия беспроводной сети достаточно небольшой (около 25м) и значительно зависит не только от выбора используемого оборудования, но и от конфигурации вашего офисного помещения. В помещении площадью до 150 м<sup>2</sup> разделенном перегородками или гипсокартонными стенами, как правило, достаточно для покрытия одной точки доступа.

В случае если в офисе основательные стены и множество габаритной мебели, то необходимо использование дополнительных точек доступа, работающих в режиме «Repeater» (Повторитель), расположенных в местах, где возможно затухание сигнала от базовой точки доступа.

Если в офисе уже существует проводная сеть с выходом в Интернет и к ней подключены серверы, рабочие станции, сетевые принтеры и т.д., рекомендуется сохранить имеющуюся инфраструктуру, и только дополнить ее беспроводными возможностями.

Устанавливается одна или несколько точек доступа настроенных в режиме «Access Point», используемых для объединения всех беспроводных устройств в качестве прозрачного моста между беспроводной и проводной сегментами сети, и каждая точка должна подключаться к порту проводного коммутатора/маршрутизатора.

При использовании в офисе нескольких не связанных между собой сегментов проводной сети, расположенных в разных комнатах или соседних зданиях, их возможно связать с помощью дополнительных точек доступа работающих в режиме «Wireless/Multiple Bridge».

Для улучшения качества сигнала возможно использование внешних дополнительных антенн: узконаправленной для соединения в зоне прямой видимости, либо когда необходимо чтобы сигнал распространялся в одном направлении и всенаправленной, когда необходимо увеличить зону покрытия в помещении.

При создании беспроводной сети с нуля, целесообразно использование беспроводного маршрутизатора, поддерживающего различные типы входящего соединения. Выбор маршрутизатора зависит от того, с использованием какой технологии офис подключен к сети Интернет. Этот вариант позволит полностью избавиться от кабельных соединений, кроме входящего Интернет-канала по телефонной ADSL линии или Ethernet кабелю. Используя беспроводные принт-серверы можно расположить принтеры в офисе как удобно, не привязываясь к расположению компьютеров.

Отдельная тема при проектировании беспроводных сетей – организация Hot-Spot (Хот-Спот) точки доступа. Хот-спотами называются публичные зоны беспроводного доступа, эксплуатирующиеся в коммерческом режиме. К примеру, это может быть гостиничный или ресторанный бизнес. Услуга доступа к Интернет с применением Хот-спот может быть как платной для посетителей, так и предоставляться в виде дополнительной услуги или сервиса посетителям. С технической точки зрения создание хот-спотов не представляет особой сложности. Для этого необходимо подвести каналы связи и организовать точку доступа (access point), выполняющую функции концентратора беспроводной сети (Access Point).

Хот-споты также могут исполнять одновременно и роль точек доступа корпоративной сети, но оборудование должно поддерживать такие режимы.

*Многофункциональная точка доступа (Access Point, AP)* может быть настроена для работы в режиме точки доступа (AP), *беспроводного клиента (Wireless Client)*, *моста (Wireless Distribution System или WDS)*, WDS с точкой доступа или *беспроводного повторителя (Repeater)*. Также многие точки доступа поддерживают *WLAN Stations centu (WLAN STA)*, функцию удобную для развертывания сетей, подобных Хот-Спотам.

Для корпоративных беспроводных сетей также существует технология «*виртуальных точек доступа*». Эта идея вызвана потребностью представить множественные подсети различным группам пользователей. Например, на единственной точке доступа беспроводная сеть «Маркетинг» связана с проводной подсетью «Маркетинг»; тогда как беспроводная сеть «Развитие» связана с проводной подсетью «Развитие». Начальные реализации концепции виртуальных точек доступа были ограничены использованием одной беспроводной сети на точке доступа. Однако в данный момент уже есть много производителей, которые предлагают полнофункциональные виртуальные точки доступа с дифференцированными беспроводными подсетями, как на «облегченных», так и на полнофункциональных точках доступа.



## 7.2 Выбор расположения оборудования

Особо следует отметить необходимость предпроектного обследования. Оно заключается в измерении и анализе того, как распространяются сигналы от реальных точек доступа, временно устанавливаемых в помещениях объекта. Многие пользователи и системные администраторы сталкиваются с проблемами покрытия своего офиса или дома уверенной связью. Чем хуже качество приёма сигнала на компьютере клиента, тем на меньшей скорости будет установлено соединение [9].

Обследование позволяет учесть наличие таких препятствий для радиосигналов, как скрытая в стенах металлическая сетка, трубопроводы и кабелепроводы, оценить степень поглощения радиосигналов стенами и перегородками, установить уровень помех от «чужих» беспроводных сетей. Другая проблема – обеспечение устойчивой связью пользователей на большом расстоянии от точки доступа.

По результатам обследования становится возможным уточнить требуемое количество, местоположение и мощность точек доступа, типы антенн и требования к монтажу, которые обеспечивают требуемую зону радиопокрытия и скорость подключения.

В России, для беспроводных сетей определён диапазон частот 2400 - 2483.5 МГц, в котором могут работать передатчики мощностью не больше 100 мВт.

Увеличить дальность действия своей беспроводной сети можно двумя способами. Первый – устанавливать ретрансляторы, которые будут повторять ваш сигнал через какое-то расстояние, создавая коридор для беспроводной сети. В качестве ретранслятора может работать и точка доступа в режиме "Repeater". Другой способ проще в реализации – потребуется лишь специальная Wi-Fi антенна.

Несколько точек доступа позволяют организовать "соты" – перекрывающиеся зоны для уверенного приема. При этом пользователь, даже перемещаясь из зоны в зону, связь не потеряет, так как одна точка доступа "передает" его другой. Эта технология называется «беспроводной роуминг».

Проектирование места расположения точек доступа обычно происходит в три этапа. На первом этапе, после предпроектного обследования, определяют средний

радиус действия беспроводных точек на местах. Исходя из этого радиуса, строят окружности на плане помещения (рисунок 7.1). Обычно в стандартных домах перекрытия снижают зону покрытия на 10-15%, поэтому одна точка доступа по вертикали может покрыть еще 1 или 2 этажа.

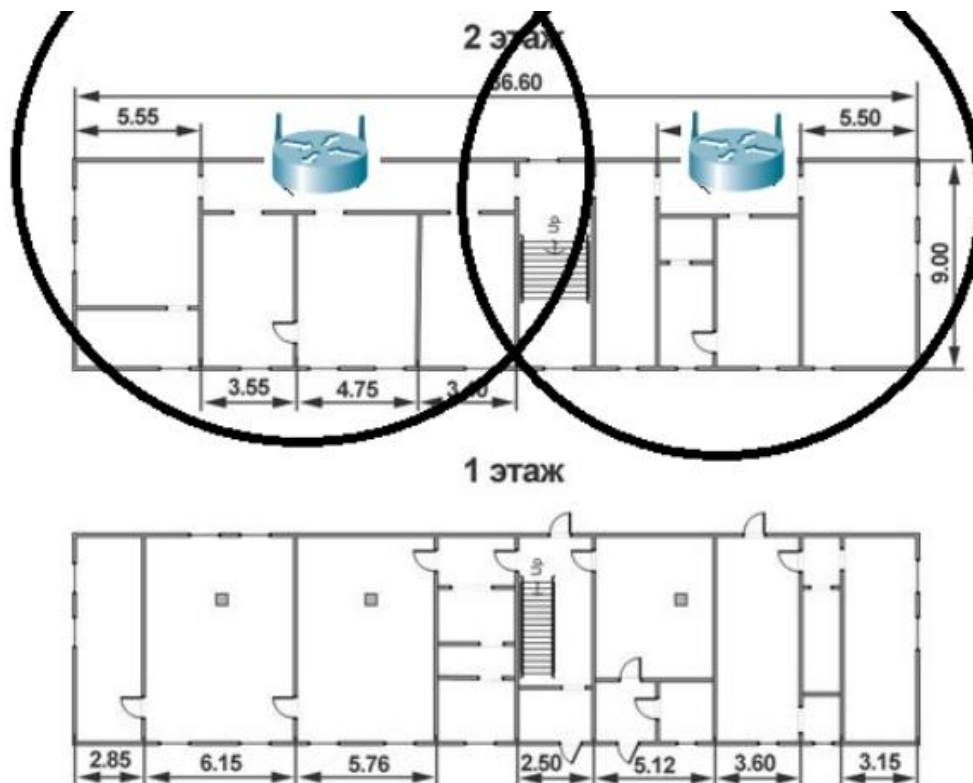


Рисунок 7.1 – Проектирование зоны покрытия беспроводной сети

Зоны покрытия должны перекрываться минимум на 20% для обеспечения уверенного приема. Каждая из точек доступа обозначается цифрой от 1 до 3 (различные частотные каналы, цифра 1 будет означать первый канал, 2 – шестой, 3 – одиннадцатый), причем никакие соседние точки не должны иметь одинаковый номер. На соседних точках доступа следует настраивать непересекающиеся или различные каналы, если они имеют зону перекрытия. Если каналы будут пересекаться, то это вызовет снижение пропускной способности и может привести к потерям соединения беспроводного клиента.

Если точки доступа будут функционировать в режиме WDS с точкой доступа, то необходимо предусмотреть наличие связи между точками доступа на отдельном

канале. В других случаях к каждой точке доступа необходимо протянуть кабель Ethernet.

### 7.3 Настройка оборудования

Настройку беспроводного оборудования следует производить только после проектирования параметров беспроводной сети. Сначала необходимо выбрать имя беспроводной сети (SSID), метод защиты информации (шифрование), метод аутентификации (локально или через сервер Radius). Для маленьких сетей рекомендуется шифрование WPA –PSK или WPA2-PSK, авторизация локально на точке доступа. Для крупных сетей – WPA или WPA2 с авторизацией через сервер Radius.

На следующем примере будет показана малая сеть с шифрованием на основе точки доступа. Для начала необходимо разместить в эмуляторе Packet Tracer необходимое оборудование (рисунок 7.2).

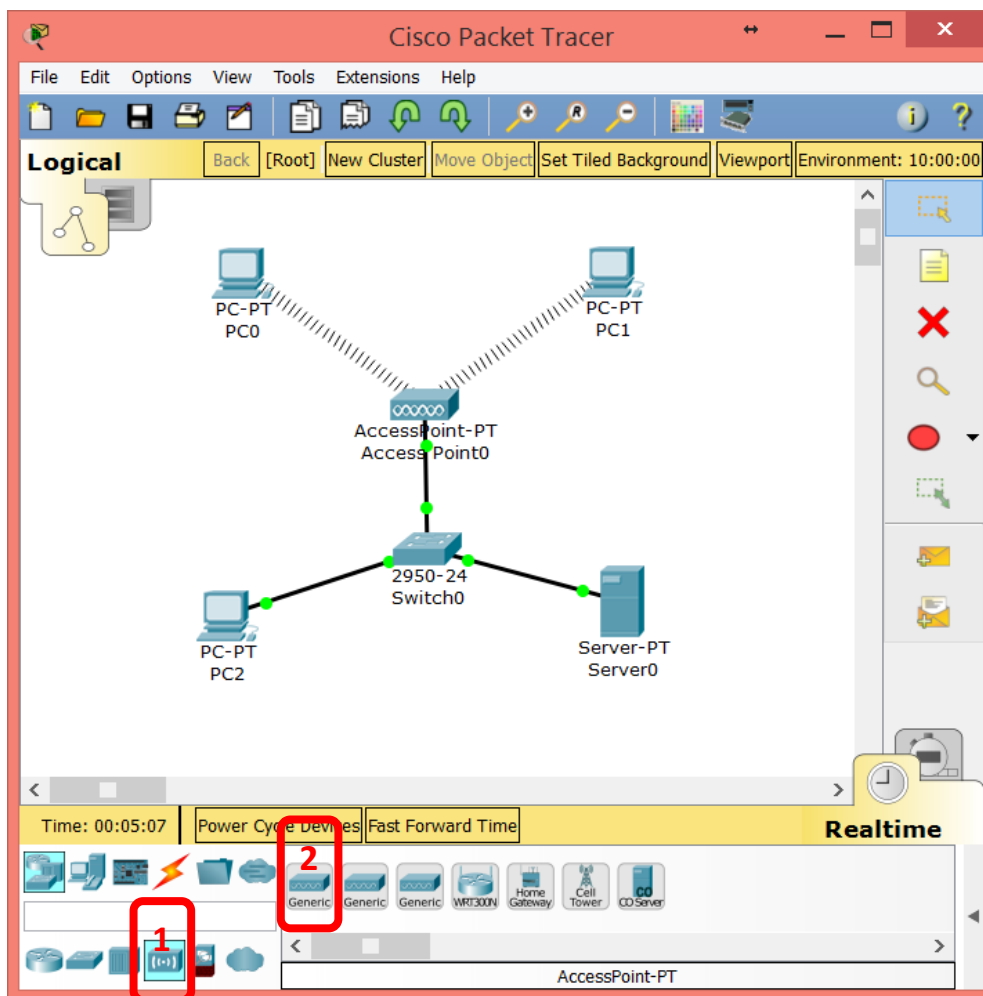


Рисунок 7.2 – Схема сети

На вкладке Wireless Devices (элемент 1) необходимо перетащить AccessPoint-PT (элемент 2) на рабочую область. Для подключения компьютера к беспроводной сети необходимо добавить ему модуль PT-HOST-NM-1W.

После этого между устройствами сразу возникнет беспроводная связь. Затем необходимо добавить коммутатор, компьютер и сервер. Но это еще не настроенная небезопасная сеть. Теперь настроим точку доступа (рисунок 7.3).

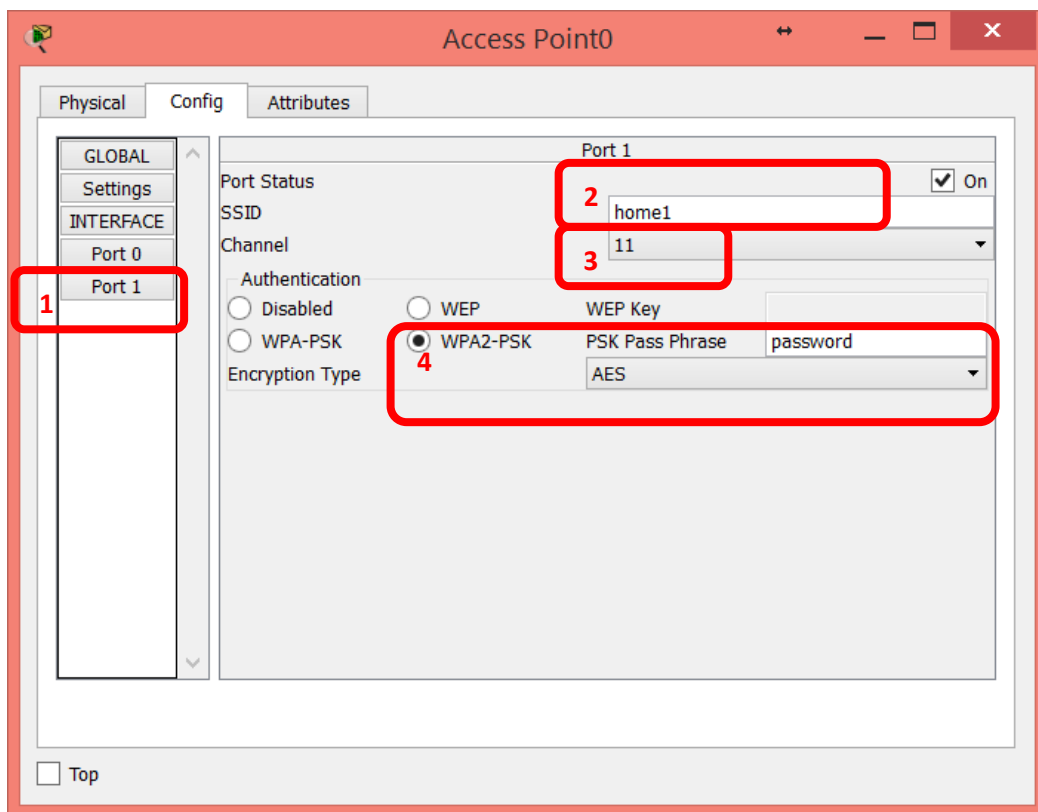


Рисунок 7.3 – Настройка точки доступа

На вкладке Port 1 (элемент 1) необходимо задать имя сети (SSID, элемент 2), номер канала (элемент 3) и шифрование (элемент 4). После этого необходимо настроить все компьютеры (рисунок 7.4).

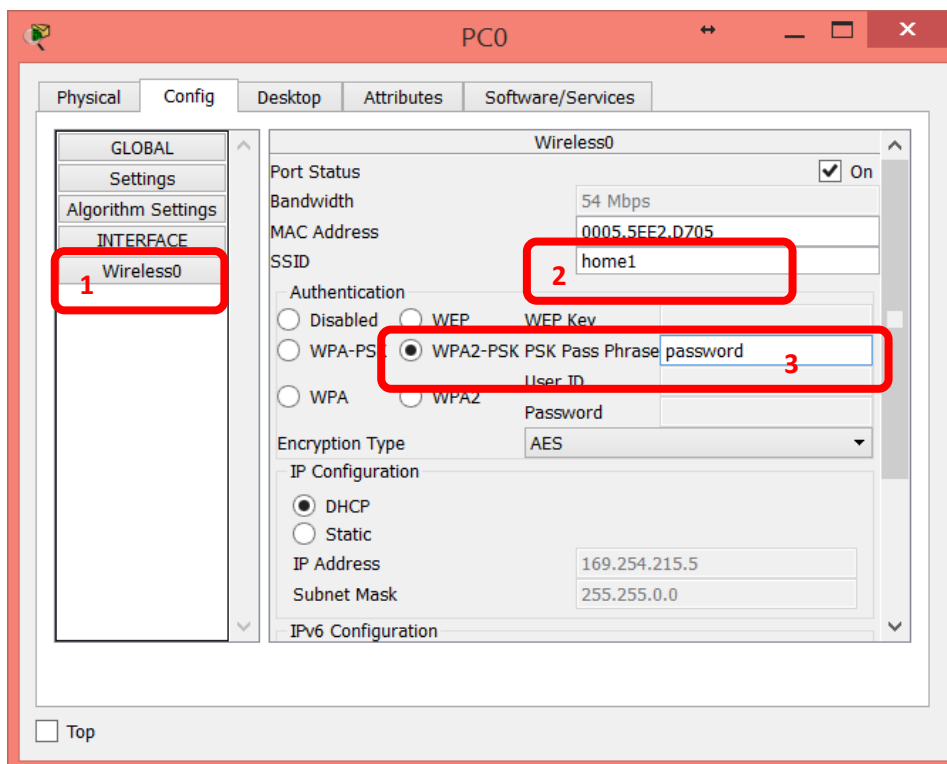


Рисунок 7.4 – Настройка беспроводного компьютера

На вкладке Wireless0 (элемент 1) необходимо задать имя сети (SSID, элемент 2, должен совпадать с SSID на точке доступа) и параметры шифрования (элемент 3, должны совпадать с настройками точки доступа). После завершения всех настроек компьютеры должны подключиться к точке доступа (должна возникнуть связь).

Теперь для упрощения остальных настроек необходимо настроить IP адрес 10.1.1.1/255.255.255.0 и DHCP сервер.

Для настройки DHCP сервера (рисунок 7.5) необходимо задать начальный адрес (Start IP Address) 10.1.1.10/255.255.255.0, количество клиентов (Maximum number of Users) 20, и сохранить параметры нажатием кнопки Save.

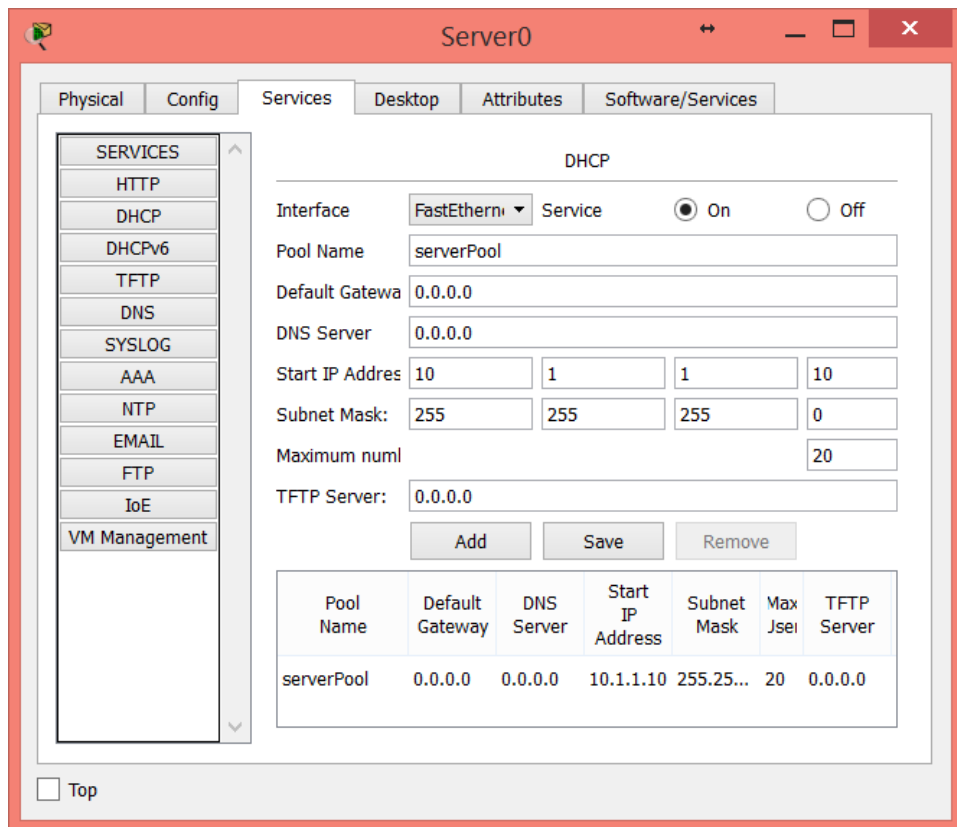


Рисунок 7.5 – Настройка DHCP сервера

Проверить правильность настройки можно командой *ping* из *command prompt* компьютеров. Так как настройка DHCP сервера была произведена после включения компьютеров, необходимо обновить IP параметры командой *ipconfig /renew*, затем выполнить команду *ping* до соседнего компьютера или до сервера (рисунок 7.6).

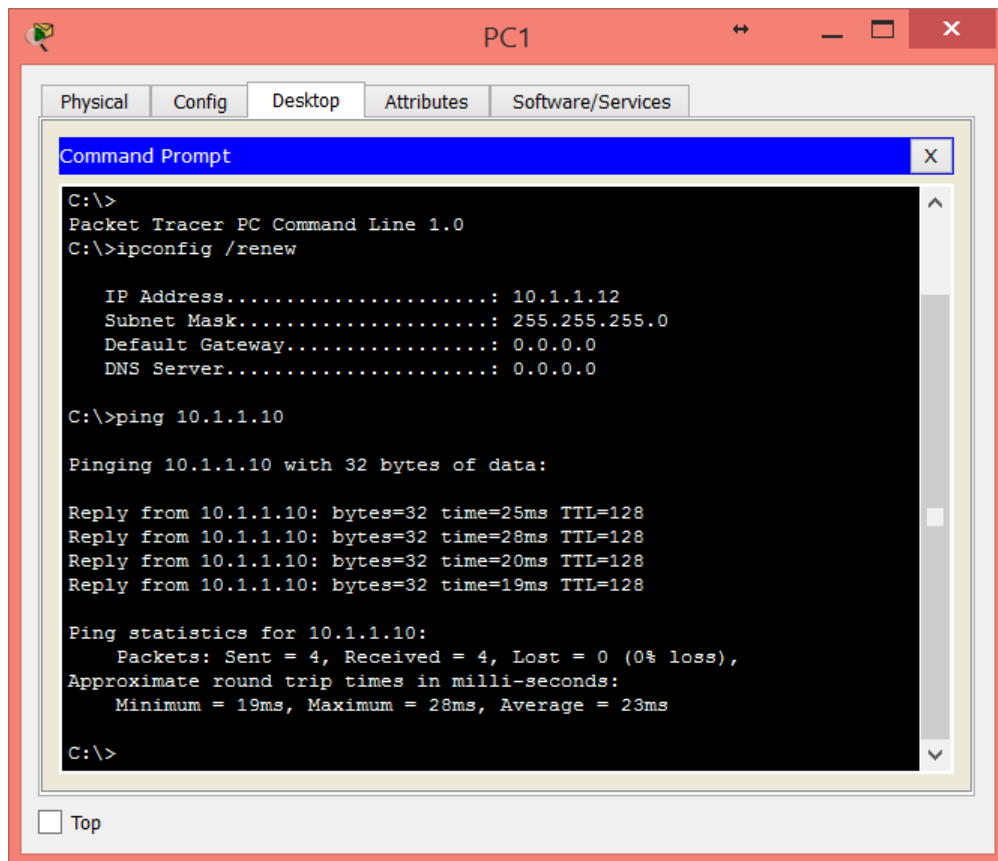


Рисунок 7.6 – Проверка беспроводного соединения.

Часто в домашних и малых сетях используются не точки доступа, а беспроводные маршрутизаторы. По большому счету, настройка таких устройств очень схожа, но маршрутизаторы обычно настраиваются через Web-интерфейс, представленный вкладкой GUI (рисунок 7.7). На вкладке Setup (элемент 1) настраиваются сетевые параметры. Прежде всего, каким образом устройство подключается к проводной сети (элемент 2). Кроме варианта DHCP и Static (задание вручную), часто бывают варианты PPP, PPPoE, PPTP и т.д. Они нужны для подключения к провайдерам Интернет напрямую, без участия компьютера.

Каждый беспроводной маршрутизатор имеет встроенный DHCP сервер, который настраивается аналогично DHCP-серверу на обычном сервере (элемент 4), а базовые настройки IP адреса беспроводного интерфейса выполняются в элементе 3.

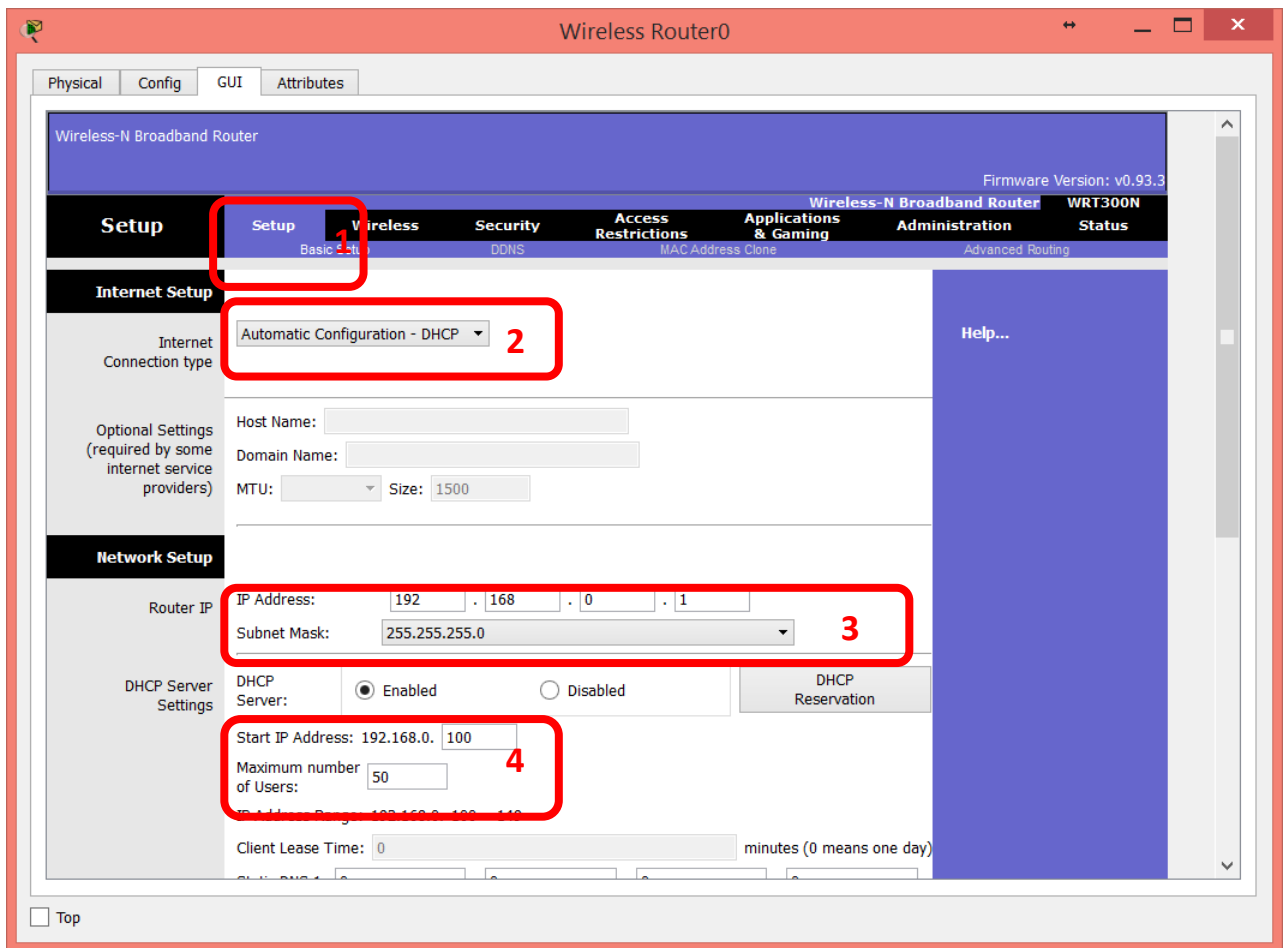


Рисунок 7.7 – Настройка беспроводного маршрутизатора

Настроек в маршрутизаторе обычно на порядок больше, чем в точке доступа. Выбор типа настроек осуществляется с помощью меню (рисунок 7.8, элемент 1) и подменю (элемент 2). Например, для настройки шифрования беспроводной сети необходимо выбрать меню **Wireless** и подменю **Wireless Security**.

После выполнения всех настроек обязательно нужно сохранить все настройки нажатием кнопки **Save**, находящейся в нижней части окна (элемент 3)



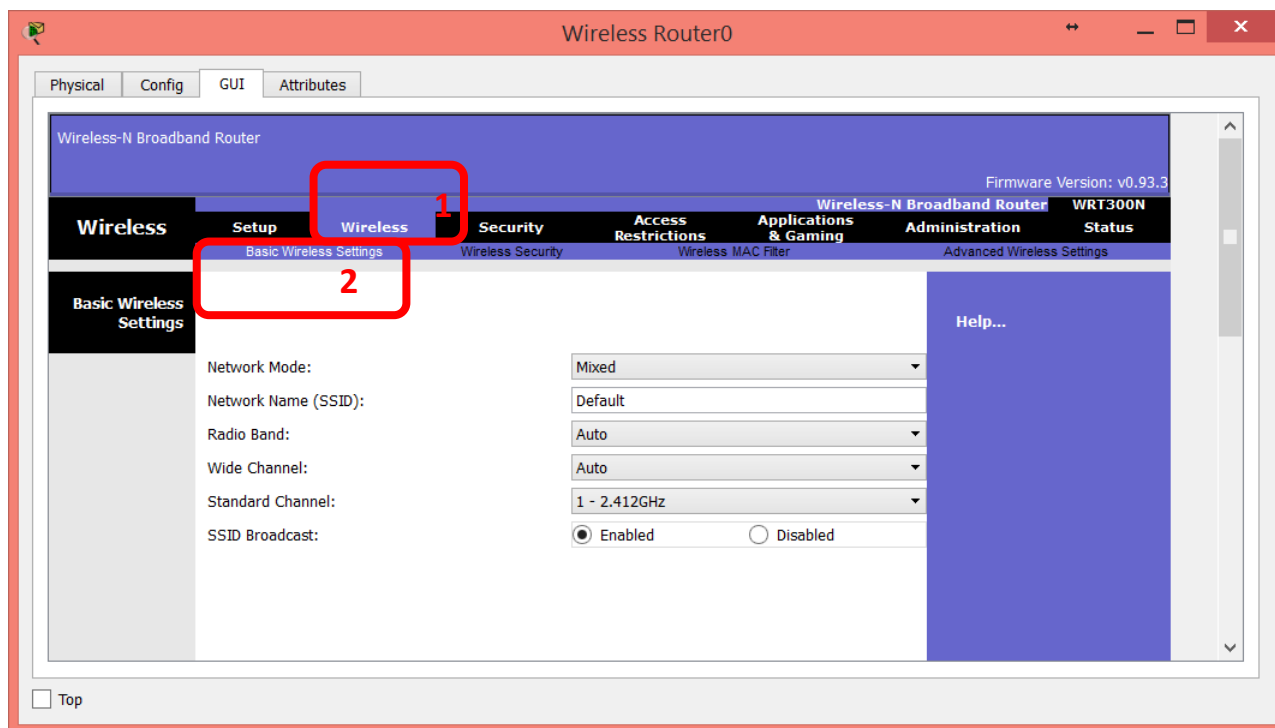


Рисунок 7.8 – Настройка беспроводной части маршрутизатора

#### 7.4 Рабочее задание

Необходимо создать беспроводную сеть, состоящую из точки доступа, беспроводного маршрутизатора, двух беспроводных компьютеров, сервера и коммутатора (рисунок 7.9). Следующие требования должны быть выполнены:

- 1) Каждый из двух беспроводных компьютеров должен быть подключен к своему беспроводному устройству.
- 2) SSID на маршрутизаторе должно быть wifi\_1, на точке доступа wifi\_2.
- 3) Радиоканал на точке доступа должен быть установлен на 6, на маршрутизаторе – на 11.
- 4) Шифрование на точке доступа – WPA-PSK, на маршрутизаторе – WPA2-PSK.
- 5) На сервере должен быть настроен IP адрес и DHCP-сервис на 20 адресов.

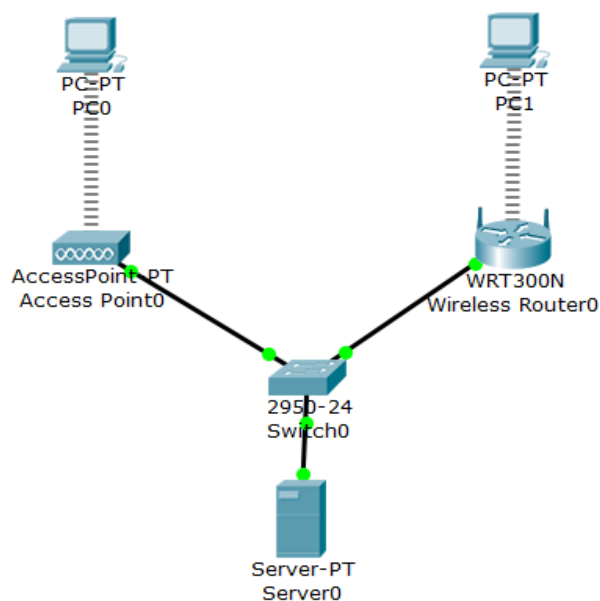


Рисунок 7.9 – Исходная сеть

После сборки необходимо протестировать сеть командой ping.

Таблица 7.1 – Варианты заданий к работе 7

Вариант	IP сеть для сети 1	IP сеть для сети 2
1	172.16.32.32/27	10.14.2.192/26
2	10.18.22.16/28	192.168.100.128/26
3	192.168.100.64/27	10.18.22.16/28
4	10.14.2.192/26	172.16.32.32/27
5	192.168.100.128/26	192.168.100.64/27
6	172.16.32.32/27	10.14.2.192/26
7	10.18.22.16/28	192.168.100.128/26
8	192.168.100.64/27	10.18.22.16/28
9	10.14.2.192/26	172.16.32.32/27
10	192.168.100.128/26	192.168.100.64/27

## **8 Лабораторная работа №8. Проектирование физической схемы сети, расчет комплектующих и расходных материалов**

*Цель работы.* Изучить принципы проектирования физической схемы сети.

Получить навыки выбора оборудования для проектируемой сети.

### **8.1 Общие сведения**

Создание рабочего проекта сети очень трудоемко и требует значительных временных затрат. На этапе проектирования решаются следующие задачи:

1) На основе определенных целевых требований к сети определяется необходимый состав оборудования и, прежде всего, компьютеров: количество, характеристики и т.д.

2) Определяется физическое расположение рабочих мест. Если речь идет о создании сети в одном здании, то определяются этажи и комнаты, которые должны охватываться сетью. При решении этой задачи должна учитываться принципиальная возможность прокладки линий связи к рабочим местам/помещениям.

3) Исходя из решаемых задач, стоимости и расположения, определяется тип физических линий связи, соединяющих рабочие места, а также состав и расположение коммуникационного оборудования (например, концентраторов).

4) Определяется способ подключения к Интернету, выбирается провайдер – организация, обеспечивающая подключение организации к сети Интернет.

5) Исходя из технических требований, определяется узел проектируемой сети, который будет являться шлюзом для подключения к Интернету и определяется место его расположения. При этом учитывается удобство физического соединения шлюза с проектируемой сетью и удобство подведения физических линий для подключения к Интернету.

Проектирование инфраструктуры является самой трудоемкой задачей в проекте. Оно решает следующие задачи:

1) Определяются протоколы, которые будут использоваться в сети. Основными протоколами для сетей Windows являются протоколы стека TCP/IP. Они же используются для подключения к Интернету. Если в сети используются

компьютеры под управлением других ОС, необходимо выбирать протоколы, поддерживаемые всем используемым оборудованием (например, IP телефония).

2) Осуществляется планирование IP-сетей – сетям назначаются диапазоны IP-адресов, планируется топология маршрутизации.

3) Определяется, будет ли планируемая сеть одноранговой (все компьютеры такой сети равноправны) или в ней предполагается разместить выделенные серверы для поддержки определенных функций.

4) Определяется, будут ли компьютеры планируемой сети объединяться в рабочие группы или в домены.

5) Определяется, какие службы будут развертываться в сети.

6) Определяются группы пользователей сети, и планируется политика безопасности в сети.

Исходя из плана какого-либо помещения, необходимо выполнить проектирование сети. При создании новой сети желательно учитывать следующие факторы:

- требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу);

- структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия);

- основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальнейшей перспективе);

- характер передаваемой по сети информации;

- технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов);

- возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля;

- обслуживание сети и контроль ее безотказности и безопасности;

- требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям

контроля обмена информацией и т.д. (например, если предполагается использование одного ресурса многими пользователями, то следует использовать серверную ОС);

- необходимость подключения к другим сетям (например, глобальным);
- имеющиеся компьютеры и их программное обеспечение, а также периферийные устройства (принтеры, сканеры и т.д.).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара UTP. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости.

Для физического проектирования сетей применяют метод пятидесятиметровой окружности. Метод пятидесятиметровой окружности заключается в следующем. Необходимо на плане сети нарисовать несколько окружностей радиусом 50м. Затем выбрать то количество и расположение окружностей, которые оптимально покрывают все компьютеры. Например, в длинном помещении оптимально будет две-три окружности (рисунок 8.1). Все окружности должны пересекаться минимум на 20%. Центр каждой окружности – оптимальное место для установки коммутатора. Однако надо учитывать и особенности помещения, так как шкаф с оборудованием может висеть только на стене (за редким исключением).

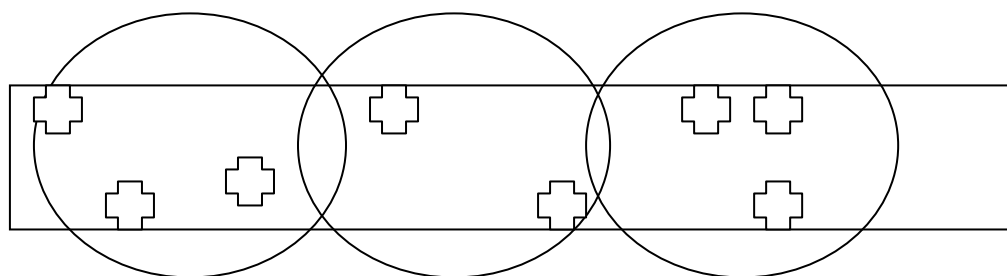


Рисунок 8.1 – Пример оптимального изображения пятидесятиметровых окружностей в длинном здании.

Длина кабеля рассчитывается для каждого помещения отдельно методом средней длины. При этом:

- 1) Кабель делится на два отрезка: от коммутатора до ввода в помещение (эту длину обозначим  $L1$ ) и от ввода в помещение до компьютеров (эту длину обозначим  $L2$ ).
- 2) Длина каждого отрезка кабеля измеряется по плану здания.
- 3) Общая длина кабеля, необходимая для подключения  $n$  компьютеров в помещении рассчитывается по формуле (8.1):

$$L = n * (L1 + L2 * 0.7) \quad (8.1)$$

где  $n$  – количество компьютеров.

Затем рассчитывается общее число портов каждого коммутатора суммированием всех подведенных к нему кабелей. Реальное количество портов коммутатора должно превышать требуемое количество не менее чем на 20% или на 5шт. Это делается для обеспечения масштабируемости.

## **8.2 Рабочее задание**

В соответствии с вариантами заданий (таблица 8.1) и планом помещений (рисунок 8.2):

- 1) Определить количество компьютеров и комнаты, в которых они будут стоять, выбрать комнату – центральную серверную.
- 2) Разместить компьютеры по помещениям.
- 3) Исходя из расположения компьютеров, методом пятидесятиметровой окружности выбрать оптимальные места расположения коммутаторов.
- 4) Визуально провести кабель до коммутаторов, рассчитать требуемое количество портов коммутаторов.
- 5) Рассчитать длину требуемого кабеля для каждого помещения.
- 6) Рассчитать длину кабеля от коммутаторов до центральной серверной.
- 7) Рассчитать количество портов центрального коммутатора.

8) Составить список требуемого оборудования (серверы, коммутаторы, маршрутизаторы, беспроводные точки, модемы, ИБП, стойки, шкафы, патч-панели, патч-корды, кабель, кабель-каналы, коннекторы, дюбель-гвозди, подвесы, лотки и т.д.).

9) Выбрать конкретные модели оборудования и материалов, вставить в спецификацию модели и цены.

10) Оформить схему сети и спецификацию оборудования.

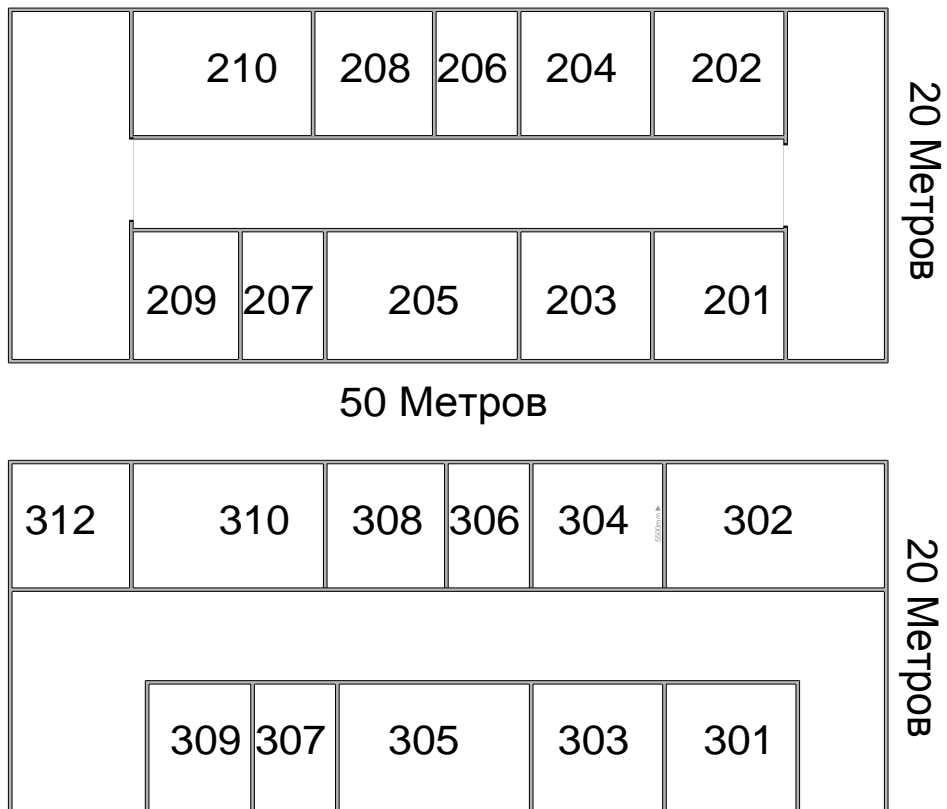


Рисунок 8.2 – План помещений 2 и 3 этажей

Таблица 8.1 – Варианты заданий

Вариант	Номера помещений с компьютерами	Общее количество компьютеров
1	2	3
1	210 206 201 310 305 302	30
2	207 208 203 301 303 309	40

3	208 206 203 201 312 302	25
4	209 207 203 308 304 303	32
5	205 203 312 306 301 302	36
6	205 206 207 307 308 312	28
7	210 205 202 301 308 309	29
8	209 207 205 309 307 310	31
9	208 204 202 303 307 310	52
10	202 206 210 308 304 303	45

### 8.3 Контрольные вопросы

- 1) Описать процесс проектирования сети.
- 2) Какие задачи решаются на этапе проектирования сети?
- 3) Какие факторы необходимо учитывать при проектировании новой сети?
- 4) В чем суть метода пятидесятиметровой окружности?
- 5) Описать алгоритм расчета длины кабеля при создании новой сети.
- 6) Как учитывается требование масштабируемости при проектировании сети?
- 7) Когда применяется метод пятидесятиметровой окружности?
- 8) Что включает в себя проектирование инфраструктуры?
- 9) Что должно учитываться при проектировании линий связи до конечных пользователей?
- 10) Что необходимо предусмотреть при выборе серверной комнаты?

## 9 Лабораторная работа №9. Настройка VLAN

### 9.1 Общие сведения

VLAN (Virtual Local Area Network) – группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга



на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

В современных сетях VLAN – главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности.

Функции VLAN:

1) Гибкое разделение устройств на группы

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения

2) Уменьшение количества широковещательного трафика в сети

Каждый VLAN – это отдельный широковещательный домен. Например, коммутатор – это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене. Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

3) Увеличение безопасности и управляемости сети

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

Компьютер при отправке трафика в сеть даже не догадывается, в каком VLAN'е он размещён. Об этом думает коммутатор. Коммутатор знает, что

компьютер, который подключен к определённому порту, находится в соответствующем VLAN'e. Трафик, приходящий на порт определённого VLAN'a, ничем особенным не отличается от трафика другого VLAN'a. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q. Существуют проприетарные протоколы, решающие похожие задачи, например, протокол ISL от Cisco Systems, но их популярность значительно ниже (и снижается).

### 9.1.1 Настройка VLAN на коммутаторах

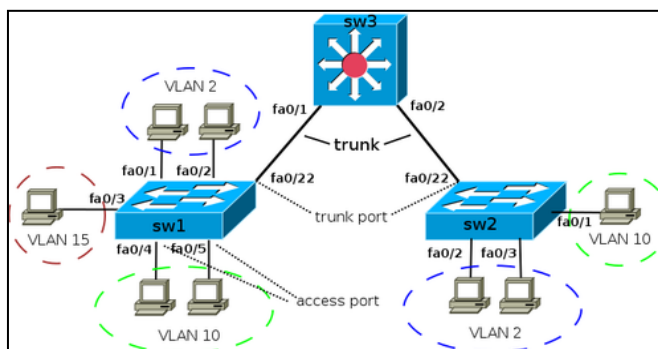


Рисунок 9.1 – Сеть с VLAN на коммутаторах

На рисунке 9.1 показана схема сети с VLANами на коммутаторах.

Для создания VLAN с именем test на коммутаторе sw1 используются команды, показанные на рисунке 9.2.

```
Sw1 (config)#vlan 2
Sw1 (config-vlan)#name test
Sw1 (config-vlan)#
```

Рисунок 9.2 – Создание VLAN

Для назначения портов 1 и 2 коммутатора в VLAN используются команды, показанные на рисунке 9.3:

```
Sw1(config)#interface range fa 0/1 - 2
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#switchport access vlan 2
```

Рисунок 9.3 – Назначение портов

VLAN можно создать на коммутаторе с помощью команды `vlan`. Кроме того, VLAN автоматически создается на коммутаторе в момент добавления в него интерфейсов в режиме `access`. Например, при выполнении команд, осуществляющих назначение диапазона портов с `fa0/4` до `fa0/5` в `vlan 10`, произойдет автоматическое создание VLAN 10 (рисунок 9.4):

```
Sw1(config)#interface range fa 0/4 - 5
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
```

Рисунок 9.4 – Автоматическое создание VLAN 10

Просмотреть информацию о VLAN можно с помощью команды `show vlan brief`, как показано на рисунке 9.5.

```
Sw1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
2	test	active	Fa0/1, Fa0/2
10	VLAN0010	active	Fa0/4, Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Рисунок 9.5 – Информация о VLAN

Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим `trunk`.

Режимы интерфейса (режим по умолчанию зависит от модели коммутатора):

– `auto` – порт находится в автоматическом режиме и будет переведён в состояние `trunk`, только если порт на другом конце находится в режиме `on` или `desirable`. Т.е. если порты на обоих концах находятся в режиме "auto", то `trunk` применяться не будет.

– `desirable` – порт находится в режиме "готов перейти в состояние `trunk`"; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние `trunk` (состояние `trunk` будет установлено, если порт на другом конце находится в режиме `on`, `desirable`, или `auto`).

– trunk – порт постоянно находится в состоянии trunk, даже если порт на другом конце не поддерживает этот режим.

– nonnegotiate – порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим "не-cisco" оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk'a.

По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

На коммутаторах sw1 и sw2 нужные VLAN будут созданы в момент добавления access-портов в соответствующие VLAN (рисунок 9.6):

```
Sw1(config)#interface fa0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 15
% Access VLAN does not exist. Creating vlan 15
```

Рисунок 9.6 – Автоматическое создание VLAN

На коммутаторе sw3 access-портов нет. Поэтому нужно явно создать все необходимые VLAN (vlan 2, vlan 10, vlan 15).

Создание статического транка показано на рисунке 9.7:

```
Sw1(config)#interface fa0/22
Sw1(config-if)#switchport mode trunk
```

Рисунок 9.7 – Создание статического транка

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.

Указать перечень разрешенных VLAN для транкового порта fa0/22 можно с помощью команд, показанных на рисунке 9.8:

```
Sw1(config)#interface fa0/22
Sw1(config-if)#switchport trunk allowed vlan 1-2,10,15
```

Рисунок 9.8 – Настройка перечня разрешенных VLAN

Для добавления еще одного разрешенного VLAN используется команда *switchport trunk allowed vlan add X*, для удаления – *switchport trunk allowed vlan remove X*, где X – номер VLAN.

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. По умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native. Например, чтобы настроить VLAN 5 как native, нужно выполнить команду *switchport trunk native vlan 5*. Теперь весь трафик, принадлежащий VLAN'у 5, будет передаваться через транковый интерфейс нетегированным, а весь пришедший на транковый интерфейс нетегированный трафик будет промаркирован как принадлежащий VLAN'у 5 (по умолчанию VLAN 1).

### 9.1.2 Настройка маршрутизации между VLAN

Все настройки по назначению портов в VLAN, сделанные ранее для sw1, sw2 и sw3, сохраняются. Дальнейшие настройки подразумевают использование sw3 как коммутатора 3 уровня.

Далее необходимо дополнить схему сети в соответствии с рисунком 9.9 и настроить адресацию согласно таблице 9.1.

Таблица 9.1 – Настройки на коммутаторе sw3

VLAN / интерфейс 3го уровня	IP-адрес
VLAN 2	10.0.2.1 /24
VLAN 10	10.0.10.1 /24
VLAN 15	10.0.15.1 /24
Fa 0/10	192.168.1.2 /24

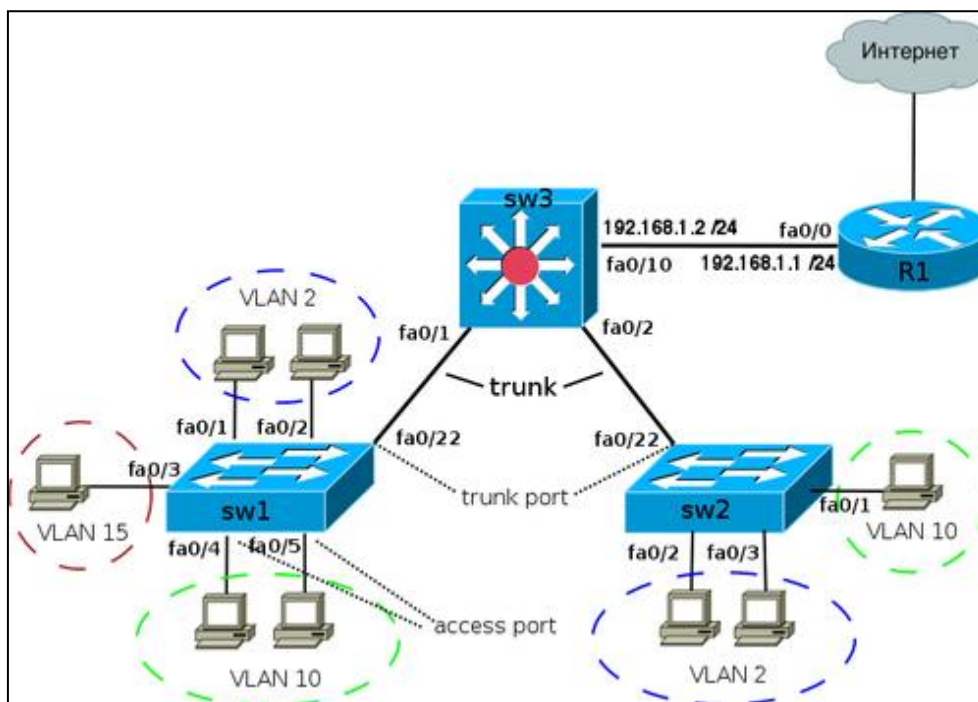


Рисунок 9.9 – Дополненная схема сети

Для включения маршрутизации на коммутаторе sw3 используется команда, показанная на рисунке 9.10:

```
Sw3(config)#ip routing
```

Рисунок 9.10 – Включение маршрутизации на коммутаторе

Для задания маршрута по умолчанию для компьютеров в VLAN 2 нужно выполнить команды, показанные на рисунке 9.11.

```
Sw3(config)# interface Vlan2
Sw3(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2,
changed state to up
Sw3(config-if)#ip address 10.0.2.1 255.255.255.0
Sw3(config-if)#no shutdown
```

Рисунок 9.11 – Настройка маршрута по умолчанию для компьютеров в VLAN2

Аналогично настраивается адрес в VLAN 10 (рисунок 9.12):

```
Sw3(config)# interface Vlan10
Sw3(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
changed state to up
Sw3(config-if)#ip address 10.0.10.1 255.255.255.0
Sw3(config-if)#no shutdown
```

Рисунок 9.12 – Настройка маршрута по умолчанию для компьютеров в VLAN

Интерфейс fa0/10 соединен с маршрутизатором. Этот интерфейс можно перевести в режим 3 уровня.

Перевод fa0/10 в режим интерфейса 3 уровня и задание IP-адреса показан на рисунке 9.13:

```
Sw3(config)#interface FastEthernet 0/10
Sw3(config-if)#no switchport
Sw3(config-if)#ip address 192.168.1.2 255.255.255.0
Sw3(config-if)#no shutdown
```

Рисунок 9.13 – Перевод fa0/10 в режим интерфейса 3 уровня и задание IP-адреса

Маршрутизатор R1 используется как шлюз по умолчанию для рассматриваемой сети. Трафик, не предназначенный сетям VLAN'ов, будет передаваться на R1.

Настройка маршрута по умолчанию выполняется с помощью команды, показанной на рисунке 9.14:

```
Sw3(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Рисунок 9.14 – Настройка маршрута по умолчанию

Информации о настройках интерфейса (о транке) можно просмотреть с помощью команды, показанной на рисунке 9.15:

```
Sw1#show interface fa0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Рисунок 9.15 – Информации о настройках транкового интерфейса

Просмотр информации о настройках интерфейса (об access-интерфейсе) выполняется с помощью команды, показанной на рисунке 9.16:

```

Sw1#show interface fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 15 (VLAN0015)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

```

Рисунок 9.16 – Просмотр информации о настройках access-интерфейса

В таблице 9.2 показаны диапазоны VLAN.

Таблица 9.2 – Диапазоны VLAN

VLANs	Диапазон	Использование	Передается VTP
0, 4095	Reserved	Только для системного использования.	--
1	Normal	VLAN по умолчанию. Можно использовать, но нельзя удалить.	Да
2-1001	Normal	Для VLANов Ethernet. Можно создавать, удалять и использовать.	Да
1002-1005	Normal	Для FDDI и Token Ring. Нельзя удалить.	Да
1006-4094	Extended	Только для VLANов Ethernet.	Версия 1 и 2 нет, версия 3 да

### 2.1.3 Пример базовой настройки VLAN, без настройки маршрутизации

В этом разделе приведены конфигурационные файлы коммутаторов для схемы, изображенной на рисунке 1. На коммутаторе sw3 не настроена маршрутизация между VLAN, поэтому в данной схеме хосты могут общаться только в пределах одного VLAN.

Например, хосты на коммутаторе sw1 в VLAN 2 могут взаимодействовать между собой и с хостами в VLAN 2 на коммутаторе sw2. Однако они не могут взаимодействовать с хостами в других VLAN на коммутаторах sw1 и sw2.



Не все настройки являются обязательными. Например, перечисление разрешенных VLAN в транке не является обязательным для работы транка, однако рекомендуется настраивать разрешенные VLAN явно.

#### Конфигурация sw1:

```
!  
interface FastEthernet0/1  
  switchport mode access  
  switchport access vlan 2  
!  
interface FastEthernet0/2  
  switchport mode access  
  switchport access vlan 2  
!  
interface FastEthernet0/3  
  switchport mode access  
  switchport access vlan 15  
!  
interface FastEthernet0/4  
  switchport mode access  
  switchport access vlan 10  
!  
interface FastEthernet0/5  
  switchport mode access  
  switchport access vlan 10  
!  
interface FastEthernet0/22  
  switchport mode trunk  
  switchport trunk allowed vlan 1,2,10,15  
!
```

#### Конфигурация sw2:

```
!  
interface FastEthernet0/1  
  switchport mode access  
  switchport access vlan 10  
!  
interface FastEthernet0/2  
  switchport mode access  
  switchport access vlan 2  
!  
interface FastEthernet0/3  
  switchport mode access  
  switchport access vlan 2  
!  
interface FastEthernet0/22  
  switchport mode trunk  
  switchport trunk allowed vlan 1,2,10  
!
```

### Конфигурация sw3:

```
!  
vlan 2,10,15  
!  
interface FastEthernet0/1  
  switchport mode trunk  
  switchport trunk allowed vlan 1,2,10,15  
!  
interface FastEthernet0/2  
  switchport mode trunk  
  switchport trunk allowed vlan 1,2,10  
!
```

### 9.1.4 Пример конфигураций с настройкой маршрутизации между VLAN

В этом разделе приведены конфигурационные файлы коммутаторов для схемы, показанной на рисунке 9.9. На коммутаторе sw3 настроена маршрутизация между VLAN, поэтому в данной схеме hosts могут общаться как в пределах одного VLAN, так и между различными VLAN.

Например, hosts на коммутаторе sw1 в VLAN 2 могут взаимодействовать между собой и с hosts в VLAN 2 на коммутаторе sw2. Кроме того, они могут взаимодействовать с hosts в других VLAN на коммутаторах sw1 и sw2.

Настройки коммутаторов sw1 и sw2 остались точно такими же, как и в предыдущем разделе. Добавились дополнительные настройки только на коммутаторе sw3.

### Конфигурация sw1:

```
!  
interface FastEthernet0/1  
  switchport mode access  
  switchport access vlan 2  
!  
interface FastEthernet0/2  
  switchport mode access  
  switchport access vlan 2  
!  
interface FastEthernet0/3  
  switchport mode access  
  switchport access vlan 15  
!  
interface FastEthernet0/4  
  switchport mode access  
  switchport access vlan 10  
!
```

```
interface FastEthernet0/5
  switchport mode access
  switchport access vlan 10
!
interface FastEthernet0/22
  switchport mode trunk
  switchport trunk allowed vlan 1,2,10,15
!
```

### Конфигурация sw2:

```
!
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 10
!
interface FastEthernet0/2
  switchport mode access
  switchport access vlan 2
!
interface FastEthernet0/3
  switchport mode access
  switchport access vlan 2
!
interface FastEthernet0/22
  switchport mode trunk
  switchport trunk allowed vlan 1,2,10
!
```

### Конфигурация sw3:

```
!
ip routing
!
vlan 2,10,15
!
interface FastEthernet0/1
  switchport mode trunk
  switchport trunk allowed vlan 1,2,10,15
!
interface FastEthernet0/2
  switchport mode trunk
  switchport trunk allowed vlan 1,2,10
!
!
interface FastEthernet0/10
  no switchport
  ip address 192.168.1.2 255.255.255.0
!
!
interface Vlan2
  ip address 10.0.2.1 255.255.255.0
!
```

```

interface Vlan10
ip address 10.0.10.1 255.255.255.0
!
interface Vlan15
ip address 10.0.15.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1

```

### 9.1.5 Настройка VLAN на маршрутизаторах Cisco

Передача трафика между VLAN может осуществляться с помощью маршрутизатора. Для того чтобы маршрутизатор мог передавать трафик из одного VLAN в другой (из одной сети в другую), необходимо, чтобы в каждой сети у него был интерфейс. Для того чтобы не выделять под сеть каждого VLAN отдельный физический интерфейс, создаются логические субинтерфейсы на физическом интерфейсе для каждого VLAN.

На коммутаторе порт, ведущий к маршрутизатору, должен быть настроен как тегированный (транковый) порт.

Изображенная на рисунке 9.17 схема, в которой маршрутизация между VLAN выполняется на маршрутизаторе, часто называется *router on a stick*.

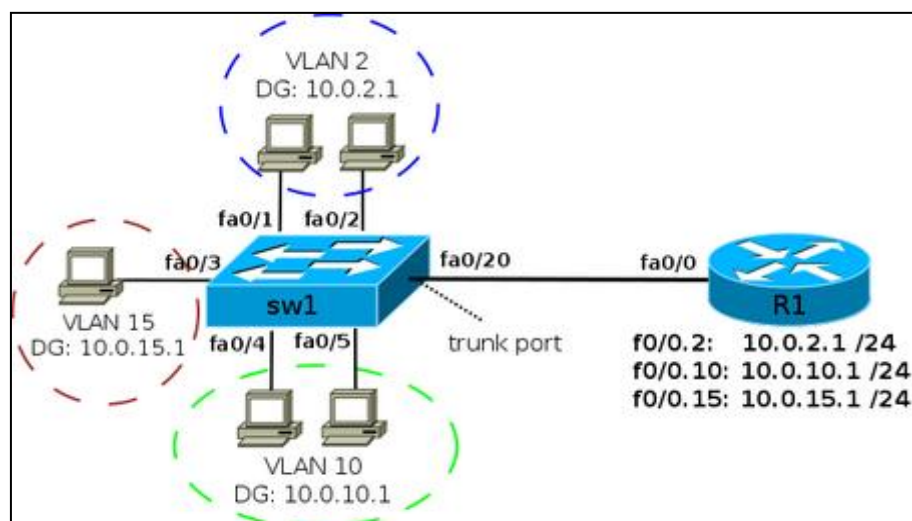


Рисунок 9.17 – Передача трафика между VLANами с помощью маршрутизатора

IP-адреса шлюза по умолчанию для VLAN (эти адреса назначаются на субинтерфейсах маршрутизатора R1) показаны в таблице 9.3.

Таблица 9.3 – IP-адреса шлюза по умолчанию для VLAN

VLAN	IP-адрес
VLAN 2	10.0.2.1 /24
VLAN 10	10.0.10.1 /24
VLAN 15	10.0.15.1 /24

Для логических субинтерфейсов необходимо указывать то, что интерфейс будет получать тегированный трафик и указывать номер VLAN соответствующий этому интерфейсу. Это задается командой в режиме настройки подинтерфейса *R1(config-if)# encapsulation dot1q «vlan-id»*. На рисунке 9.18 показаны команды для создания логических субинтерфейсов для VLAN 2, VLAN 10, VLAN 15:

```
R1(config)#interface fa0/0.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 10.0.2.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 10.0.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fa0/0.15
R1(config-subif)#encapsulation dot1q 15
R1(config-subif)#ip address 10.0.15.1 255.255.255.0
```

Рисунок 9.18 – Создание логических субинтерфейсов

Соответствие номера субинтерфейса и номера VLAN не является обязательным условием. Однако обычно номера субинтерфейсов задаются именно таким образом, чтобы упростить администрирование.

На коммутаторе порт, ведущий к маршрутизатору, должен быть настроен как статический транк (рисунок 9.19).

```
Sw1(config)#interface fa0/22
Sw1(config-if)#switchport mode trunk
```

Рисунок 9.19 – Настройка статического транка

## 9.2 Рабочее задание

- 1) В программе Packet Tracer создать схему сети, показанную на рисунке 9.20

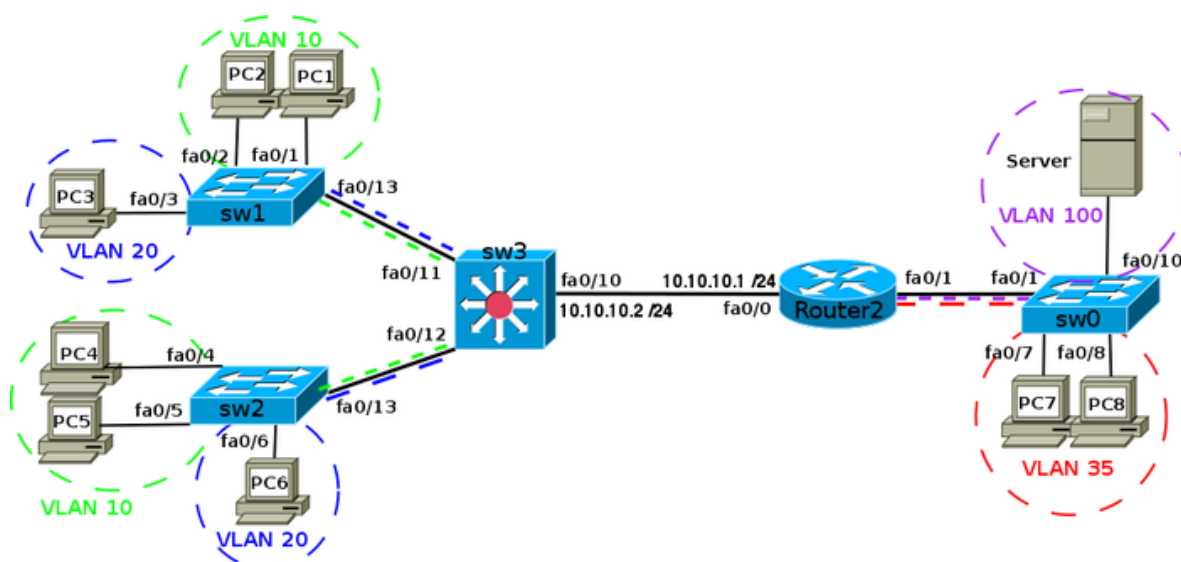


Рисунок 9.20 – Схема сети

Базовые настройки выполняются на коммутаторах sw1, sw2, sw3 и хостах PC1-PC6.

Настройки на коммутаторе sw0 будут выполняться в следующих заданиях.

IP-адреса хостов задаются таким образом:  $10.0.V.H /24$ , где V – номер VLAN, которому принадлежит хост, H – номер хоста

Таблица 9.4 – Таблица адресации

VLAN	Подсеть	Хосты в VLAN
VLAN 10	10.0.10.0 /24	PC1, PC2, PC4, PC5
VLAN 20	10.0.20.0 /24	PC3, PC6

2) Настроить access-порты и назначить их в VLAN согласно заданию и схеме. Проверить, что компьютеры в одном VLAN в пределах одного коммутатора пингуют друг друга (например, PC1 и PC2 или PC4 и PC5).

3) Настроить динамический trunk между коммутаторами sw1 и sw3.

В зависимости от модели коммутатора, порты могут быть по умолчанию в статусе dynamic desirable или dynamic auto (проверить можно командой `sh int fa0/10 switchport`)

Проверить, что trunk поднялся (команда `sh int trunk`)

Настроить статический trunk между коммутаторами sw2 и sw3.

Если появилась ошибка об инкапсуляции, то необходимо сначала соответственно настроить инкапсуляцию

Проверить, что trunk поднялся (команда `sh int trunk`)

Проверить, что на коммутаторе sw3 есть все необходимые VLAN, что все они в состоянии active и есть в соответствующих транках (команда `sh int trunk`)

Убедиться, что компьютеры в одном и том же VLAN должны пингуют друг друга

- PC1, PC2, PC4, PC5

- PC3, PC6

9) Настроить маршрутизацию между VLAN на маршрутизаторе.

Настройки выполняются на коммутаторе sw0, маршрутизаторе Router 2 и хостах PC7, PC8, Server.

VLAN	Подсеть	Хосты в VLAN	IP-адрес шлюза по умолчанию
VLAN 100	10.0.100.0 /24	Server	10.0.100.100
VLAN 35	10.0.35.0 /24	PC7, PC8	10.0.35.100

IP-адреса хостов задаются таким образом:  $10.0.V.H /24$ , где V – номер VLAN, которому принадлежит хост, H – номер хоста

IP-адрес сервера 10.0.100.10/24

Настроить access-порты на коммутаторе sw0:

- Настроить access-порты и назначить их в VLAN согласно заданию и схеме.

- Проверить, что компьютеры PC7 и PC8 пингуют друг друга

- Сервер поместить в VLAN 100. IP-адрес сервера 10.0.100.10/24

10) Настроить маршрутизацию между VLAN:

- На коммутаторе sw0 настроить на интерфейсе, который ведет к маршрутизатору Router2 статический транк.

- На маршрутизаторе, на интерфейсе, который ведет к коммутатору sw0, настроить подынтерфейсы для VLAN 35 и VLAN 100: задать на них IP-адреса из соответствующих VLAN, четвертый октет .100. Эти адреса будут шлюзами по умолчанию для хостов и сервера

- Проверить, что хосты PC7 и PC8 пингуют друг друга и сервер.

11) Настроить маршрутизацию между VLAN на коммутаторе

Настройки выполняются на коммутаторе sw3 и хостах PC1-PC6.

VLAN	Подсеть	Хосты в VLAN	IP-адрес шлюза по умолчанию
VLAN 10	10.0.10.0 /24	PC1, PC2, PC4, PC5	10.0.10.100
VLAN 20	10.0.20.0 /24	PC3, PC6	10.0.20.100

- Включить на коммутаторе sw3 маршрутизацию

- На коммутаторе sw3 настроить interface vlan для VLAN'ов 10 и 20

- На хостах указать адрес, назначенный на соответствующем interface vlan как шлюз по умолчанию.

- Проверить маршрутизацию между VLAN 10 и 20.

12) Переключить порт коммутатора в режим работы на 3 уровне

- На коммутаторе sw3 перевести порт, который ведет к маршрутизатору, в режим 3го уровня

- Настроить на коммутаторе, на интерфейсе 3го уровня IP-адрес 10.10.10.2/24, а на маршрутизаторе адрес 10.10.10.1/24

13) Настроить статические маршруты

- Прописать на коммутаторе статический маршрут по умолчанию указывающий на маршрутизатор.

- Добавить необходимые статические маршруты на маршрутизаторе, чтобы хосты с левой части сети, пинговали хосты с правой части сети.

14) Убедиться, что все хосты могут пинговать друг друга и что настроены все указанные функции.

## **10 Лабораторная работа №10. Общие сведения об VoIP**

### **10.1 Краткие теоретические положения**

VoIP (сокращённое от "Voice over Internet Protocol") в вольном переводе на русский означает "передачу голоса через Интернет". Впрочем, сам голос никуда не



передается: вся информация в Интернет транслируется только в цифровом виде. Поэтому формулировка "голос через IP" не совсем точна: передаётся не сам голос, а результаты его дробления на цифровые пакеты.

VoIP (Voice over Internet Protocol) или IP-телефония – это технология, которая обеспечивает передачу голоса в сетях с пакетной коммутацией по протоколу IP, частным случаем которых являются сети Интернет, а также другие IP-сети (например, выделенные цифровые каналы). Для связи сети Интернет (IP-сети) с телефонной сетью общего пользования PSTN (Public Switched Telephone Network), которая относится к глобальным сетям с коммутацией каналов, используются специальные аналоговые VoIP-шлюзы.

Необходимо отметить, что сети Интернет через цифровые шлюзы VoIP связаны с цифровыми телефонными сетями ISDN (Integrated Services Digital Network). Кроме того, интеграция VoIP в сети сотовой связи является практически неизбежным процессом, интеграция обеспечит более низкую по сравнению с традиционной сотовой телефонией стоимость разговоров.

На сегодняшний день доступ в Интернет возможен непосредственно с мобильных телефонов, которые поддерживают технологии: CSD (Circuit Switched Data или GSM Data), GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for Global Evolution), CDMA (Code Division Multiple Access), EV-DO (Evolution-Data Optimized), которые обеспечивают широкий спектр услуг "Мобильный Интернет" и WAP. Необходимо отметить, что в мобильной связи уже внедряются новые технологии беспроводного широкополосного доступа в Интернет на базе технологии связи 4G (GSM/WiMAX/Wi-Fi mobile phone).

В настоящее время к сетям PSTN и ISDN подключены центры коммутации сотовой связи (сотовые сети разных операторов соединены между собой), что обеспечивает звонки с сотовых телефонов на стационарные телефоны (PSTN или ISDN) и наоборот. Характерным для сетей 3G мобильной связи является скоростная беспроводная передача данных и мощные магистральные сети пакетной коммутации. В связи с тем, что сети PSTN связаны с сетями Интернет и сетями

сотовой связи, может быть обеспечена передача голосовых сигналов между этими сетями.

Голосовой сигнал из канала VoIP может непосредственно поступать на IP-телефон, подключенный к IP-сети или маршрутизироваться на мобильный телефон мобильного оператора, или на аналоговый телефон, подключенный к обычной телефонной сети PSTN, или на цифровой телефонный аппарат, подключенный к цифровой сети с интеграцией услуг ISDN.

Таким образом, IP-телефония обеспечивает передачу голосовых сигналов с компьютера на компьютер, с компьютера на телефон (аналоговый телефон, цифровой телефон, IP-телефон, мобильный телефон) и с телефона на телефон. Звонки осуществляются через провайдера услуг VOIP. Качество передачи голоса зависит от VoIP-провайдера и способа подключения к Интернету.

Одно из преимуществ IP-телефонии – это экономия финансовых средств на ведение международных и междугородних телефонных переговоров за счет того, что значительную часть расстояния между абонентами голосовой сигнал в цифровом виде (в сжатом состоянии) проходит по сетям пакетной коммутации (по сети Интернет), а не по телефонным сетям с коммутацией каналов. В настоящее время IP-телефония обеспечивает самые дешевые или бесплатные междугородние и международные звонки необходимо только оплатить использованный трафик Интернет-провайдеру.

Высокая стоимость передачи голоса в сетях PSTN объясняется тем, что эти сети имеют низкий коэффициент использования коммутируемых каналов. Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи голоса между АТС на время ведения переговоров двух абонентов. Во время пауз в процессе разговора составной физической канал не несет никакой полезной нагрузки, но эти паузы оплачиваются абонентами.

Сети с пакетной коммутацией эффективно используют сеть, так как пакеты передаются по разделяемой среде (общему для всех разговоров каналу передачи данных). Коммутация пакетов – это коммутация сообщений, представляемых в

виде адресуемых пакетов, когда канал передачи данных занят только во время передачи пакета и по ее завершению освобождается для передачи других пакетов. Таким образом, паузы в IP-сетях не оплачиваются, поэтому передача голоса по IP-сетям дешевле, чем по сетям PSTN.

Ведение международных и междугородних телефонных переговоров значительно экономят финансовые средства, как частных лиц, так и компаний. Но основное преимущество технологии VoIP для компаний – это создание систем корпоративной или офисной IP-телефонии с малыми финансовыми затратами, но с большим количеством сервисных функций VoIP. Системы офисной IP-телефонии называются IP PBX или IP АТС, или Soft PBX, или программные АТС, или VoIP мини-АТС, которые являются учрежденческой АТС-УАТС, т.е. телефонной системой для частного пользования.

В настоящее время существуют следующие VoIP-сервисы:

- IP-телефония по карточкам, которые продаются в магазинах для звонков с обычного телефона;

- компьютерная VoIP (IP-телефония), в которой используется специальная программа, работающая на ПК (программный телефон VoIP);

- телефонная VoIP (IP-телефония), в которой обычный телефонный аппарат подключается к специальному адаптеру, имеющему выход в Интернет или в которой IP-телефоны (аппаратные VoIP телефоны) подключаются к Интернет через провайдера.

Типы IP-телефонов

- 1) Программные телефоны (софтфоны) – это программы-клиенты, которые имитирует телефон на компьютере, позволяющие совершать и принимать телефонные звонки при помощи ПК. Для звонков через софтфон необходимо подключить к ПК микрофон и динамики (наушники с микрофоном) или использовать USB телефон. Софтфон бесплатно скачивают с сайтов провайдеров IP-телефонии и устанавливают на свой ПК, затем регистрируются на сайте провайдера IP-телефонии, далее пополняют счет и пользуются различными VoIP-услугами.

2) К программным телефонам относятся и двухрежимные GSM/WiFi (сотовый/VoIP) мобильные телефоны, которые могут работать одновременно в GSM и WiFi сетях. В сетях GSM эти телефоны работают как обычные мобильные телефоны, а в зоне действия точек доступа WiFi двухрежимные телефоны с клиентскими программами для VoIP-сервисов могут использовать IP телефонию. Работа в режиме IP телефонии значительно дешевле, чем работа в сетях GSM, этот режим позволяет значительно снизить расходы на роуминг, т.е. он становится практически бесплатным. В телефоне Nokia N80 Internet Edition реализована поддержка сетей WLAN (802.11g), т.е. Wi-Fi и встроен VoIP-клиент (SIP-клиент), что обеспечивает возможность пользоваться IP телефонией в зоне действия точек доступа WiFi.

3) USB VOIP телефоны (проводные и беспроводные USB-телефоны) заменяют собой микрофон и наушники. Эти телефоны обеспечивают возможность совершать и принимать звонки через Интернет с помощью ПК и установленного на нем специального программного обеспечения SoftPhone, например, Skype, SIP (SIPNET), MSN Messenger, NetMeeting и т.д. Для выполнения звонков необходимо включить USB VoIP Телефон в USB порт компьютера. Например, USB телефон для IP-телефонии "Skypemate USB-P10D" позволяет использовать Skype и SIP при звонках через Интернет. При этом для работы с провайдерами Skype или SIP-телефонии требуется установка одного из драйверов – Skypemate для Skype или X-TenMate для SIP и программы-клиента (SoftPhone) на ПК.

4) IP-телефоны. Это телефонные аппараты, которые подключаются к Интернет через Интернет-провайдера, далее осуществляется регистрация на сайте одного из провайдеров IP-телефонии. После получения логина и пароля, активизируется аккаунт на сайте провайдера IP-телефонии, при условии пополнения счета на определенную сумму. Затем можно пользоваться различными VoIP-услугами. VoIP телефоны бывают проводные (Ethernet), беспроводные (Wi-Fi / 802.11) и IP-телефоны для Dial-Up (со встроенным аналоговым модемом).

5) аналоговые телефоны, подключенные к Интернет при помощи аналогового телефонного адаптера (VoIP АТА). VoIP АТА позволяют превратить обычные телефонные аппараты в IP телефоны.

## 10.2 Рабочее задание

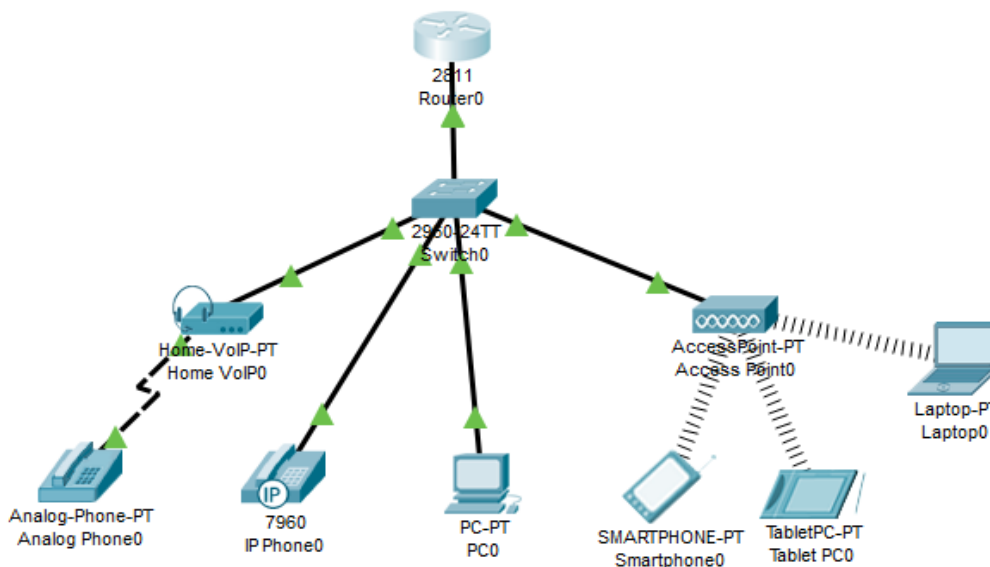


Рисунок 10.1 – Схема сети

### 1) Соберите схему сети в соответствии с рисунком 10.1.

Для этого используйте следующие устройства:

- а) Маршрутизатор 2811 (он будет являться DHCP сервером, VoIP шлюзом и TFTP сервером)
- б) Коммутатор 2960 (к нему будут подключены все устройства)
- в) Аналоговый телефон (который будет подключен к коммутатору через шлюз)
- г) IP телефон 7960
- д) Клиентский компьютер (который будет работать при помощи ПО Cisco IP Communicator - CIPC)
- е) Wi-Fi точка (для подключения к сети беспроводных устройств)
- ж) Ноутбук, планшетный компьютер и смартфон (данные устройства будут подключаться к Wi-Fi точке и работать через CIPC)

*Примечание.* Для подключения IP-телефона к коммутатору необходимо в настройках IP-телефона подключить адаптер питания VoIP (рисунок 10.2).

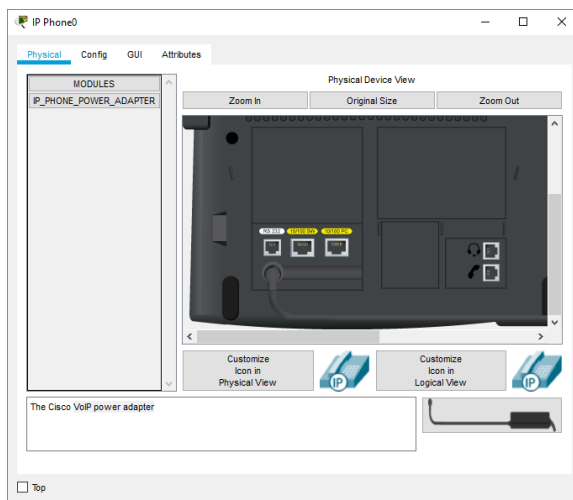


Рисунок 10.2 – Подключение адаптера питания IP-телефона

Для подключения ноутбука к точке доступа необходимо добавить ему модуль Linksys-WPC300N (рисунок 10.3).

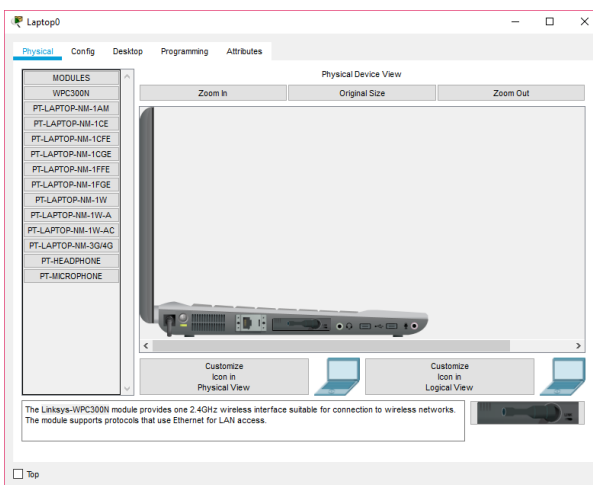


Рисунок 10.3 – Подключение модуля Linksys-WPC300N ноутбука

**2) Заполните таблицу MAC-адресов устройств, по аналогии с примером в таблице 10.1**

Таблица 10.1 – Пример MAC-адресов устройств

Устройство	MAC-адрес
Шлюз аналогового телефона	00E0.F9C2.C101

IP-телефон	000A.4159.278A
ПК	00E0.F915.A246
Смартфон	00E0.8F56.D1B2
Планшет	00D0.BA54.2803
Ноутбук	00D0.FF65.AC8D

*Примечание.*

Для компьютеров и других устройств (не телефонов), есть несколько способов узнать MAC-адрес. Например, зайти в командную строку устройства и набрать `ipconfig /all` или зайти на вкладку `config` и скопировать в буфер MAC-адрес соответствующего интерфейса. Один из способов узнать MAC-адрес телефона – это навести мышкой на устройство, и запомнить его MAC-адрес. Так же можно воспользоваться командой `show mac address-table [interface fa0/X]` на коммутаторе (рисунок 10.4).

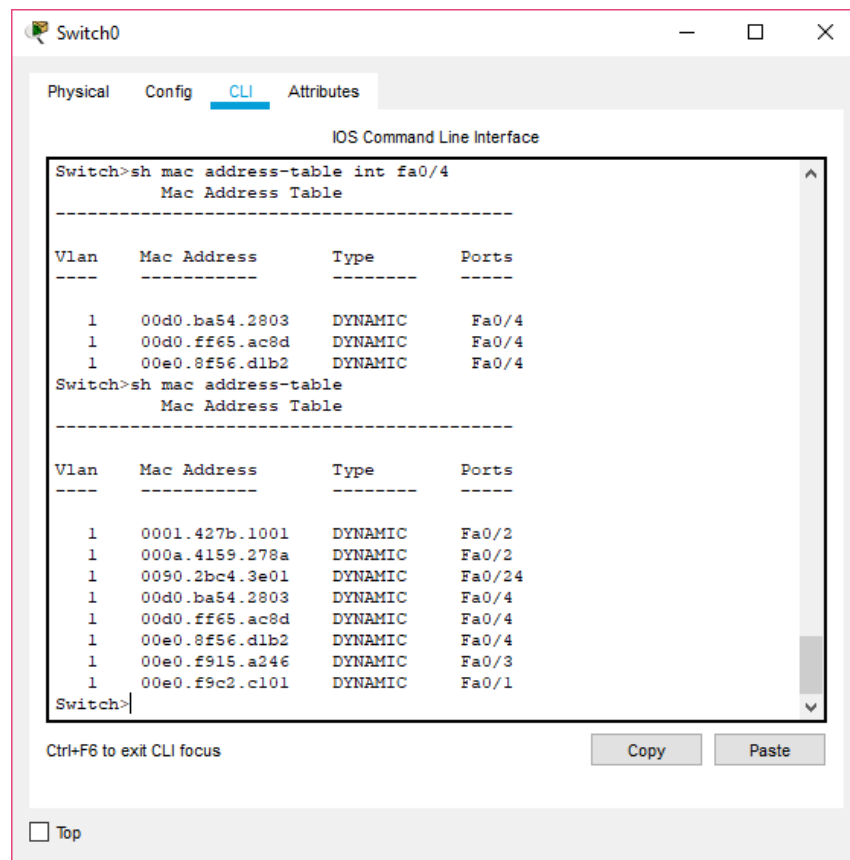


Рисунок 10.4 – Просмотр таблицы MAC-адресов устройств на коммутаторе

### 3) Настройте маршрутизатор в соответствии с таблицей вариантов:

1) Назначьте IP-адрес на интерфейс

```
interface FastEthernet0/0
ip address 10.3.0.1 255.255.255.0
no shutdown
```

2) Настройте DHCP, заранее исключив из выдачи адрес, статически присвоенный интерфейсу

```
ip dhcp excluded-address 10.3.0.1
ip dhcp pool Telephony
network 10.3.0.0 255.255.255.0 //анонсируем сеть
default-router 10.3.0.1 //указываем основной шлюз
option 150 ip 10.3.0.1 //указываем tftp сервер
```

3) Поднимите телефонный сервис и настройте на нем количество телефонов и количество линий (несмотря на то, что устройств в схеме 6, укажите количество с запасом)

```
telephony-service // поднимаем СМЕ
max-ephones 10 //указываем кол-во телефонов
max-dn 10 //указываем кол-во линий
ip source-address 10.3.0.1 port 2000 //указываем с какого интерфейса
он будет принимать звонки
auto assign 1 to 10 //назначаем автоматическое
присвоение линий от 1 до 10
```

4) Настройте линии

```
ephone-dn 1 //создаем линию
number 101 //присваиваем ей номер
ephone-dn 2 //создаем линию
number 102 //присваиваем ей номер
```

Аналогично создайте еще 4 линии. Пример выполнения пунктов 1-4 настройки маршрутизатора показан на рисунке 10.5.



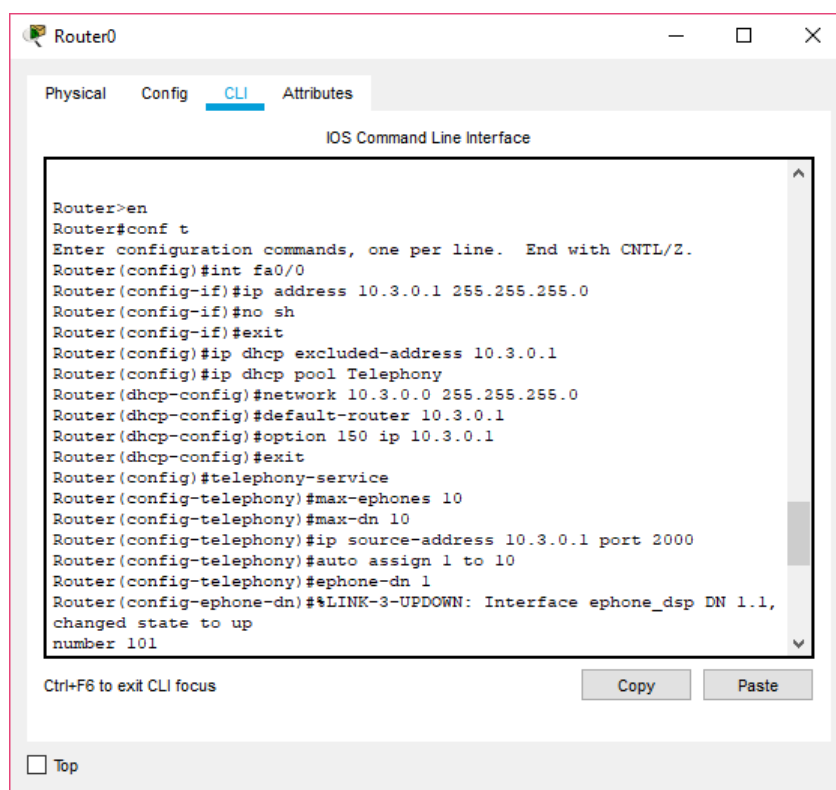


Рисунок 10.5 – Настройка маршрутизатора

5) Создайте телефоны и привяжите определенный номер к MAC-адресу устройства (рисунок 6)

```

ephone 1 //для аналогового телефона
mac-address 00E0.F9C2.C101 //MAC-адрес шлюза аналогового телефона
type ata //указывает, что телефон аналоговый
button 1:1 //привязывает данный телефон к первому номеру, т.е. 101

```

```

ephone 2 //для ip-телефона
mac-address 0001.63EB.ED01 //MAC-адрес ip-телефона
type 7960 //указывает, тип устройства cisco 7960
button 1:2 //привязывает данный телефон ко второму номеру, то есть 102

```

```

ephone 3 //для компьютера

```

*mac-address 00E0.F915.A246*

*type CIPC*

*//указывает, что будет использоваться программа CIPC*

*button 1:3*

*ephone 4*

*//для смартфона*

*mac-address 00E0.8F56.D1B2*

*type CIPC*

*button 1:4*

*ephone 5*

*//для планшета*

*mac-address 00D0.BA54.2803*

*type CIPC*

*button 1:5*

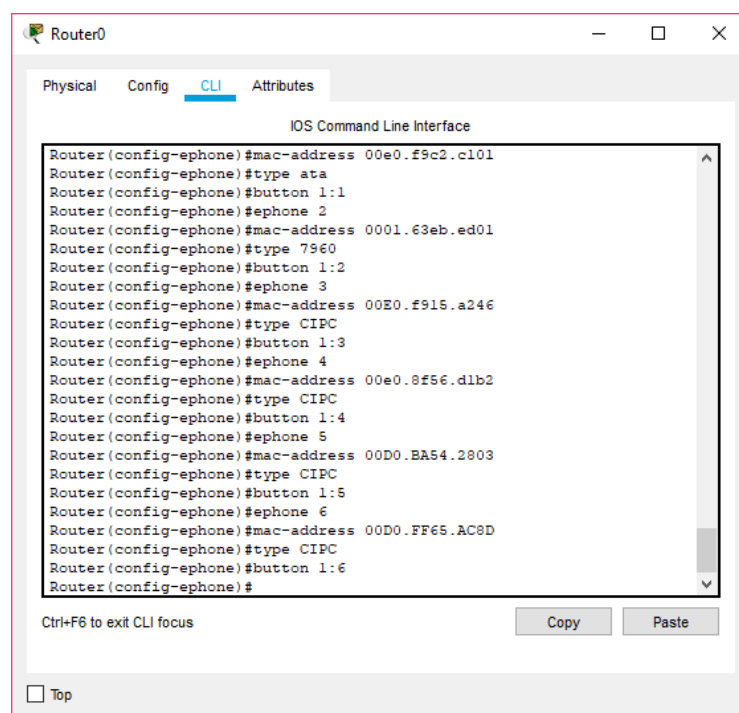
*ephone 6*

*//для ноутбука*

*mac-address 00D0.FF65.AC8D*

*type CIPC*

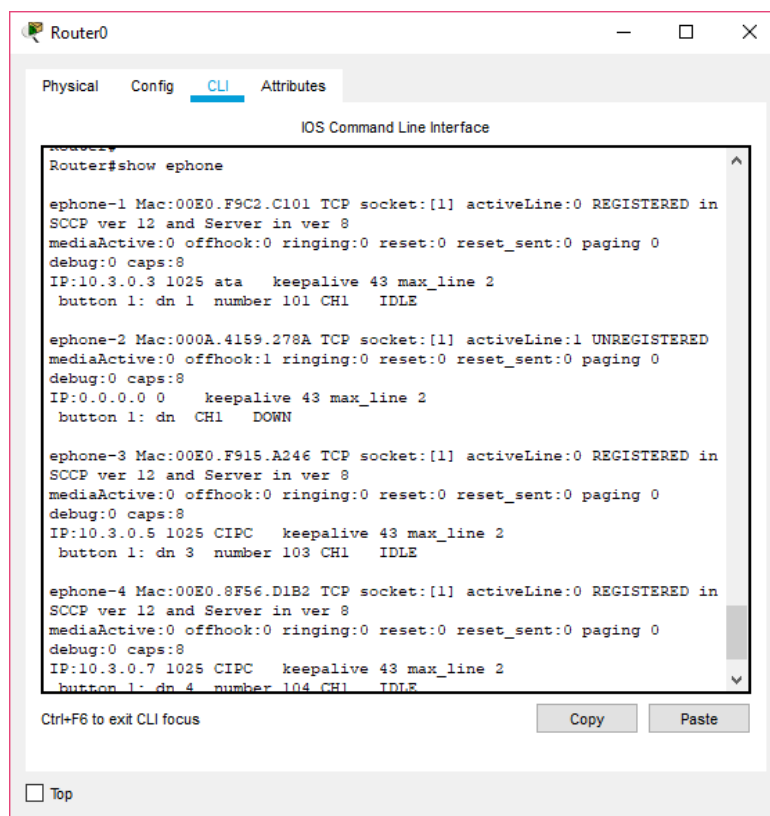
*button 1:6*



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-ephone)#mac-address 00e0.f9c2.c101
Router(config-ephone)#type ata
Router(config-ephone)#button 1:1
Router(config-ephone)#ephone 2
Router(config-ephone)#mac-address 0001.63eb.ed01
Router(config-ephone)#type 7960
Router(config-ephone)#button 1:2
Router(config-ephone)#ephone 3
Router(config-ephone)#mac-address 00E0.f915.a246
Router(config-ephone)#type CIPC
Router(config-ephone)#button 1:3
Router(config-ephone)#ephone 4
Router(config-ephone)#mac-address 00e0.8f56.d1b2
Router(config-ephone)#type CIPC
Router(config-ephone)#button 1:4
Router(config-ephone)#ephone 5
Router(config-ephone)#mac-address 00D0.BA54.2803
Router(config-ephone)#type CIPC
Router(config-ephone)#button 1:5
Router(config-ephone)#ephone 6
Router(config-ephone)#mac-address 00D0.FF65.AC8D
Router(config-ephone)#type CIPC
Router(config-ephone)#button 1:6
Router(config-ephone)#
```

## Рисунок 10.6 – Настройка номеров

Просмотреть информацию об устройствах, подключенных к телефонной линии, можно с помощью команды *show ephone* (рисунок 10.7)



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router#show ephone

ephone-1 Mac:00E0.F9C2.C101 TCP socket:[1] activeLine:0 REGISTERED in
SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:10.3.0.3 1025 ata keepalive 43 max_line 2
button 1: dn 1 number 101 CH1 IDLE

ephone-2 Mac:000A.4159.278A TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:0.0.0.0 0 keepalive 43 max_line 2
button 1: dn CH1 DOWN

ephone-3 Mac:00E0.F915.A246 TCP socket:[1] activeLine:0 REGISTERED in
SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:10.3.0.5 1025 CIPC keepalive 43 max_line 2
button 1: dn 3 number 103 CH1 IDLE

ephone-4 Mac:00E0.8F56.D1B2 TCP socket:[1] activeLine:0 REGISTERED in
SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:10.3.0.7 1025 CIPC keepalive 43 max_line 2
button 1: dn 4 number 104 CH1 IDLE

Ctrl+F6 to exit CLI focus Copy Paste
Top
```

Рисунок 10.7 – Результат выполнения команды *show ephone*

4) Настройте коммутатор:

1) Переведите 4 порта коммутатора, которые смотрят на наши устройства, в голосовой VLAN

```
interface FastEthernet0/1
```

```
switchport voice vlan 1
```

```
exit
```

```
interface FastEthernet0/2
```

```
switchport voice vlan 1
```

```
exit
```

```
interface FastEthernet0/3
```

```
switchport voice vlan 1
exit
interface FastEthernet0/4
switchport voice vlan 1
```

## 5) Настройте VoIP шлюз аналогового телефона:

Так как данный аналоговый телефон не умеет работать с IP адресами, но ему надо получить номер, он подключается к сети при помощи шлюза. Для корректной работы, шлюзу нужно прописать адрес сервера, куда обращаться (рисунок 10.8).

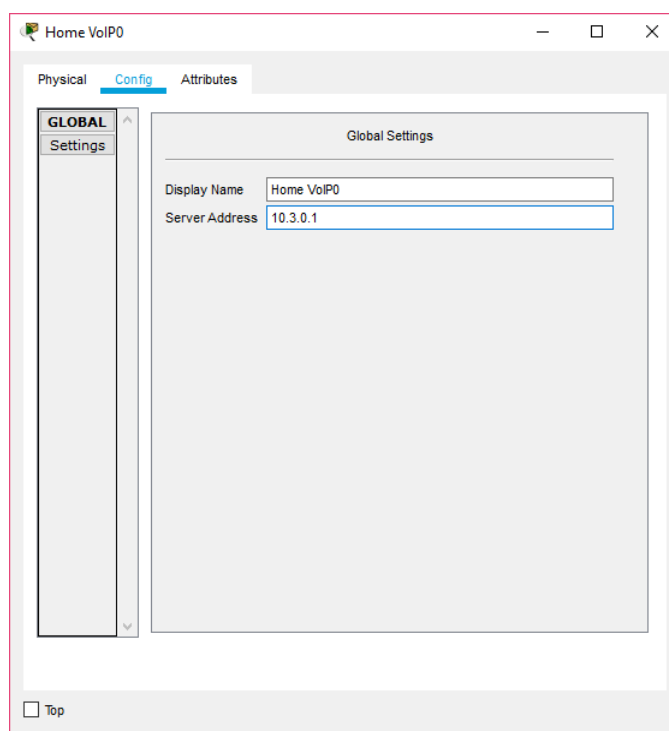


Рисунок 10.8 – Настройка VoIP шлюз аналогового телефона

## 6) Настройте Wi-Fi

Так как на используемых переносных устройствах нет Ethernet портов, то работать они будут при помощи Wi-Fi точки, соединенной с общей сетью. Подключите точку к коммутатору и зайдите в ее настройки.

На вкладке Config - Port 1 выполните настройку в соответствии с рисунком 10.9:

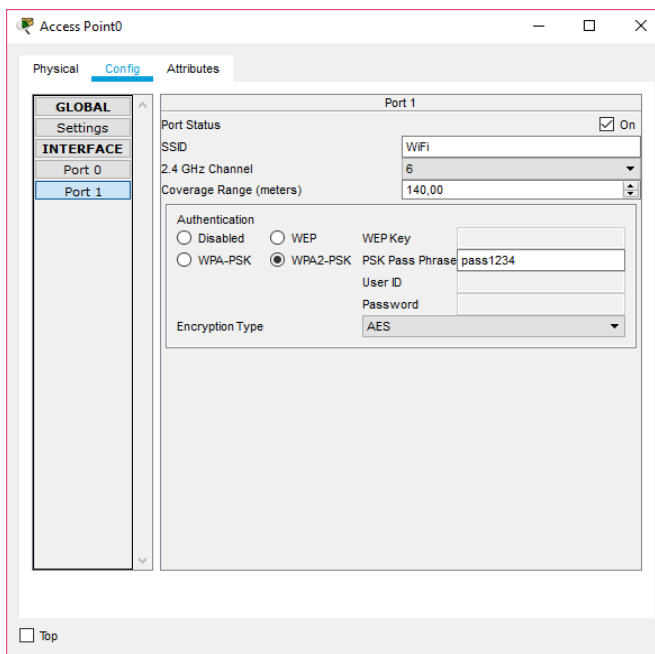


Рисунок 10.9 – Настройка точки доступа

Теперь введите эти данные на устройствах, которые будут подключаться по Wi-Fi. Например, для настройки Wi-Fi на смартфоне перейдите на вкладку Config - Wireless0 и выполните настройку в соответствии с рисунком 10.10.

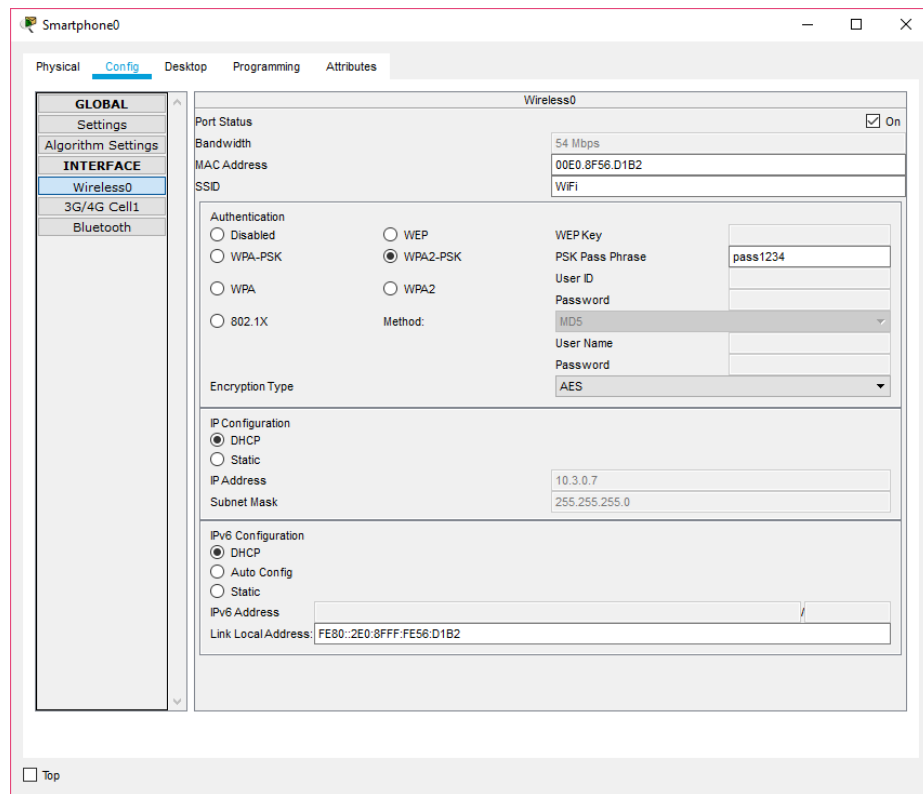


Рисунок 10.10 – Настройка смартфона

Убедитесь, что галочка напротив port status стоит в положение On, и в поле IP Configuration выбрано DHCP.

**7) Получите адреса и настройте SIPС на устройствах.** На данном этапе телефоны уже должны зарегистрироваться и получить номера (во вкладке GUI, в правом верхнем углу должен появиться номер полученного телефона). На рисунке 10.11 показан GUI аналогово телефона, где в правом верхнем углу дисплея виден номер 101.

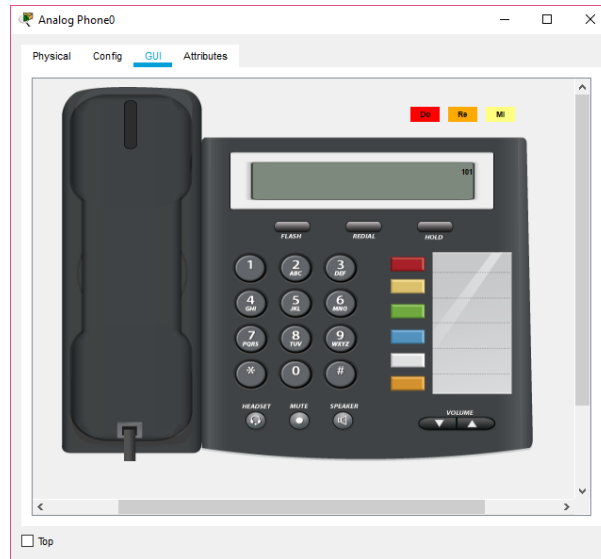


Рисунок 10.11 – GUI аналогово телефона

Аналогично можно убедиться в готовности IP-телефона.

Перейдем к другим устройствам. После того как все устройства получают IP-адреса, перейдите на вкладку Desktop и выберите Cisco IP Communicator. После этого в правом верхнем углу видно, что номер присвоен. На рисунке 10.12 показан присвоенный компьютеру номер.

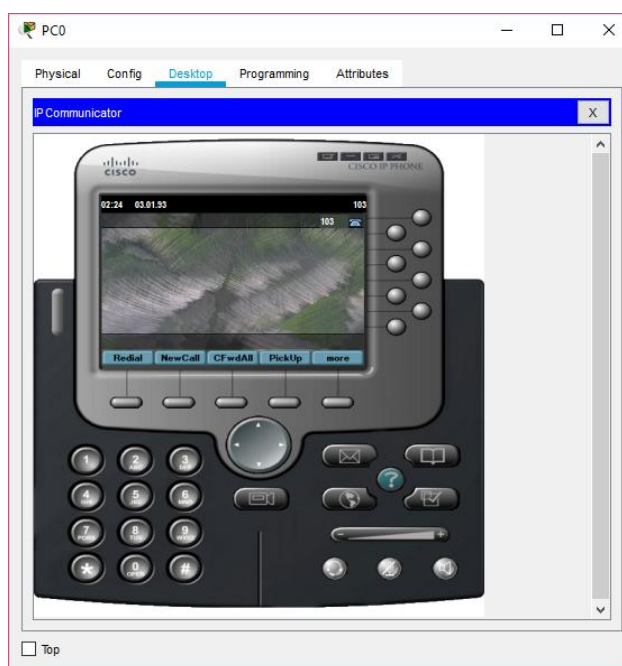


Рисунок 10.12 – Номер ПК

Как видно, все устройства получили номера согласно резервациям на маршрутизаторе.

### 8) Проверьте работоспособность:

Организируйте звонок с планшетного компьютера на обычный аналоговый телефон и наоборот, а также с аналогового телефона на ip телефон и обратно.

Совершите звонок с аналогового телефона (номер 101) на планшет (номер 105) и убедитесь, что соединение установлено и возможен разговор (рисунок 10.13).

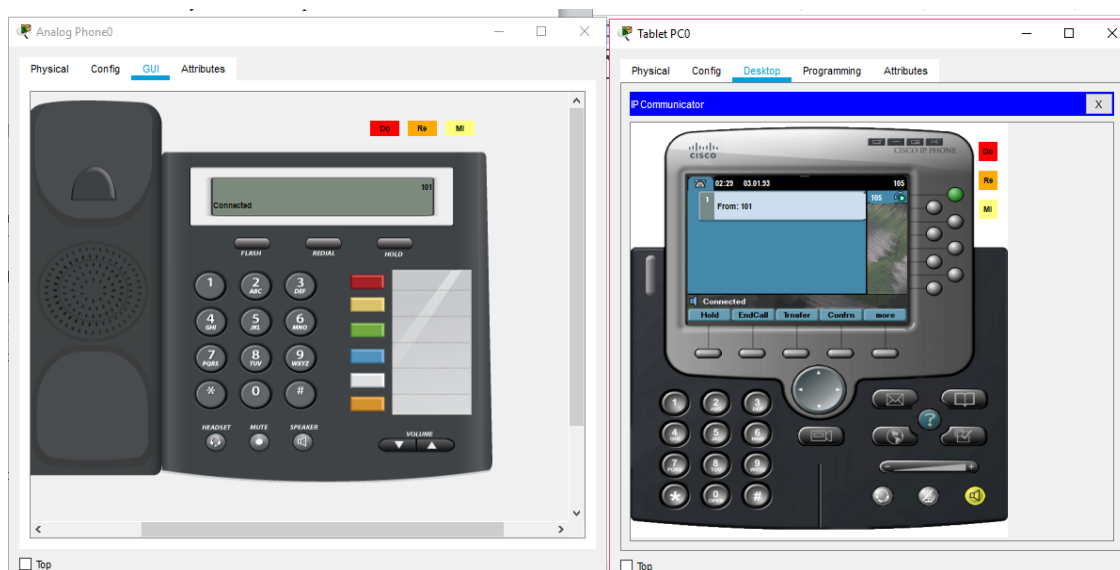


Рисунок 10.13 – Звонок с аналогового телефона на планшет

Совершите звонок с планшета на аналоговый телефон и убедитесь, что соединение установлено и возможен разговор.

Совершите звонки с участием остальных устройств, проверив таким образом работоспособность.

Таблица вариантов

Вариант	IP сеть
1	192.168.100.128/26
2	192.168.100.64/27
3	10.14.2.192/26



4	10.18.22.16/28
5	172.16.32.32/27
6	192.168.100.128/26
7	192.168.100.64/27
8	10.14.2.192/26
9	10.18.22.16/28
10	172.16.32.32/27

## **11 Лабораторная работа №11. Добавление устройств IoT в умную домашнюю сеть**

### **11.1 Краткие теоретические положения**

Интернет вещей (англ. *internet of things, IoT*) – концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключаяющее из части действий и операций необходимость участия человека [10].

Концепция сформулирована в 1999 году как осмысление перспектив широкого применения средств радиочастотной идентификации для взаимодействия физических предметов между собой и с внешним окружением. Наполнение концепции «интернета вещей» многообразным технологическим содержанием и внедрение практических решений для её реализации начиная с 2010-х годов считается устойчивой тенденцией в информационных технологиях, прежде всего, благодаря повсеместному распространению беспроводных сетей, появлению облачных вычислений, развитию технологий межмашинного взаимодействия, началу активного перехода на IPv6 и освоению программно-конфигурируемых сетей.

«Умный дом» – единая система управления в доме, офисе, квартире или здании, включающая в себя датчики, управляющие элементы и исполнительные устройства.

## 11.2 Рабочее задание

### 11.2.1 Изучение возможностей Packet Tracer для построения схемы интеллектуальной домашней сети

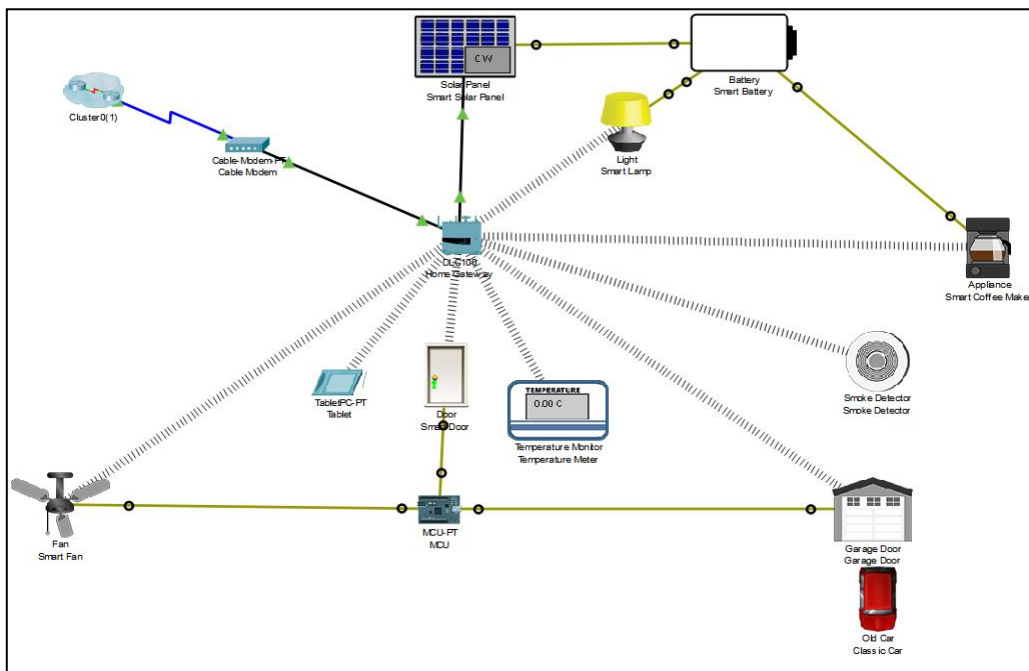


Рисунок 11.1 – Пример схемы сети «Умный дом»

Изучите возможности Packet Tracer для построения схемы интеллектуальной домашней сети.

В левом нижнем углу окна Packet Tracer найдите и щелкните значок «End Devices» в верхней строке и значок «Home» в нижней строке окна «Тип устройства» (рисунок 11.2).



Рисунок 11.2 – Выбор устройства

В нижней части окна Packet Tracer в поле «Выбор устройства» отображается множество различных устройств Smart Home IoT. Переместите указатель мыши на каждое устройство и обратите внимание, что описательное имя устройства отображается в нижней части окна «Выбор устройства». Посмотрите на каждый тип устройства.

Когда вы размещаете свой курсор над устройством в логической рабочей области, например Smoke Detector (датчик дыма), открывается информационное окно, содержащее основную сетевую информацию об этом устройстве.

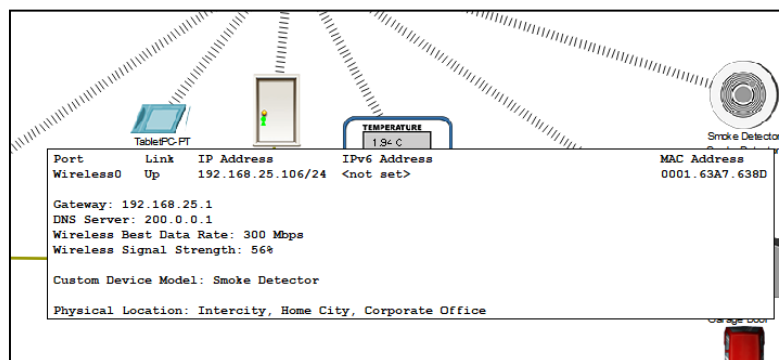


Рисунок 11.3 – Информационное окно устройства Smoke Detector

Чтобы включить или активировать устройство, удерживайте нажатой клавишу Alt на клавиатуре, а затем щелкните левой кнопкой мыши по устройству. Попробуйте это на каждом из умных устройств, чтобы наблюдать за тем, что они делают. Интеллектуальная домашняя сеть также состоит из инфраструктурных устройств, таких как домашний шлюз. Изучите устройство домашнего шлюза Home Gateway, добавив его на рабочую область. Щелкните значок Home Gateway, чтобы открыть окно настройки. Затем перейдите на вкладку «Config» и просмотрите настройки локальной сети (LAN) главного шлюза.

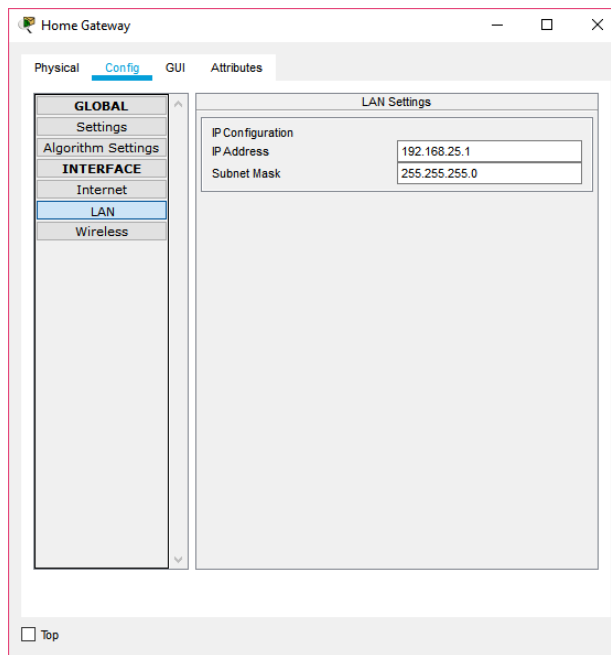


Рисунок 11.4 – Пример настройки локальной сети главного шлюза  
Посмотрите настройки беспроводной сети (Wireless) домашнего шлюза.

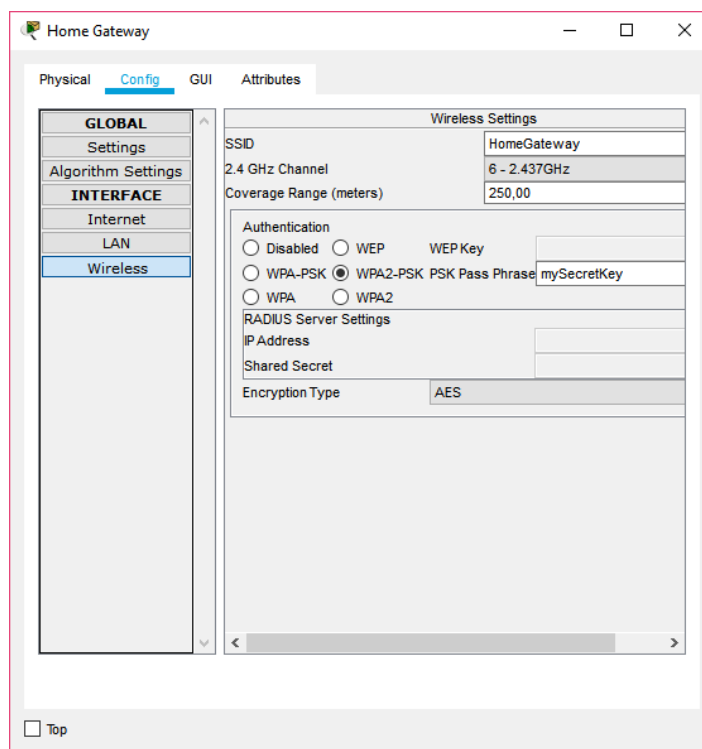


Рисунок 11.5 – Пример настройки беспроводной сети домашнего шлюза

#### 11.2.4 Согласование работы датчика движения и веб-камеры

Откройте в Packet Tracer новый файл. Соберите схему сети в соответствии с рисунком 11.6, используя следующие устройства: Motion Detector (датчик движения), Webcam (вебкамера), коммутатор и сервер.

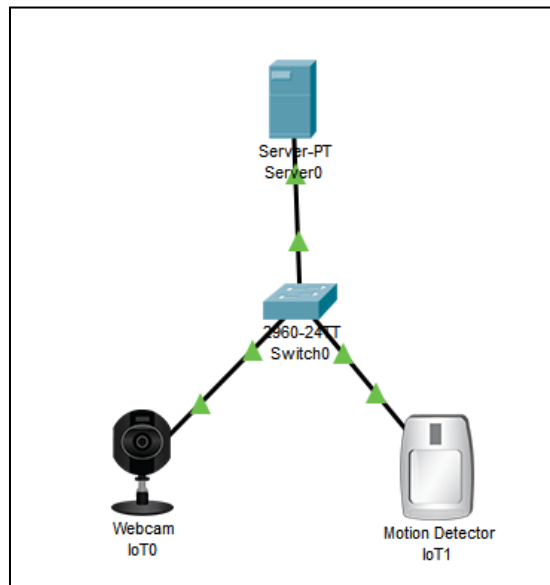


Рисунок 11.6 – Схема сети

Назначьте устройствам IP-адреса в соответствии с таблицей вариантов (например, сервер 192.168.0.1/24, веб-камера 192.168.0.2/24, датчик движения 192.168.0.3/24).

Таблица 11.1 – Параметры IP

Вариант	IP сеть
1	192.168.100.128/26
2	192.168.100.64/27
3	10.14.2.192/26
4	10.18.22.16/28
5	172.16.32.32/27
6	192.168.100.128/26
7	192.168.100.64/27
8	10.14.2.192/26
9	10.18.22.16/28
10	172.16.32.32/27

Для удобства дальнейшей работы переименуйте устройства IoT0 и IoT1 в Webcam и MotionDetector соответственно. Далее необходимо включить на сервере режим регистрации. Для этого на вкладке Services – IoT установите переключатель On (рисунок 11.7).

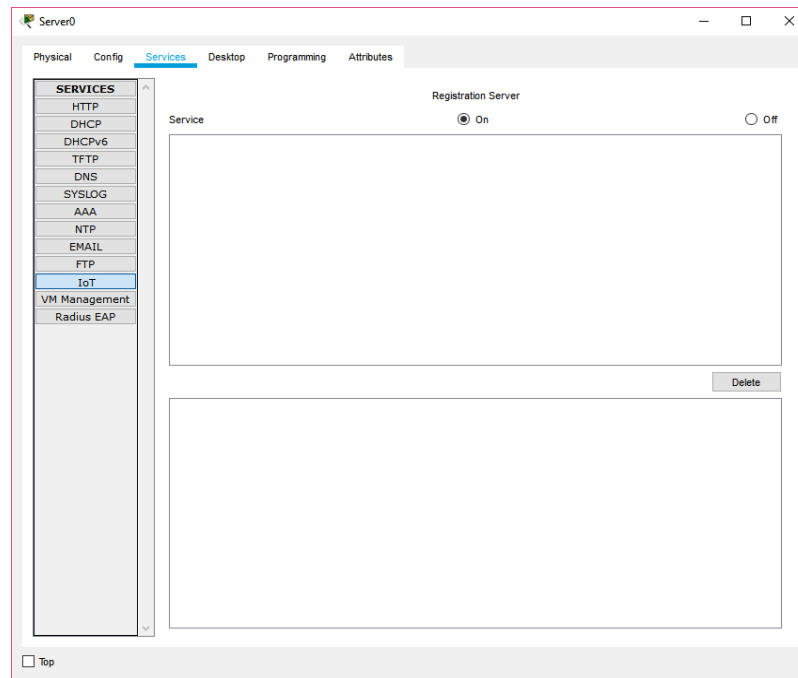


Рисунок 11.7 – Настройка сервера

Откройте веб-браузер и перейдите на страницу сервера, используя его IP-адрес (рисунок 11.8).

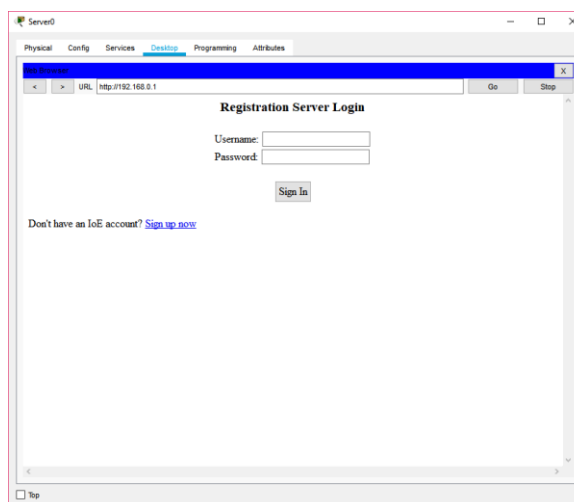


Рисунок 11.8 – Веб-браузер сервера

Создайте аккаунт ЮЕ с именем пользователя и паролем admin для управления подключенными интеллектуальными устройствами.

Для подключения к регистрационному серверу датчика движения и веб-камеры зайдите на вкладку Config окна настроек устройства, выберите Remote Server, задайте параметры сервера и нажмите кнопку Connect (рисунок 11.9).

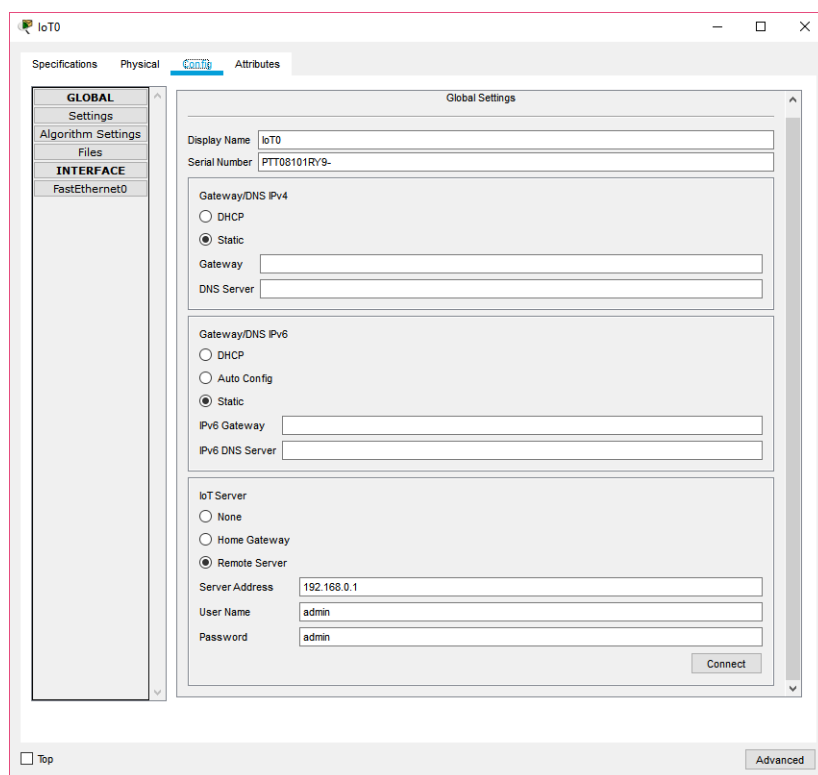


Рисунок 11.9 – Подключение устройства к серверу

При успешном подключении кнопка Connect заменится кнопкой Refresh. Кроме того, в веб-браузере сервера теперь можно увидеть список подключенных устройств (рисунок 11.10).

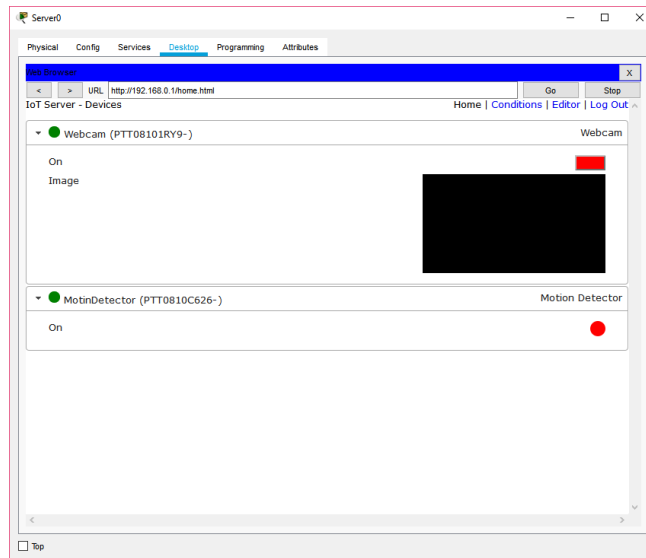


Рисунок 11.10 – Список подключенных устройств на сервере

Сейчас веб-камера и датчик движения работают независимо друг от друга. Для согласования работы этих двух устройств выполните следующие действия:

- в правом верхнем углу веб-браузера нажмите Condition
- нажмите кнопку Add, задайте правило, как показано на рисунке 11.11, и нажмите Ок.

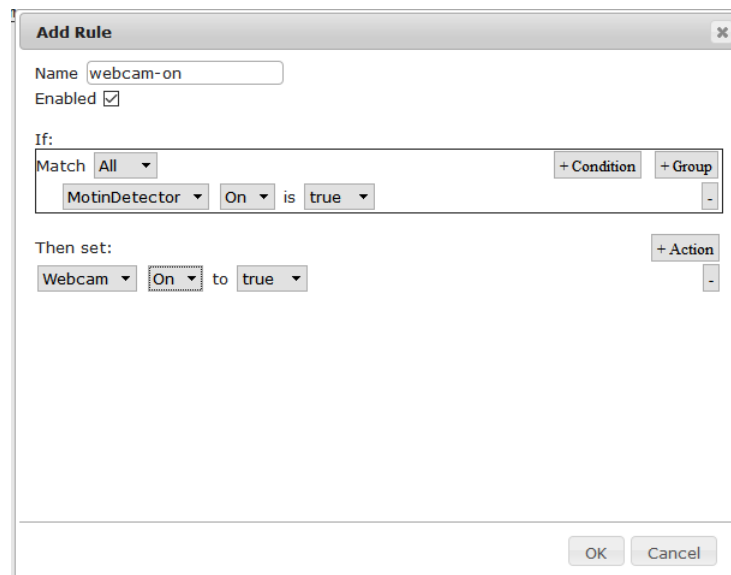


Рисунок 11.11 – Создание правила

- добавьте второе правило, согласно которому при выключенном датчике движения камера тоже будет выключена.



Для того чтобы убедиться, что настройки работают верно в рабочей области включите датчик движения с помощью кнопки alt. При этом в списке устройств на сервере будет отображена анимация (рисунок 11.12).

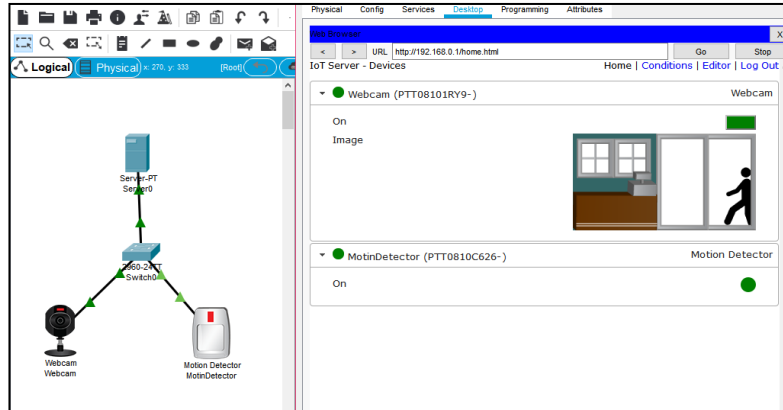


Рисунок 11.12 – Демонстрация связи камеры и датчика движения

## Список использованных источников

1. Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / Н.А. Олифер, В.Г. Олифер. – СПб.: Питер, 2019. – 992с.
2. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер, 2019. – 960с.
3. Букатов, А.А. Компьютерные сети. Расширенный начальный курс / А.А. Букатов, С.А. Гуда. – СПб.: Питер, 2019. – 496с.
4. Ушаков, И. Организация, принципы построения и функционирования компьютерных сетей: учебник / И. Ушаков, А. Красов, Н. Савинов. – Москва: Академия, 2019. – 240с.
5. Кутузов, О. Инфокоммуникационные системы и сети: учебник / О. Кутузов, Т. Татарникова, В. Цехановский. – СПб.: Лань, 2020. – 244с.
6. Баринов, В. Компьютерные сети: учебник / В. Баринов [и др.]. – Москва: Академия, 2020. – 192с.
7. Уэнделл, О. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-105 / О. Уэнделл. – Москва: Вильямс, 2017. – 1088с.
8. Меньшуткин, А. Справочник по настройке сетевого оборудования Cisco / А. Меньшуткин. – Москва: ЛитРес, 2020. – 282с.
9. Смирнова, Е.В. Технология современных беспроводных сетей Wi-Fi: учебное пособие / Е.В. Смирнова, А.В. Пролетарский. – Москва: Издательство МГТУ им. Н. Э. Баумана, 2017. – 448с.
10. Грингард, С. Интернет вещей. Будущее уже здесь / С. Грингард. – Альпина Паблишер, 2019. – 188с.