

Министерство образования Республики Беларусь  
Учреждение образования  
«Белорусский государственный университет  
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра защиты информации

**Е. С. Белоусова**

## **ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ**

*Рекомендовано УМО по образованию в области  
информатики и радиоэлектроники в качестве учебно-методического пособия  
для специальности 1-98 01 02 «Защита информации в телекоммуникациях»*

Минск БГУИР 2020

УДК 004.732(076.5)  
ББК 32.971.35я73  
Б43

Рецензенты:

кафедра телекоммуникационных систем  
учреждения образования «Белорусская государственная академия связи»  
(протокол №3 от 05.11.2019);

начальник научно-исследовательской лаборатории  
кафедры автоматизированных систем управления войсками  
учреждения образования «Военная академия Республики Беларусь»  
кандидат технических наук, доцент А. В. Хижняк

**Белоусова, Е. С.**

Б43 Основы построения локальных сетей. Лабораторный практикум : учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2020. – 103 с. : ил.  
ISBN 978-985-543-562-5.

Состоит из восьми лабораторных работ, содержащих краткие теоретические сведения, описание хода выполнения лабораторного задания, вопросы для самоконтроля, ответы на которые оцениваются программной экспертной системой.

Предназначено для студентов, изучающих дисциплину «Компьютерные сети».

**УДК 004.732(076.5)**  
**ББК 32.971.35я73**

**ISBN 978-985-543-562-5**

© Белоусова Е. С., 2020  
© УО «Белорусский государственный университет информатики и радиоэлектроники», 2020

## СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1 ОСНОВЫ СОЗДАНИЯ ЛОКАЛЬНЫХ СЕТЕЙ...	5
1.1 Теоретическая часть .....	5
1.2 Лабораторное задание .....	11
1.3 Содержание отчета .....	18
1.4 Контрольные вопросы и задания.....	18
ЛАБОРАТОРНАЯ РАБОТА №2 МОДЕЛЬ OSI.....	19
2.1 Теоретическая часть .....	19
2.2 Лабораторное задание .....	26
2.3 Содержание отчета .....	28
2.4 Контрольные вопросы и задания.....	28
ЛАБОРАТОРНАЯ РАБОТА №3 НАСТРОЙКА КОММУТАТОРА .....	29
3.1 Теоретическая часть .....	29
3.2 Лабораторное задание .....	37
3.3 Содержание отчета .....	39
3.4 Контрольные вопросы и задания.....	39
ЛАБОРАТОРНАЯ РАБОТА №4 БАЗОВАЯ НАСТРОЙКА МАРШРУТИЗАТОРА .....	40
4.1 Теоретическая часть .....	40
4.2 Лабораторное задание .....	52
4.3 Содержание отчета .....	54
4.4 Контрольные вопросы и задания.....	54
ЛАБОРАТОРНАЯ РАБОТА №5 НАСТРОЙКА СЕРВЕРОВ .....	55
5.1 Теоретическая часть .....	55
5.2 Лабораторное задание .....	66
5.3 Содержание отчета .....	68
5.4 Контрольные вопросы и задания.....	69
ЛАБОРАТОРНАЯ РАБОТА №6 ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ .....	70
6.1 Теоретическая часть .....	70
6.2 Лабораторное задание .....	77
6.3 Содержание отчета .....	79
6.4 Контрольные вопросы и задания.....	79
ЛАБОРАТОРНАЯ РАБОТА №7 VOIP-ТЕЛЕФОНИЯ .....	80
7.1 Теоретическая часть .....	80
7.2 Лабораторное задание .....	86
7.3 Содержание отчета .....	89

7.4 Контрольные вопросы и задания .....	89
ЛАБОРАТОРНАЯ РАБОТА №8 ТЕХНОЛОГИЯ IOT .....	90
8.1 Теоретическая часть .....	90
8.2 Лабораторное задание.....	99
8.3 Содержание отчета .....	101
8.4 Контрольные вопросы и задания .....	101
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	102

Библиотека БГУИР

# ЛАБОРАТОРНАЯ РАБОТА №1

## ОСНОВЫ СОЗДАНИЯ ЛОКАЛЬНЫХ СЕТЕЙ

**Цель:** изучить принципы организации, построения и настройки локальных сетей; овладеть навыками создания простейших локальных сетей, осуществления диагностики соединений.

### 1.1 Теоретическая часть

Локальные сети служат для объединения рабочих станций, терминалов и других устройств. Локальная сеть позволяет повысить эффективность работы компьютеров за счет совместного использования ими ресурсов, например файлов и принтеров. Как результат, это дает возможность предприятию использовать локальную сеть для связи, выполнения функций обмена и вычислений, а также хранения информации на файл-серверах. Характерными особенностями локальной сети являются:

- ограниченные географические пределы;
- обеспечение большому количеству пользователей доступа к среде с высокой пропускной способностью;
- постоянное подключение к локальным сервисам;
- физическое соединение рядом стоящих устройств.

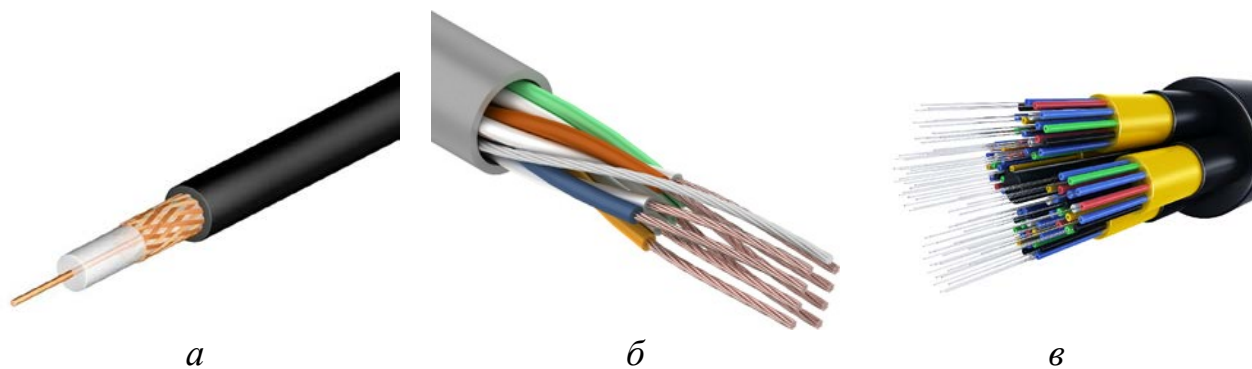
Локальная сеть – это также совокупность устройств и систем, подключенных друг к другу (логически или физически) и общающихся между собой. Размер этой сети может достигать больших размеров, а может состоять всего из двух устройств, соединенных между собой. Все компоненты сети можно разделить на следующие группы: сетевая среда, оконечные устройства, промежуточные устройства.

**Сетевая среда** – физическая среда, пригодная для прохождения сигнала в целях обмена кодированной информацией между оконечными устройствами и обеспечивающая их физическое соединение друг с другом.

Существует несколько видов сред, применяемых для соединения устройств в локальных сетях (рисунок 1.1):

- коаксиальный кабель;
- витая пара;
- радиоволны;
- оптоволоконный кабель.

Коаксиальный кабель состоит из двух проводящих элементов. Один из них – медный провод, находящийся в центре кабеля и окруженный слоем гибкой изоляции. Поверх изоляционного материала расположен экран из тонких переплетающихся медных проводов или из металлической фольги, который в электрической цепи играет роль второго провода. Как следует из названия, внешняя оплетка служит для экранирования центрального провода от влияния помех. Снаружи экран покрыт оболочкой (рисунок 1.1, а).



*a* – коаксиальный кабель; *б* – витая пара, *в* – оптоволоконный кабель

Рисунок 1.1 – Виды сетевых сред

Кабель на основе неэкранированной витой пары (Unshielded Twisted-Pair, UTP) используется во многих сетях и представляет собой четыре пары скрученных между собой проводов, при этом каждая пара изолирована от других (рисунок 1.1, б). Кабель UTP, применяемый в сетях передачи данных, имеет четыре пары медных проводов и наружный диаметр около 4,35 мм.

Кабель на основе экранированной витой пары (Shielded Twisted-Pair, STP) объединяет в себе методы экранирования и скручивания проводов (рисунок 1.2). Предназначенный для использования в сетях передачи данных и правильно установленный STP-кабель по сравнению с UTP-кабелем имеет большую устойчивость к электромагнитным и радиочастотным помехам без существенного увеличения веса или размера кабеля.

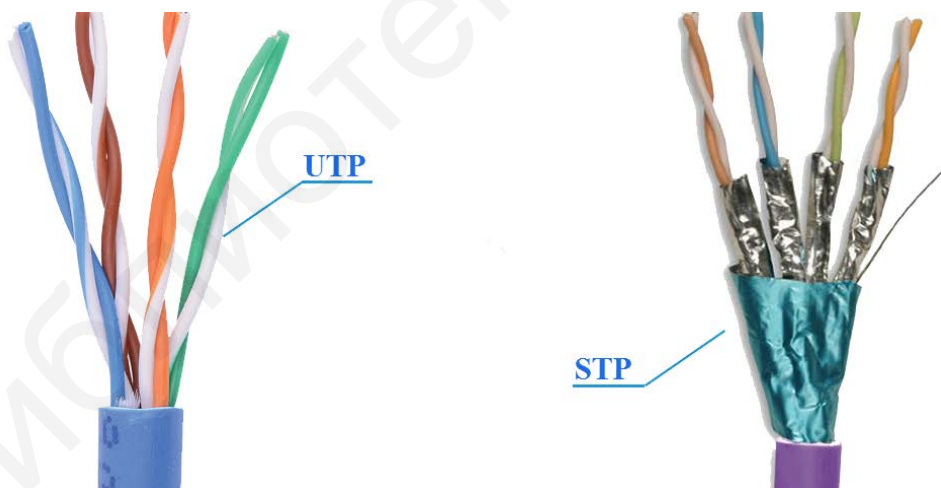


Рисунок 1.2 – UTP- и STP-кабели

Оптоволоконный кабель (рисунок 1.1, в) содержит оптические волокна, каждое из которых состоит из двух концентрических слоев – сердцевины и оболочки (рисунок 1.3). Сердцевина является средой передачи оптического сигнала, оболочка обеспечивает полное внутреннее отражение светового луча в сердцевину, и, как следствие, снижение излучения световой энергии в окружающее пространство. В целях повышения прочности и тем самым надежности оптических волокон поверх оболочки, как правило, накладывается

защитное покрытие. Защитная оболочка представляет собой один или несколько слоев полимера, предохраняющего сердцевину и оптическую оболочку от воздействий, которые могут повлиять на их оптические свойства. Защитная оболочка не влияет на процесс распространения света по оптическому волокну, а всего лишь предохраняет от ударов.

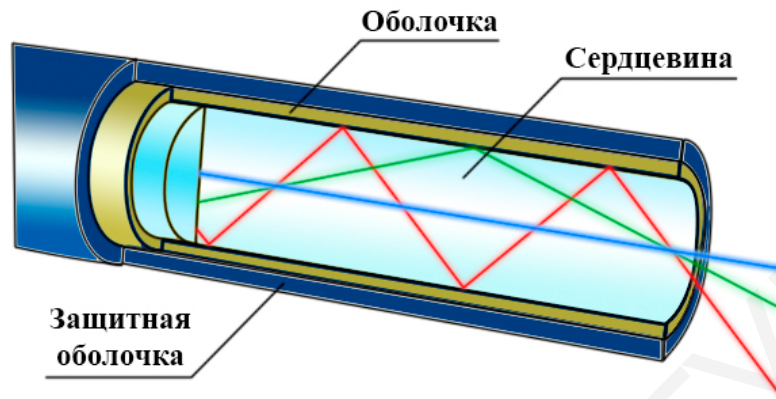


Рисунок 1.3 – Структура оптического волокна

**Оконечные устройства** – устройства, которые передают и/или принимают какие-либо данные (компьютеры, телефоны, серверы, терминалы, телевизоры).

Каждый компьютер независимо от того, подключен он к сети или нет, имеет уникальный физический адрес. Не существует двух одинаковых физических адресов. Физический адрес (MAC-адрес) установлен на плате сетевого адаптера.

Когда в сети одно устройство пересылает данные другому, оно устанавливает канал связи с этим устройством, воспользовавшись его MAC-адресом. Отправляемые источником данные содержат MAC-адрес пункта назначения. По мере продвижения пакета в среде передачи данных сетевые адаптеры каждого из устройств сети сравнивают MAC-адрес пункта назначения, имеющийся в пакете данных, со своим собственным физическим адресом. Если адреса не совпадают, сетевой адаптер игнорирует этот пакет, и данные продолжают движение к следующему устройству.

MAC-адрес представляет собой 6-байтную последовательность, закодированную в шестнадцатеричном формате (рисунок 1.4). Первая тройка байтов (OUI) содержит служебную информацию о производителе. Вторая тройка (NIC) – обозначает конкретное устройство, которым может быть сетевая карта, Wi-Fi или Bluetooth-модуль. Параметры сведены в шесть октетов, разделенных двоеточиями. В общем виде такая запись имеет структуру «AA:A0:A1:BB:B0:B2».

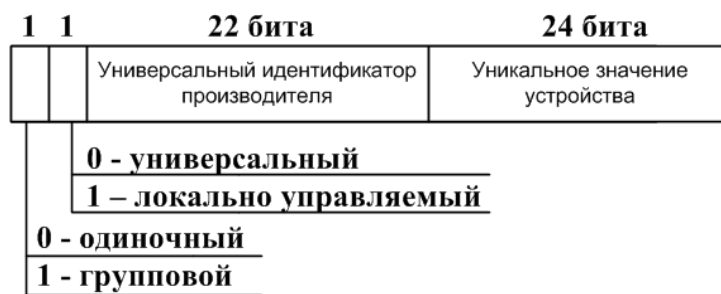


Рисунок 1.4 – Структура MAC-адреса

**Промежуточные устройства** – устройства, которые соединяют оконечные узлы между собой (повторители, концентраторы, коммутаторы, маршрутизаторы, точки доступа Wi-Fi и др.).

Повторители позволяют увеличить протяженность сети, гарантируя при этом, что сигнал будет распознан принимающими устройствами; принимают ослабленный сигнал, очищают его от помех, усиливают и отправляют дальше в сеть, тем самым увеличивая расстояния, на которых сеть может функционировать.

В локальных сетях каждое оконечное устройство подключается с помощью передающей среды. Как правило, у каждого файл-сервера имеется только один сетевой адаптер. Как результат, непосредственное подключение всех оконечных устройств к файл-серверу невозможно. Чтобы решить эту проблему, в сетях используются концентраторы, которые являются наиболее распространенными сетевыми устройствами.

Концентратор (hub, центр деятельности) – промежуточное устройство, выполняющее следующие функции: получение сигнала от устройства, одновременное его усиление и восстановление формы, побитная передача на все порты, кроме порта, с которого сигнал был получен. В этот момент прием сигнала на любом другом порту невозможен.

Сетевой коммутатор (switch, переключатель) – это устройство, позволяющее соединять несколько участков компьютерной сети, обладающее свойством адресной отправки пакетов, что достигается путем фиксации индивидуальных MAC-адресов подключенных компьютеров.

Чтобы создать локальную сеть, нужно подготовить сетевые кабели. Для этого применяются два основных варианта обжима кабеля витой пары: прямой и перекрестный (кроссовый). Прямой обжим используется при изготовлении кабелей для подключения сетевого интерфейса компьютера и других устройств к коммутаторам или маршрутизаторам, а также соединения между собой сетевого оборудования; кроссовый обжим – для соединения напрямую между собой или двух концентраторов, или двух коммутаторов, или двух оконечных узлов без применения коммутационного оборудования.

Обжим витой пары – это процесс закрепления специальных разъемов на концах кабеля, в качестве которых используются 8-контактные коннекторы 8P8C, которые обычно называют RJ-45.



Внутри коннектора RJ-45 для укладки проводов нарезаны восемь маленьких канавок, по одной для каждой жилы. Над ними в конце расположены металлические контакты. В процедуре обжима важна нумерация контактов, поэтому надо запомнить следующее: если держать разъем контактами вверх и защелкой к себе, то слева будет располагаться первый контакт, а справа – восьмой. Различают две схемы для распределения жил: EIA/TIA-568A и EIA/TIA-568B. Отличие между схемами заключается в расположении жил (рисунок 1.5). Для получения прямого кабеля необходимо оба его конца обжать по схеме 568B, для получения кроссового кабеля – один конец обжать по схеме 568A, а другой – по схеме 568B.

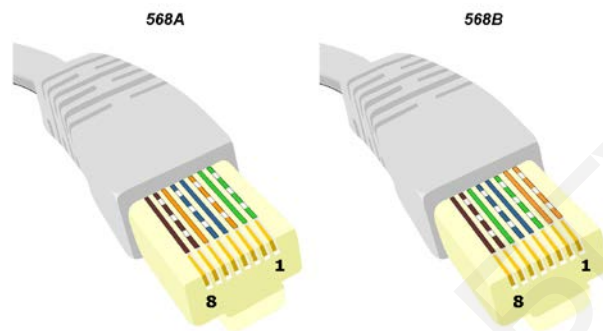


Рисунок 1.5 – Схемы расположения жил витой пары в коннекторе RJ-45

Порядок действий при обжиме кабеля следующий.

1. Отмерить и отрезать под прямым углом кабель нужной длины.
2. С каждой его стороны снять общую внешнюю изоляционную оболочку на 25–30 мм, не повредив собственную изоляцию проводников, которая находится внутри витой пары.
3. Распределить жилы по цветам в соответствии с выбранной схемой, для чего необходимо расплести и выровнять провода, разложить их в ряд в нужном порядке, плотно прижать друг к другу и обрезать концы, оставив приблизительно 12–13 мм от края изоляции.
4. Надеть коннектор на кабель так, чтобы жилы не перепутались, и каждая из них вошла в свой канал. Жилы должны упереться в переднюю стенку разъема. Если длина концов проводников обработана правильно, все они должны зайти в разъем до упора, а изоляционная оболочка должна обязательно оказаться внутри корпуса.
5. Зафиксировать разъем на конце кабеля обжимным инструментом.

Команда ping – это одна из наиболее употребляемых утилит командной строки, предназначенная для диагностики качества соединений, устранения неполадок соединения, проверки разрешения имен и возможности доступа путем отправки эхо-запросов и получение соответствующих эхо-ответов.

Данная команда имеет следующий формат:

```
ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS]
[-r число] [-s число] [-j список_узлов] | [-k список_узлов]]
[-w тайм-аут] конечное_имя
```

Использование всех параметров не обязательно, но необходимо при определенных видах проверки соединения, их описание представлено в таблице 1.1. Для завершения и вывода статистики используются комбинации клавиш Ctrl+Break (вывод статистики и продолжение), и Ctrl+C (вывод статистики и завершение).

Таблица 1.1 – Описание параметров команды ping

Параметр	Описание
-t	Непрерывная отправка пакетов
-a	Определение адресов по именам узлов
-n число	Число отправляемых эхо-запросов
-l размер	Размер поля данных в байтах отправляемого запроса
-f	Установка флага, запрещающего фрагментацию пакета
-i TTL	Задание срока жизни пакета (поле «Time To Live»)
-v TOS	Задание типа службы (поле «Type Of Service»)
-r число	Запись маршрута для указанного числа переходов
-s число	Штамп времени для указанного числа переходов
-j список узлов	Свободный выбор маршрута по списку узлов
-k список узлов	Жесткий выбор маршрута по списку узлов
-w тайм-аут	Максимальное время ожидания каждого ответа в миллисекундах

Для выполнения проверки соединения с определенным узлом, IP-адрес которого известен, может использоваться следующий формат команды (если параметры не указаны, то их значение устанавливается по умолчанию, количество пакетов равно четырем, длина массива данных – 32 байта):  
 ping 192.168.1.1

В результате ввода данной команды на устройство с указанным в команде IP-адресом отправляется четыре пакета размером 32 байта (рисунок 1.6). При удачной отправке команда возвращает значение времени передачи данных.

Существуют следующие модификации команды ping. Например, отправка пяти эхо-запросов на узел test.ru осуществляется следующим образом:  
 ping -n 5 test.ru

Опрос узла test.ru производится 5000 раз пакетами с данными длиной 1000 байт (допустимая максимальная длина данных – 65 500) можно осуществить, указав следующие параметры команды ping:  
 ping -n 5000 -l 1000 test.ru

Проверка соединения с указанием времени жизни TTL=5:  
 ping -i 5 test.com

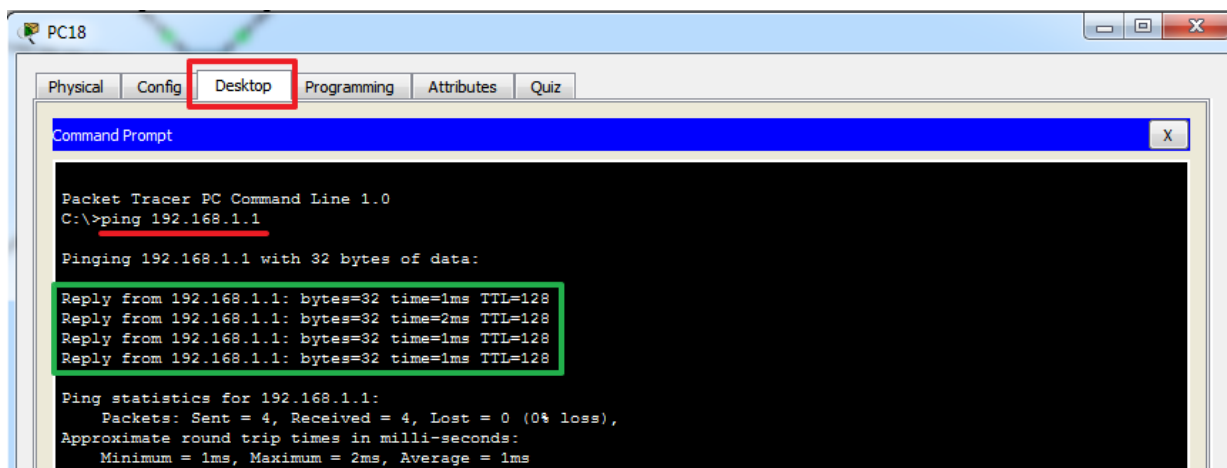


Рисунок 1.6 – Результат проверки соединения с помощью команды ping

Если для достижения конечного узла потребуется большее количество переходов по маршруту, то маршрутизатор, прервавший доставку ответит сообщением «Превышен срок жизни (TTL) при передаче пакета». Отправка пакетов с тайм-аутом ожидания, равным 5000 мс (по умолчанию 4 с):

```
ping -w 5000 ya.ru
```

Проверка установки и работоспособности сетевых программных компонентов узла:

```
ping 127.0.0.1
```

## 1.2 Лабораторное задание

1. Изучить рабочее пространство симулятора Cisco Packet Tracer (рисунок 1.7).

2. Перейти на вкладку моделирования физического пространства (рисунок 1.7, кнопка 2). Создать простейшую сеть, состоящую из двух компьютеров (PC-PT в разделе «End Devices», рисунок 1.7, кнопки 6 и 9) и концентратора (Hub-PT в разделе «Network Devices» → «Hubs», рисунок 1.7, кнопка 5). Используя прямой кабель (Copper Straight-Through, в разделе «Connections», рисунок 1.8, кнопки 1, 2), соединить компьютеры с концентратором.

3. Перемещая один из компьютеров, определить максимальную длину кабеля, при которой будет осуществляться передача данных. Если порты загораются красным цветом (рисунок 1.8), значит, сигнал не поступает от одного устройства к другому. Зафиксировать в отчете максимальную длину кабеля, при которой можно передавать данные. Установить повторитель (Repeater-PT в разделе «Network Devices» → «Hubs», рисунок 1.7, кнопка 5) и проверить работоспособность передачи данных.

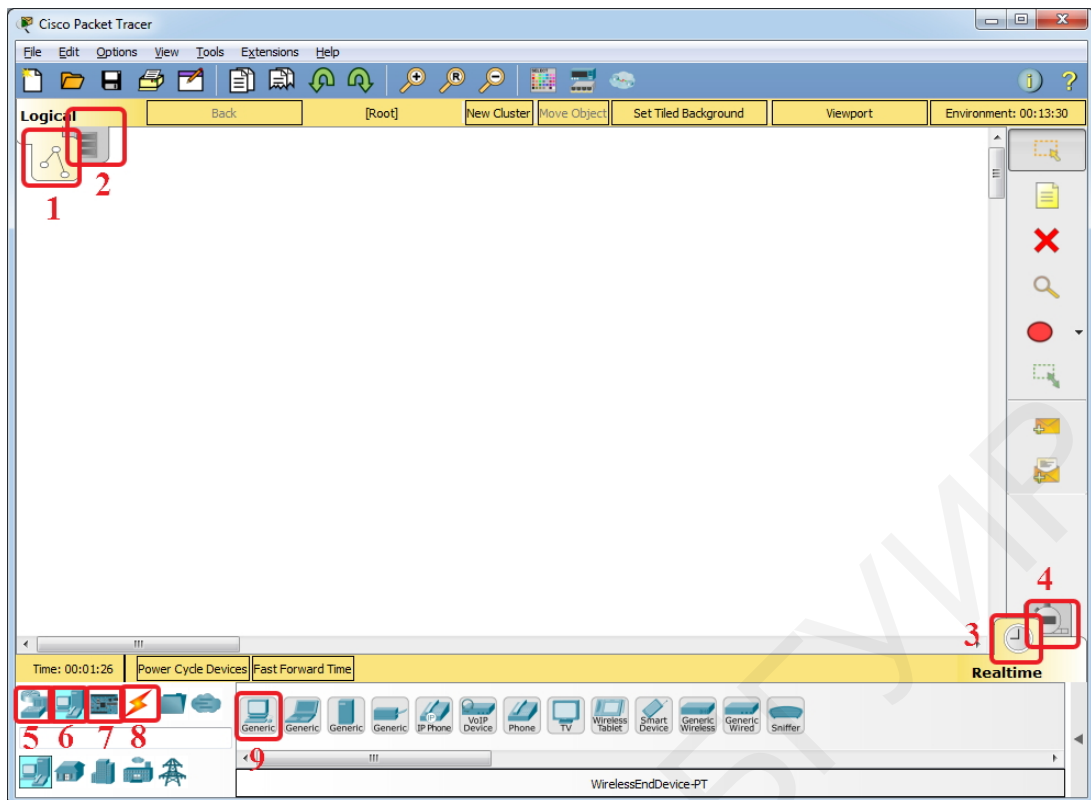


Рисунок 1.7 – Внешний вид рабочего пространства симулятора Cisco Packet Tracer

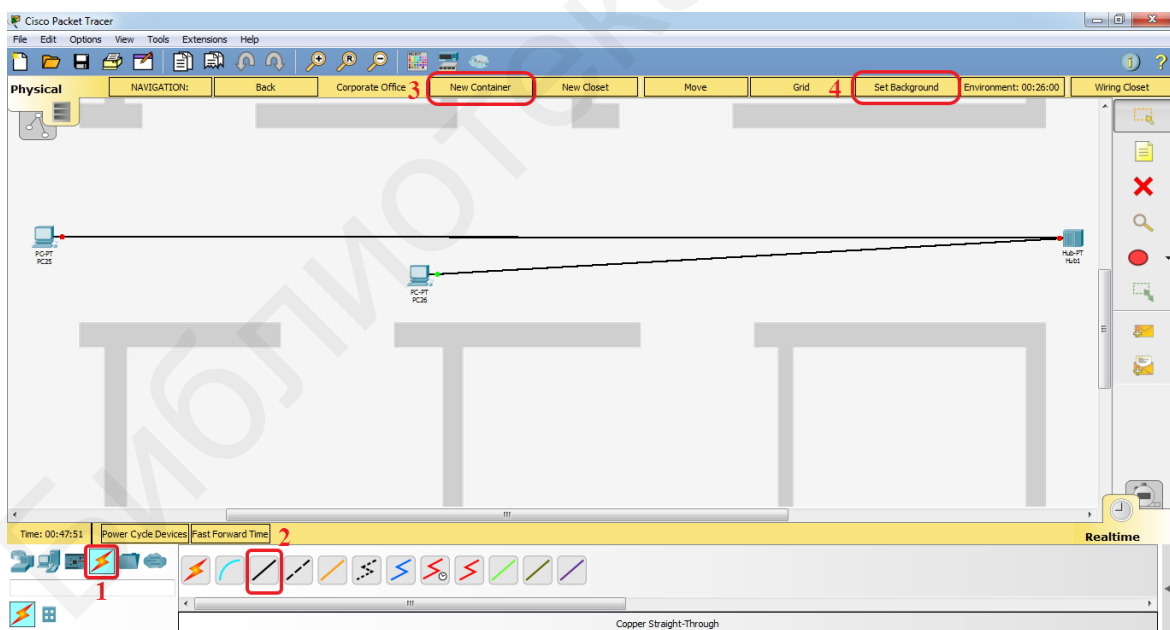


Рисунок 1.8 – Проверка дальности передачи сигнала

4. Добавить новый контейнер (рисунок 1.9, кнопка 2). Нажав «Set Background» (рисунок 1.8, кнопка 4), в открывшемся окне (рисунок 1.10) добавить изображение плана помещения (кнопка «Browse», рисунок 1.10, кнопка 1). Выбор плана помещения осуществить в соответствии с заданным шифром (таблица 1.2), который выдается преподавателем каждому студенту

индивидуально. Длина и ширина контейнера выставляется в полях «Width» и «Length» в соответствии с заданием из таблицы 1.2.

Таблица 1.2 – Варианты планов помещений

Первая цифра шифра	Номер схемы	Ширина/длина контейнера, м
0	1	40 × 20
1	0	30 × 30
2	9	40 × 25
3	8	40 × 25
4	7	30 × 20
5	6	28 × 20
6	5	25 × 15
7	4	23 × 23
8	3	30 × 20
9	2	25 × 23

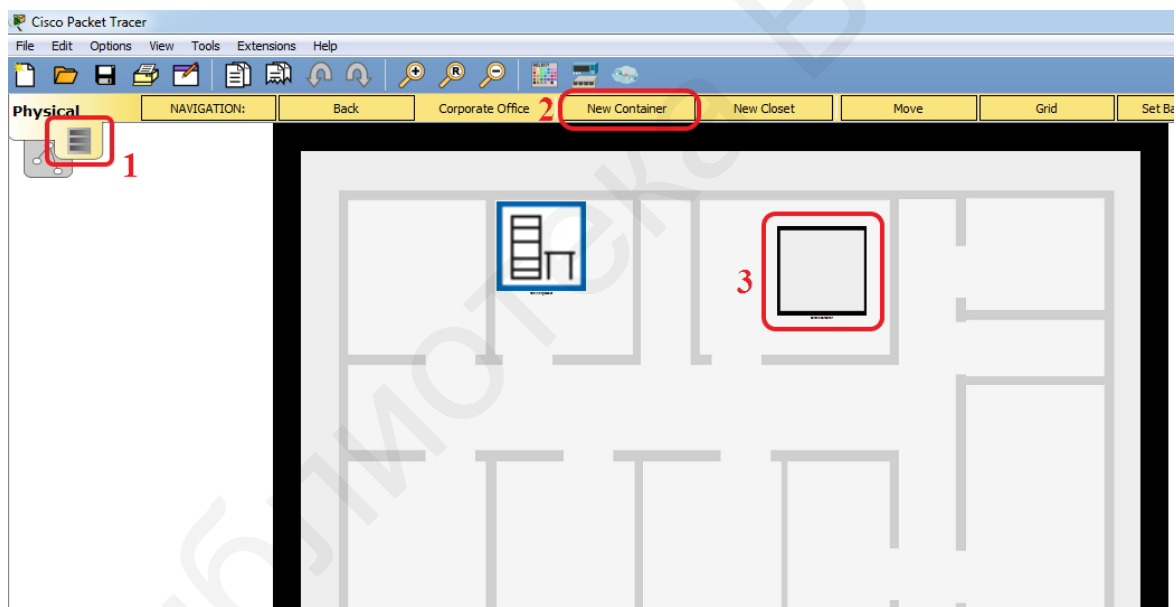


Рисунок 1.9 – Добавление нового контейнера для размещения плана здания

5. Осуществить расстановку оконечных устройств на плане здания. Количество устройств выбирается из таблицы 1.3 в соответствии с заданным преподавателем шифром. Выбрать и установить на плане необходимое количество концентраторов. Осуществить соединение компьютеров с концентраторами. Выбор топологии произвести самостоятельно, обозначить в выводе лабораторной работы тип выбранной топологии и обосновать свой выбор.

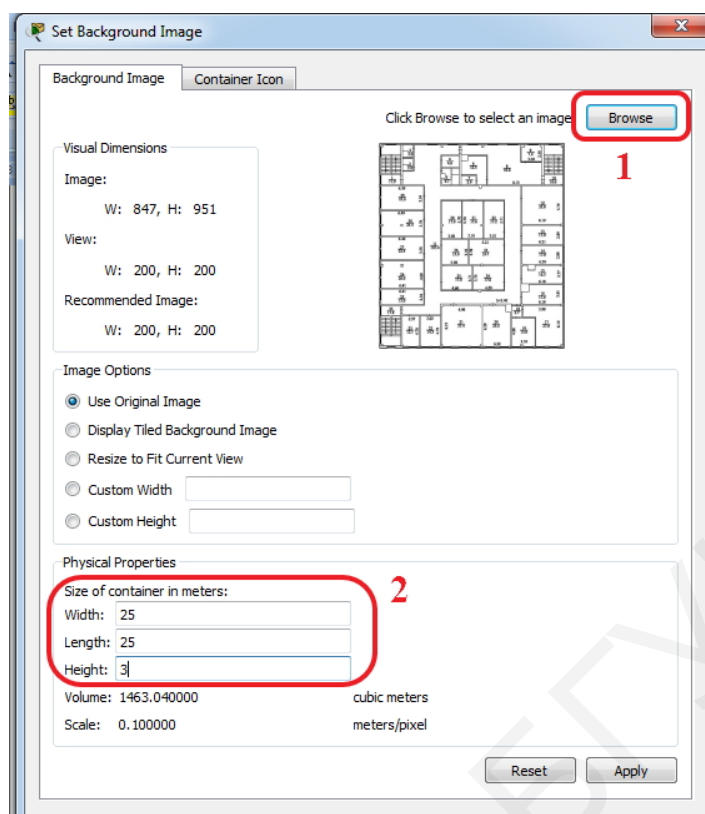


Рисунок 1.10 – Выбор плана здания и установка параметров

Таблица 1.3 – Настройка IP-адресации сети

Вторая цифра шифра	Количество компьютеров	Диапазон IP-адресов для оконечных устройств	IP-адрес маршрутизатора
0	24	192.168.12.2–192.168.12.100	192.168.12.1
1	23	192.168.14.2–192.168.14.100	192.168.14.1
2	25	192.168.122.2–192.168.122.100	192.168.122.1
3	20	192.168.58.2–192.168.58.100	192.168.58.1
4	21	192.168.32.2–192.168.32.100	192.168.32.1
5	22	192.168.9.2–192.168.9.100	192.168.9.1
6	23	192.168.8.2–192.168.8.100	192.168.8.1
7	25	192.168.3.2–192.168.3.100	192.168.3.1
8	24	192.168.114.2–192.168.114.100	192.168.114.1
9	26	192.168.76.2–192.168.76.100	192.168.76.1

6. Настроить IP-адресацию на каждом компьютере в соответствии с приведенными в таблице 1.3 параметрами (маска подсети 255.255.255.0, адрес шлюза – это IP-адрес маршрутизатора). Заполнить таблицу адресации (таблица 1.4). Для задания IP-адреса нажать на оконечное устройство, перейти на вкладку «Desktop», выбрать «IP Configuration». Пример заполнения полей в появившемся окне представлен на рисунке 1.11. Для проверки правильности установленного IP-адреса и получения сведений о MAC-адресе устройства необходимо в командной строке устройства осуществить команду `ipconfig/all` (рисунок 1.12).

Таблица 1.4 – Таблица адресации устройств в смоделированной сети

Имя компьютера	IP-адрес	MAC-адрес

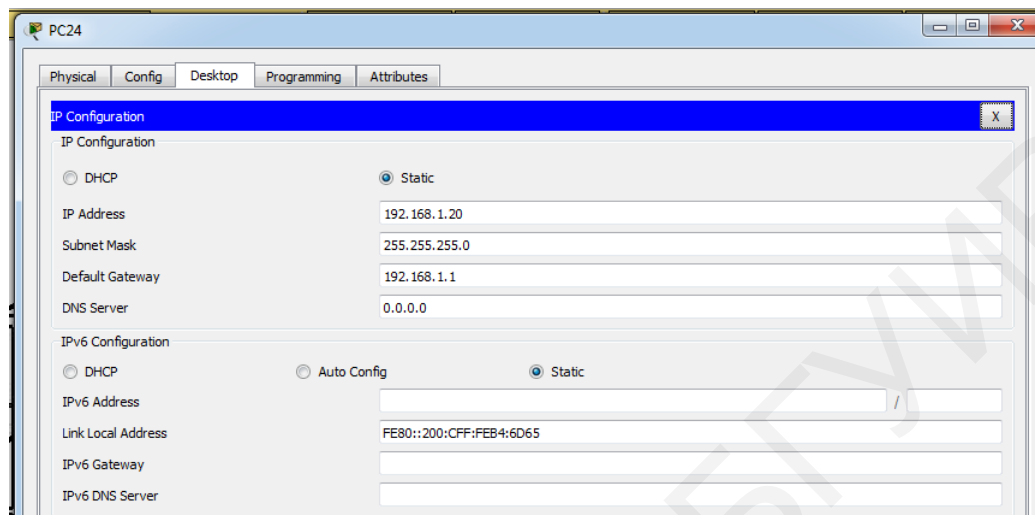


Рисунок 1.11 – Окно настройки IP-адреса оконечного устройства

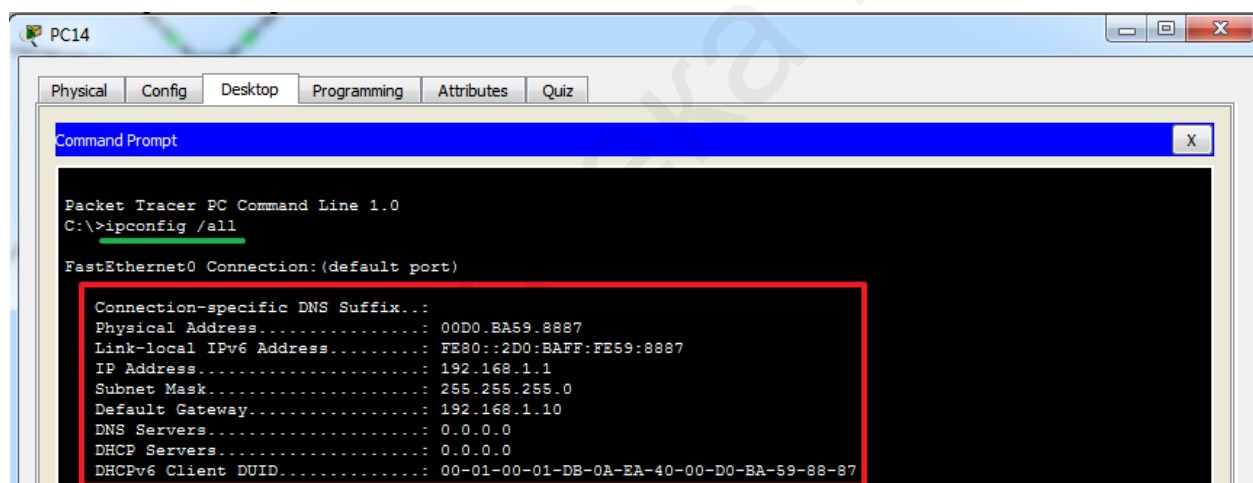


Рисунок 1.12 – Использование команды ipconfig/all для получение информации о сетевых настройках оконечного устройства

7. Проверить правильность подключения устройств в сети с помощью команды ping с любого компьютера. Для чего нажать на любое устройство, перейти на вкладку «Desktop», выбрать «Command Prompt», откроется окно командной строки, в которую необходимо ввести команды, осуществляющие следующие действия:

- отправку запросов по умолчанию;
- отправку семи запросов на любой компьютер;
- непрерывную отправку пакетов, которую можно остановить, нажав Ctrl + C.

Успешные результаты команды ping представить в отчете. Сохранить файл проекта Cisco Packet Tracer под именем lab1-1.pkt.

8. Перейти в режим симуляции времени (рисунок 1.7, кнопка 4). Нажать кнопку «Show All/None» для сброса настроек фильтра пакетов. Далее нажать клавишу «Edit Filters» и отметить на закладке «IPv4» пакеты ARP и ICMP (рисунок 1.13).

9. Отправить ping-запрос с любого устройства. Нажимая кнопку «Capture/Forward», проследить, как передается запрос и получается ответ. Записать последовательность передачи в таблицу 1.5.

Таблица 1.5 – Последовательность действий в смоделированной сети с концентраторами при отправке ping-запроса

Номер шага	Отправитель	Получатель
1		
2		
3		

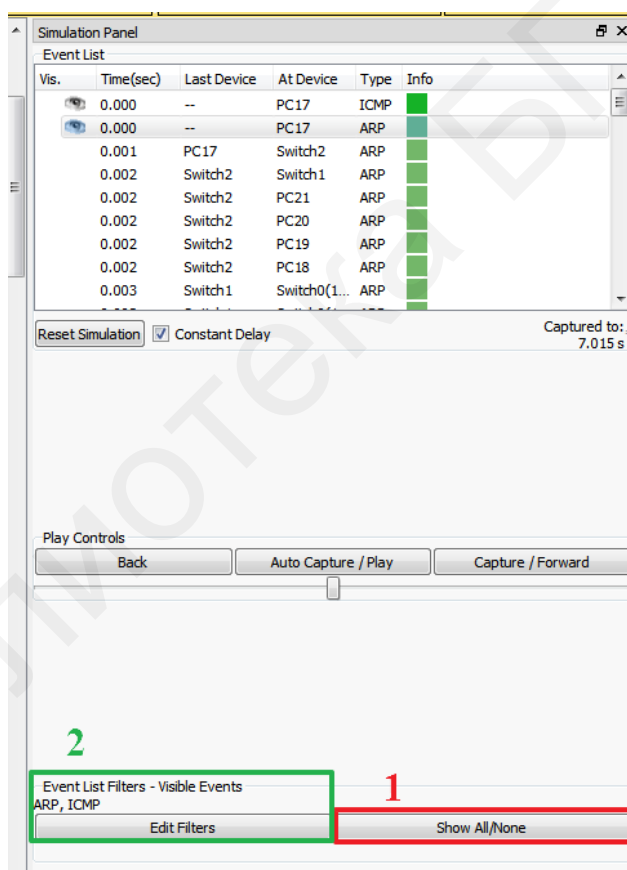


Рисунок 1.13 – Настройка отображения ARP- и ICMP-пакетов при симуляции

10. Осуществить замену всех концентраторов на коммутаторы («Switch-PT» в разделе «Network Devices» → «Switches»), сохранив топологию построенной сети. Когда цвета портов на всех коммутаторах станут зелеными, перейти в режим симуляции времени. Отправить ping-запрос с любого устройства. Нажимая кнопку «Capture/Forward», проследить, как передается запрос и получается ответ. Записать последовательность передачи

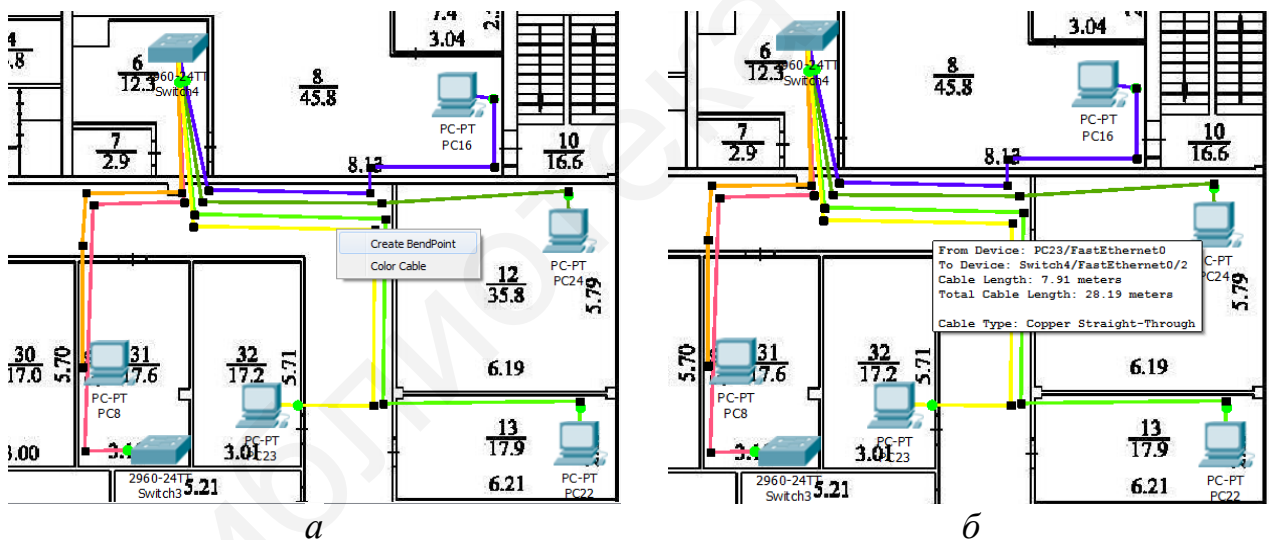


в таблицу 1.6. Сохранить файл проекта Cisco Packet Tracer под именем lab1-2.pkt. Сравнить процесс передачи запросов и ответов в смоделированных сетях с коммутаторами и концентраторами. Сделать вывод.

Таблица 1.6 – Последовательность действий в смоделированной сети с коммутаторами при отправке ring-запроса

Номер шага	Отправитель	Получатель
1		
2		
3		

11. Осуществить прокладку кабеля. Для чего, нажав на определенный кабель, выбрать «Create BendPoint», в результате появится точка на кабеле, перемещая которую, можно проложить маршрут кабеля (пример представлен на рисунке 1.14, а). Внести данные о длине каждого кабеля, которые можно просмотреть путем наведения курсора мыши на необходимый участок (рисунок 1.14, б), в таблицу 1.7. Сохранить файл проекта Cisco Packet Tracer под именем lab1.pkt. Данный файл будет использоваться в последующих лабораторных работах.



а – добавление точки; б – информация о длине кабеля

Рисунок 1.14 – Пример прокладки кабеля в Cisco Packet Tracer

Таблица 1.7 – Длина кабеля

Начальная точка	Конечная точка	Общая длина участка кабеля, м

### **1.3 Содержание отчета**

1. Цель работы, исходные данные из таблиц 1.2, 1.3.
2. Изображения смоделированных сетей согласно пунктам 3, 5, 10, 11 (см. подраздел 1.2).
3. Заполненные таблицы 1.4, 1.5, 1.6, 1.7.
4. Вывод по работе, содержащий заключения по пунктам 3, 10 (см. подраздел 1.2).
5. Ответы на контрольные вопросы.

### **1.4 Контрольные вопросы и задания**

1. Перечислить функции локальных сетей и их основные компоненты.
2. Объяснить назначение и структуру MAC-адреса.
3. Представить подробное описание видов сетевых сред передачи информации.
4. Описать методы обжима кабеля и пояснить порядок действий при обжиме кабеля.
5. В чем заключается назначение команды ping? Какие параметры используются для данной команды?

## ЛАБОРАТОРНАЯ РАБОТА №2 МОДЕЛЬ OSI

**Цель:** изучить структуру модели OSI и ее отличие от модели TCP/IP; ознакомиться с функциями основных протоколов; на практике изучить инкапсуляцию данных.

### 2.1 Теоретическая часть

Стек протоколов Transmission Control Protocol/Internet Protocol (TCP/IP) – это набор взаимодействующих протоколов разных уровней. Каждый уровень взаимодействует с соседним и производит обмен данными в сети, т. е. протокол – это набор правил, согласно которым происходит обмен данными. Протоколы разделены по уровням функциональности, что делает работу сетевого оборудования и программного обеспечения гораздо проще и прозрачнее, а также позволяет выполнять определенные задачи.

Для разделения набора протоколов по уровням была разработана модель OSI (Open Systems Interconnection Basic Reference Model, 1978 г.), которая является базовой эталонной моделью взаимодействия открытых систем и представляет собой обобщенные стандарты для разработчиков программ. При помощи данных стандартов любой компьютер может расшифровать информацию, полученную с другого компьютера.

Сетевой протокол – это правила и технические процедуры, позволяющие компьютерам одной сети осуществлять соединение и обмен данными. Группа протоколов, объединенных общей конечной целью, называется стек протоколов. Модель OSI имеет семь уровней.

#### **Уровень 7. Уровень приложений (Application Layer).**

Уровень приложений является ближайшим к пользователю и предоставляет службы приложениям внутри уровня. От других уровней он отличается тем, что не предоставляет служб другим уровням; вместо этого он предоставляет службы только приложениям, которые находятся вне рамок эталонной модели OSI. Примерами таких приложений могут служить электронные таблицы (например, программа Excel) или текстовые процессоры (например, программа Word). Уровень приложений определяет доступность партнеров по сеансу связи друг для друга, а также синхронизирует связь и устанавливает соглашение о процедурах восстановления данных в случае ошибок и процедурах контроля целостности данных. Примерами приложений седьмого уровня могут служить протоколы Telnet и HTTP.

#### **Уровень 6. Уровень представления данных (Presentation Layer).**

Задача уровня представления данных состоит в том, чтобы информация уровня приложений, которую посылает отправитель, могла быть прочитана уровнем приложений получателя. При необходимости уровень представления преобразует данные в один из многочисленных существующих форматов, который поддерживается обеими системами. Другая важная задача этого

уровня – шифрование и расшифрование данных. Типовыми графическими стандартами шестого уровня являются PICT, TIFF и JPEG, примерами стандартов шестого уровня эталонной модели, описывающих формат представления звука и видео, – MIDI и MPEG.

#### **Уровень 5. Сеансовый уровень (Session Layer).**

Как показывает само название, сеансовый уровень устанавливает сеанс связи между двумя рабочими станциями, управляет им и разрывает его. Сеансовый уровень предоставляет свои службы уровню представления данных. Он также синхронизирует диалог между уровнями представления двух систем и управляет обменом данными. Кроме своей основной постоянной функции управления, уровень сеанса связи обеспечивает эффективную передачу данных, требуемый класс обслуживания и рассылку экстренных сообщений о наличии проблем на сеансовом уровне, уровне представления данных или уровне приложений.

#### **Уровень 4. Транспортный уровень (Transport Layer).**

Транспортный уровень сегментирует данные передающей станции и вновь собирает их в одно целое на принимающей стороне. Границу между транспортным уровнем и уровнем сеанса связи можно рассматривать как границу между протоколами приложений и протоколами передачи данных. В то время как уровни приложений, представления данных и сеанса связи отвечают за аспекты коммуникаций, которые связаны с работой приложений, нижние четыре уровня «решают» вопросы транспортировки данных по сети. Транспортный уровень обеспечивает службу передачи данных таким образом, чтобы скрыть от верхних уровней детали процесса передачи. В частности, задачей уровня является обеспечение надежности передачи данных между двумя рабочими станциями.

Для выполнения службы связи транспортный уровень устанавливает, поддерживает и соответствующим образом ликвидирует виртуальные каналы. Выявление ошибок при передаче данных и управление информационными потоками – основные средства обеспечения надежности транспортной службы. К четвертому уровню относятся протокол управления передачей TCP и протокол пользовательских дейтаграмм UDP.

#### **Уровень 3. Сетевой уровень (Network Layer).**

Сетевой уровень является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть расположены в географически удаленных друг от друга сетях. Кроме того, он «решает» вопросы логической адресации. К третьему уровню относится Internet-протокол (IP).

#### **Уровень 2. Канальный уровень (Data Link Layer).**

Канальный уровень обеспечивает надежную передачу данных по физическому каналу. При этом он «решает» задачи физической (в противоположность логической) адресации, анализа сетевой топологии, доступа к сети, уведомления об ошибках, упорядоченной доставки фреймов и управления потоками. Примерами протоколов являются Ethernet, ARP.

## Уровень 1. Физический уровень (Physical Layer).

Физический уровень определяет электрические, процедурные и функциональные спецификации для активизации, поддержки и отключения физических каналов между конечными системами. Спецификациями физического уровня определяются уровни напряжений, синхронизация изменений напряжения, физическая скорость передачи данных, максимальная дальность передачи, физические соединения и другие аналогичные параметры. К первому уровню относятся протоколы, основанные на принципах кодирования информации.

Таблица 2.1 – Стек протоколов моделей OSI и TCP/IP

Уровень модели OSI	Уровень модели TCP/IP	Протоколы	Представление информации
Прикладной	Прикладной	HTTP, Telnet, SMTP, POP, FTP, DNS	Данные
Представления			
Сеансовый			
Транспортный	Транспортный	UDP, TCP	Сегменты
Сетевой	Сетевой	IP, ICMP	Пакеты
Канальный	Доступа к среде	ARP	Кадры
Физический		Ethernet	Биты

**Инкапсуляция** – это процесс передачи данных с верхнего уровня приложений вниз (по стеку протоколов) к физическому уровню для дальнейшей передачи по сетевой физической среде (витая пара, оптическое волокно, Wi-Fi и др.). Причем на каждом уровне различные протоколы добавляют к передающимся данным свою информацию.

**TCP** (Transmission Control Protocol, протокол управления передачей) – один из основных протоколов передачи данных в сети Интернет, предназначенный для управления передачей данных, отдельными сеансами связи между серверами и клиентами. TCP делит сообщения HTTP на более мелкие части, называемые сегментами. Эти сегменты передаются между веб-сервером и клиентскими процессами, запущенными на узле назначения. TCP также отвечает за управление размером и скоростью, с которой происходит обмен сообщениями между сервером и клиентом.

**UDP** (User Datagram Protocol – протокол пользовательских дейтаграмм) – использует простую модель передачи без обеспечения надежности, упорядочивания или целостности данных. Дейтаграммы могут прийти не по порядку, дублироваться или пропасть. Подразумевается, что проверка ошибок и их исправление либо не нужны, либо должны выполняться в приложении.

**Протокол IP** (Internet Protocol – межсетевой протокол) отвечает за прием форматированных сегментов от TCP, инкапсуляцию их в пакеты, присвоение им соответствующих адресов и доставку по наилучшему пути к узлу назначения.

Общий сценарий работы протокола на каком-либо узле сети, принимающем дейтаграмму, следующий:

1) с одного из интерфейсов уровня доступа к среде передачи (например, Ethernet) поступает дейтаграмма;

2) модуль IP анализирует ее заголовок;

3) если пунктом назначения дейтаграммы является данный компьютер:

- если дейтаграмма является фрагментом большей дейтаграммы, ожидаются остальные фрагменты, после чего из них собирается исходная большая дейтаграмма;

- из дейтаграммы извлекаются данные и направляются на обработку одному из протоколов вышележащего уровня;

4) если дейтаграмма не направлена ни на один из IP-адресов данного узла, то дальнейшие действия зависят от того, разрешена или запрещена ретрансляция (forwarding) дейтаграмм:

- если ретрансляция разрешена, то определяются следующий узел сети, на который должна быть переправлена дейтаграмма для доставки ее по назначению, и интерфейс нижнего уровня, после чего дейтаграмма передается на нижний уровень этому интерфейсу для отправки (при необходимости может быть произведена фрагментация дейтаграммы);

- если же дейтаграмма ошибочна или по каким-либо причинам не может быть доставлена, она уничтожается, при этом, как правило, отправителю дейтаграммы отсылается ICMP-сообщение об ошибке.

При получении данных от вышестоящего уровня для отправки их по сети IP-модуль формирует дейтаграмму с этими данными, в заголовок которой заносятся адреса отправителя и получателя (также полученные от транспортного уровня) и другая информация, после чего выполняются следующие шаги:

- если дейтаграмма предназначена этому же узлу, из нее извлекаются данные и направляются на обработку одному из протоколов транспортного уровня;

- если дейтаграмма не направлена ни на один из IP-адресов данного узла, то определяются следующий узел сети, на который должна быть переправлена дейтаграмма для доставки ее по назначению, и интерфейс нижнего уровня, после чего дейтаграмма передается на нижний уровень этому интерфейсу для отправки (при необходимости может быть произведена фрагментация дейтаграммы);

- если же дейтаграмма ошибочна или по каким-либо причинам не может быть доставлена, она уничтожается.

IP-адрес является уникальным 32-битовым идентификатором IP-интерфейса в сети Интернет. IP-адреса принято записывать разбивкой всего адреса по октетам, каждый октет записывается в виде десятичного числа, цифры разделяются точками. Например, адрес 10100000010100010000010110000011 записывается как 10100000.01010001.00000101.10000011 = 160.81.5.131.

IP-адрес состоит из номера IP-сети, который занимает старшую область адреса, и номера устройства в этой сети, занимающего младшую часть.

**HTTP** (HyperText Transfer Protocol – протокол передачи гипертекста) – протокол прикладного уровня определяет, каким образом взаимодействуют веб-сервер и веб-клиент. HTTP определяет содержание и формат запросов и ответов, которыми обмениваются клиент и сервер. HTTP реализует программное обеспечение и веб-клиента, и веб-сервера как часть приложения. Для управления процессом передачи сообщений между клиентом и сервером HTTP обращается к другим протоколам.

**SMTP** (Simple Mail Transfer Protocol – простой протокол передачи почты) – это широко используемый сетевой протокол, предназначенный для передачи электронной почты.

**DNS** (Domain Name System – система доменных имен) – компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), а также информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

**ARP** (Address Resolution Protocol – протокол определения адреса) – протокол в компьютерных сетях, предназначенный для определения MAC-адреса при наличии IP-адреса другого компьютера. Протокол ARP выполняет две основные функции: сопоставление адресов IPv4 и MAC-адресов, сохранение таблицы сопоставлений.

**POP** (Post Office Protocol – протокол почтового отделения) – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP-соединению.

**Протокол Telnet** обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленной ЭВМ.

**FTP** (File Transfer Protocol – протокол пересылки файлов) реализует удаленный доступ к файлу. Для того чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений – TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов, FTP позволяет пользователю указывать тип и формат запоминаемых данных. Наконец, FTP выполняет аутентификацию пользователей. Прежде чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол – **TFTP** (Trivial File Transfer Protocol – простейший протокол пересылки файлов). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения – UDP.

Для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений **ICMP** (Internet Control Message Protocol). Команда ping позволяет выполнить отправку управляющего сообщения типа Echo Request (тип равен восьми и указывается в заголовке ICMP-сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого ICMP-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос опрашиваемый узел должен отправить ICMP-пакет с теми же данными, которые были приняты, и типом сообщения Echo Reply (код типа в ICMP-заголовке равен нулю). Если при обмене ICMP-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики.

Одним из примеров протокола сетевого доступа является **Ethernet**. Такие протоколы управления каналами передачи данных принимают пакеты от протокола IP и форматируют их для передачи в среде. Стандарты и протоколы физической передачи данных управляют отправлением сигналов и их интерпретацией клиентами при получении.

На сегодняшний день Ethernet является наиболее широко используемой технологией локальных сетей, функционирующей на канальном и физическом уровнях. Это семейство сетевых технологий, которые регламентируются стандартами IEEE 802.2 и 802.3. Технология Ethernet поддерживает передачу данных на скоростях: 10 Мбит/с, 100 Мбит/с, 1000 Мбит/с (1 Гбит/с), 10 000 Мбит/с (10 Гбит/с), 40 000 Мбит/с (40 Гбит/с), 100 000 Мбит/с (100 Гбит/с). Стандарты Ethernet регламентируют как протоколы уровня 2, так и технологии уровня 1. Для протоколов второго уровня, как и в случае со всеми стандартами группы IEEE 802, технология Ethernet полагается на работу этих двух отдельных подуровней канального уровня, а также на подуровни управления логическим каналом (LLC) и MAC (рисунок 2.1).

Подуровень LLC технологии Ethernet обеспечивает связь между верхними и нижними уровнями. Как правило, это происходит между сетевым программным обеспечением и аппаратным обеспечением устройства. Подуровень LLC использует данные сетевых протоколов, которые обычно представлены в виде пакета IPv4, и добавляет управляющую информацию, чтобы помочь доставить пакет к узлу назначения. LLC используется для связи с верхними уровнями приложений и перемещает пакет для доставки на нижние уровни. LLC реализован в программном обеспечении, и его применение не зависит от оборудования. LLC для компьютера можно рассматривать как программное обеспечение драйвера сетевой платы (NIC).

Драйвер сетевой платы – это программа, которая непосредственно взаимодействует с аппаратными средствами компьютера на сетевой интерфейсной плате для передачи данных между подуровнем MAC и физической средой.



MAC представляет собой более низкий подуровень канального уровня и реализуется на сетевой интерфейсной плате устройства. Спецификации содержатся в стандартах IEEE 802.3.

Канальный	Подуровень LLC	Ethernet	IEEE 802.2		
	Подуровень MAC		IEEE 802.3 Ethernet	IEEE 802.3u FastEthernet	IEEE 802.3z Gigabit-Ethernet
Физический					

Рисунок 2.1 – Подуровни канального уровня

Далее приведено описание основных полей кадра Ethernet, представленных на рисунке 2.2.

**Поля «Преамбула» (7 байт) и «Начало разделителя кадра (SFD)»** (также называется «Начало кадра») (1 байт) используются для синхронизации отправляющих и получающих устройств. Эти первые 8 байт кадра необходимы для привлечения внимания получающих узлов. По существу, первые несколько байтов сообщают получателю о необходимости приготовиться к поступлению нового кадра.

**Поле «MAC-адрес назначения» (6 байт)** является идентификатором для предполагаемого получателя. Этот адрес используется уровнем 2, чтобы помочь устройствам определить, адресован ли кадр именно им. Адрес в кадре сравнивается с MAC-адресом в устройстве. В случае совпадения устройство принимает кадр.

**Поле «MAC-адрес источника» (6 байт)** определяет сетевую плату или интерфейс, с которого был отправлен кадр.

7	1	6	6	2	46-1500	4
Преамбула	Начало разделителя кадра	Адрес источника	Адрес назначения	Длина	Заголовок и данные	Контрольная последовательность кадра

Рисунок 2.2 – Формат Ethernet-кадра по IEEE 802.3

**Поле «Длина».** В любом стандарте IEEE 802.3, используемом до 1997 г., поле «Длина» определяет точную длину поля данных кадра. Позже оно применялось как часть контрольной последовательности кадра (FCS), чтобы обеспечить правильность получения сообщения. В других случаях это поле используется с целью описать, какой протокол более высокого уровня присутствует. Если 2-октетное значение равно или превышает шестнадцатеричный формат 0x0600 или десятичное число 1536, то содержимое поля «Данные» декодируется в соответствии с указанным протоколом EtherType. Если же значение равно или меньше шестнадцатеричного формата

0×05DC или десятичного числа 1500, то поле «Длина» позволяет обозначить использование формата кадра IEEE 802.3.

**Поле «Данные»** (46–1500 байт) содержит инкапсулированные данные из более высокого уровня, который является универсальным PDU уровня 3, пакет IPv4. Длина всех кадров должна быть не менее 64 байт. В случае инкапсуляции небольшого пакета используются дополнительные биты, которые называются символами-заполнителями, для увеличения размера кадра до этого минимального значения.

**Поле «Контрольная последовательность кадра»** (4 байта) используется для обнаружения ошибок в кадре. В нем применяется циклический контроль избыточности (CRC). Отправляющее устройство включает в себя результаты циклического контроля избыточности в поле FCS кадра. Получающее устройство принимает кадр и создает CRC для поиска ошибок. Если расчеты совпадают, ошибки отсутствуют. Несовпадение расчетов означает изменение данных, следовательно, кадр сбрасывается. Данные могут измениться в результате нарушения электрических сигналов, которые представляют последовательность битов.

## 2.2 Лабораторное задание

1. Открыть файл lab1-2.pkt Cisco Packet Tracer, сохраненный в лабораторной работе №1. Задания данной лабораторной работы выполнять в пространстве логической топологии.

2. Открыть командную строку на любом компьютере и выполнить команду `arp -d`, чтобы очистить таблицу ARP. Командой `arp -a` проверить, что таблица чистая.

3. Перейти в режим симуляции времени (рисунок 2.3, кнопка 1). Отправить ICMP-пакет с любого компьютера, используя команду `ping`. Будут созданы два пакета PDU (см. рисунок 2.3). При нажатии на пакет ARP (рисунок 2.3, кнопка 2) появляется окно содержания данных (PDU), в котором представлена информация по инкапсуляции данных на каждом уровне модели OSI (рисунок 2.3, область 3). Проследить прохождение пакета, нажимая клавишу «Capture/Forward», и заполнить таблицу 2.2. Сделать вывод о необходимости отправки ARP-пакета перед отправкой ICMP-пакета.

4. Проверить таблицу ARP командой `arp -a`, зафиксировать в отчете ее содержимое.

5. Открыть командную строку на любом компьютере и выполнить команду `arp -d`, чтобы очистить таблицу ARP. Командой `arp -a` проверить, что таблица чистая. Перейти в режим симуляции времени. Отправить ICMP-пакет с любого компьютера, используя команду `ping`. Используя данные окна «PDU Information» для ARP-запроса на закладке «Outbound PDU Details» (рисунок 2.3, закладка 4), отобразить вид передаваемых кадров в таблицах 2.3, 2.4. Прodelать аналогичные действия для ICMP-пакета (заполнить таблицы 2.5, 2.6).

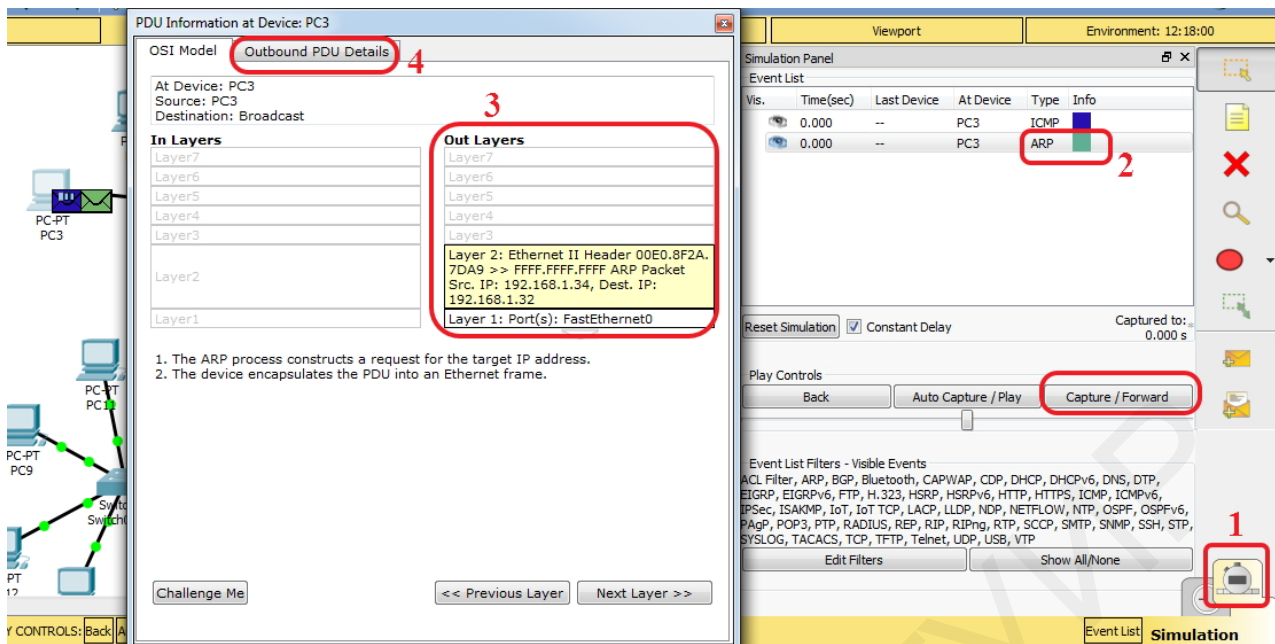


Рисунок 2.3 – Просмотр содержимого пакета в режиме симуляции времени

Таблица 2.2 – Последовательность действий в смоделированной сети с коммутаторами при отправке ping-запроса

Номер шага	Отправитель	Получатель	Содержание уровня	Описание действий
1				
2				
3				

Таблица 2.3 – Формат кадра Ethernet для ARP-запроса

Количество байтов							
Тип поля							
Содержание							

Таблица 2.4 – Формат ARP-запроса

Количество битов							
Тип поля							
Содержание							

Таблица 2.5 – Формат кадра IP для ICMP-запроса

Количество байтов							
Тип поля							
Содержание							

Таблица 2.6 – Формат ICMP-запроса

Количество битов									
Тип поля									
Содержание									

6. Заполнить таблицы 2.3–2.6 для пришедшего ответа ARP и ICMP. Сравнить структуру полученных и отправленных пакетов, отобразить различия и особенности в выводе лабораторной работы.

### 2.3 Содержание отчета

1. Цель работы.
2. Заполненные таблицы 2.2–2.6 для отправленных и полученных данных.
3. Вывод по работе, содержащий заключения по пунктам 3, 4, 6 (см. подраздел 2.2).
4. Ответы на контрольные вопросы.

### 2.4 Контрольные вопросы и задания

1. Перечислить уровни моделей OSI и TCP/IP, назвать основные отличия.
2. Привести описания уровней модели OSI.
3. Объяснить назначение протоколов HTTP, Telnet, SMTP, POP, FTP, DNS, UDP, TCP, IP, ICMP, ARP, Ethernet.
4. Какие существуют подуровни канального уровня? В чем заключается их сущность?
5. Представить формат Ethernet-кадра и назначения его полей.

## ЛАБОРАТОРНАЯ РАБОТА №3 НАСТРОЙКА КОММУТАТОРА

**Цель:** овладеть базовыми навыками настройки коммутаторов; изучить принципы заполнения таблиц MAC-адресов; научиться избегать коллизий в локальных компьютерных сетях.

### 3.1 Теоретическая часть

Коммутатор осуществляет коммутацию и фильтрацию только на основе MAC-адреса канального уровня модели OSI, в процессе передачи данных между независимыми IP-подсетями полагается на маршрутизаторы, и является полностью прозрачным для сетевых протоколов и пользовательских приложений. Коммутатор уровня 2 создает таблицу MAC-адресов, которые предназначены для передачи данных по сети через свою коммутирующую матрицу на соответствующий порт в направлении узла назначения.

Коммутирующая матрица представляет собой интегрированные каналы и дополняющие средства машинного программирования, что позволяет контролировать пути прохождения данных через коммутатор. Чтобы коммутатор смог использовать для передачи кадра одноадресной рассылки нужный порт, необходима информация об узлах, имеющих на каждом из его портов.

Описание этого процесса представлено на рисунках 3.1 и 3.2.

1. Коммутатор получает кадр от PC1 на порт 1.

2. Коммутатор вводит MAC-адрес источника и порт коммутатора, получившего кадр, в таблицу MAC-адресов.

3. Поскольку адрес назначения компьютера 3, коммутатор рассылает ARP-кадр по всем портам, кроме порта, по которому он был получен, чтобы узнать MAC-адрес устройства назначения (рисунок 3.1).

4. Устройство назначения отвечает на широковещательную рассылку индивидуальным кадром.

5. Коммутатор добавляет MAC-адрес компьютера 3 и номер порта коммутатора, получившего кадр, в таблицу MAC-адресов. Адрес назначения кадра и соответствующий порт находятся в таблице MAC-адресов (рисунок 3.2).

6. Теперь коммутатор может пересылать кадры между устройствами источника и назначения без широковещательной рассылки, поскольку у него есть записи в таблице MAC-адресов, которые идентифицируют соответствующие порты.

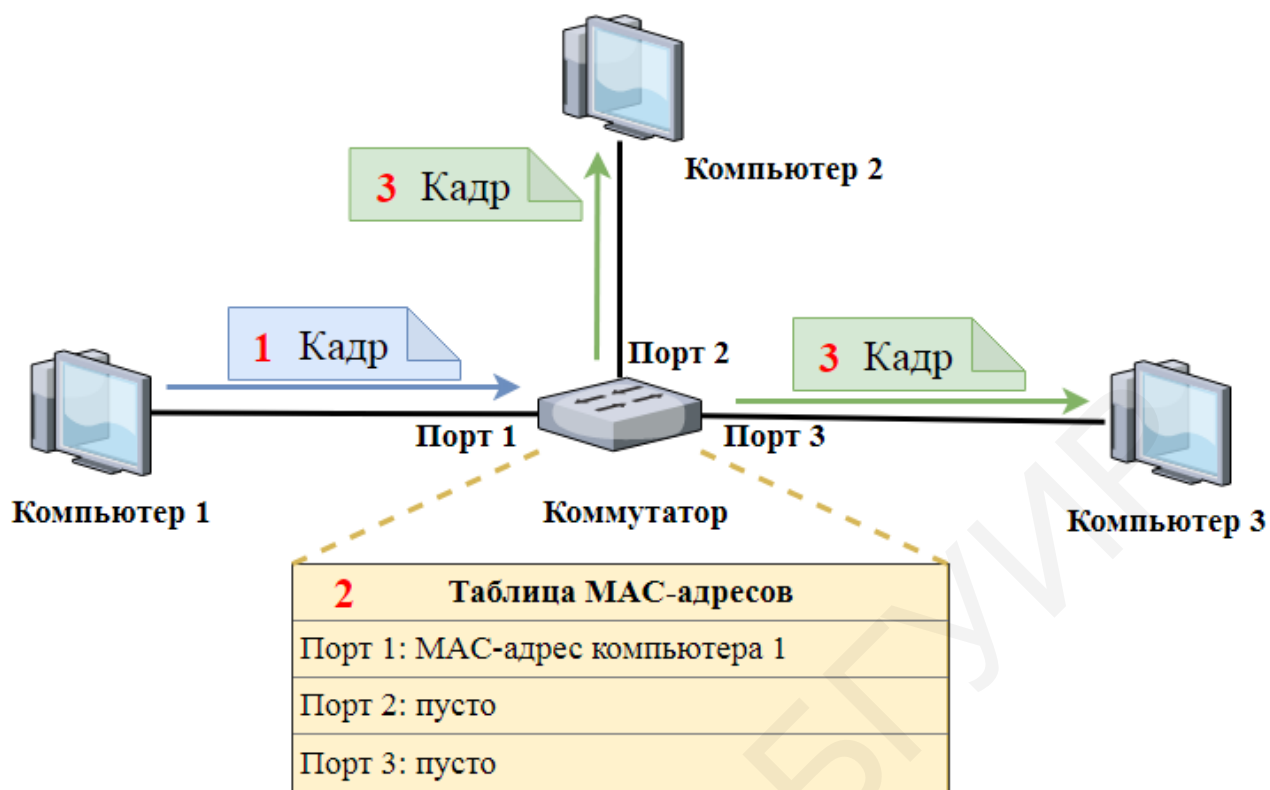


Рисунок 3.1 – Процесс добавления в таблицу MAC-адресов коммутатора адреса источника



Рисунок 3.2 – Процесс добавления в таблицу MAC-адресов коммутатора адреса назначения

Несмотря на то что коммутаторы прозрачны для сетевых протоколов и пользовательских приложений, они способны функционировать в разных режимах, что может отразиться на пересылке кадров Ethernet по сети как положительно, так и отрицательно. Одним из базовых параметров коммутатора является дуплексный режим для каждого отдельного порта, подключенного к каждому главному устройству. Порт на коммутаторе должен быть настроен таким образом, чтобы совпадать с параметрами дуплексного режима определенного типа среды передачи данных. Для обмена данными в сетях Ethernet используются два типа настроек дуплексного режима: полудуплексный и полнодуплексный.

В полудуплексной связи применяется однонаправленный поток данных, когда отправка и получение данных выполняются не в одно и то же время. Это похоже на использование радиации, когда одновременно не могут говорить два человека, только один. Иначе происходит коллизия. Поэтому при полудуплексной связи используется множественный доступ с контролем несущей и определением коллизий, что позволяет снизить их вероятность и обнаружить их в случае возникновения. При полудуплексной связи возможно снижение производительности, вызванное постоянным пребыванием в режиме ожидания, поскольку данные могут передаваться одновременно только в одном направлении. Полудуплексные соединения, как правило, встречаются на более старом оборудовании, например на концентраторах. Узлы, которые подключены к концентраторам, совместно использующим подключение к порту коммутатора, должны работать в полудуплексном режиме, так как конечным компьютерам необходимо иметь возможность обнаруживать коллизии. Узлы также могут функционировать в полудуплексном режиме, если сетевую интерфейсную плату нельзя настроить для работы в полнодуплексном режиме. В этом случае для порта на коммутаторе по умолчанию также устанавливается полудуплексный режим. Из-за этих ограничений полнодуплексная связь заменила полудуплексную на более современном оборудовании.

В полнодуплексной связи поток данных передается в обе стороны, что позволяет одновременно отправлять и получать информацию. Поддержка двухсторонней передачи данных повышает производительность за счет сокращения времени ожидания между передачами. В данном режиме детектор коллизий отключен. При этом исключена возможность столкновения кадров, пересылаемых двумя связанными конечными узлами, поскольку эти узлы используют два отдельных канала связи в сетевой кабеле. Каждое полнодуплексное соединение использует только один порт. Полнодуплексным соединениям требуется коммутатор, который поддерживает полнодуплексный режим, или прямое подключение, между двумя узлами, каждый из которых поддерживает полнодуплексную передачу данных. Узлы, которые непосредственно подключены к выделенному порту коммутатора с помощью сетевых адаптеров, поддерживающих полнодуплексную связь, должны

подключаться к портам коммутатора, настроенным для работы в полнодуплексном режиме.

Большинство продаваемых сегодня сетевых адаптеров Ethernet, Fast Ethernet и Gigabit Ethernet работают в полнодуплексном режиме.

Одной из функций подуровня MAC является управление доступом к среде передачи данных. Она отвечает за размещение кадров в этой среде и удаление из нее кадров.

**Метод ассоциативного доступа** (или недетерминированный метод) означает, что любое устройство может постоянно предпринимать попытку передать данные в общей среде при наличии у него таких данных для отправки. При этом если несколько устройств в одной среде начнут вместе передавать информацию (подобно тому, как два человека попытаются разговаривать одновременно), то возникнет конфликт при передаче данных, который приведет к их повреждению и невозможности дальнейшего использования. Чтобы не допустить подобной ситуации, Ethernet задействует метод множественного доступа с контролем несущей (CSMA) для управления общим доступом узлов.

Процесс CSMA используется для того, чтобы сначала определить, передается ли сигнал в среде. Если в среде обнаружен сигнал несущей частоты, исходящий от другого узла, это значит, что в данный момент другое устройство осуществляет передачу данных. В случае если устройство пытается передать данные тогда, когда среда занята, оно подождет и повторит попытку позже. При отсутствии сигнала несущей частоты данное устройство начнет передачу данных. Существует вероятность возникновения сбоя процесса CSMA, в результате чего два устройства будут передавать данные одновременно. Это называется коллизией данных (рисунок 3.3). В этом случае данные, отправленные обоими устройствами, будут повреждены, из-за чего потребуется их повторная отправка.

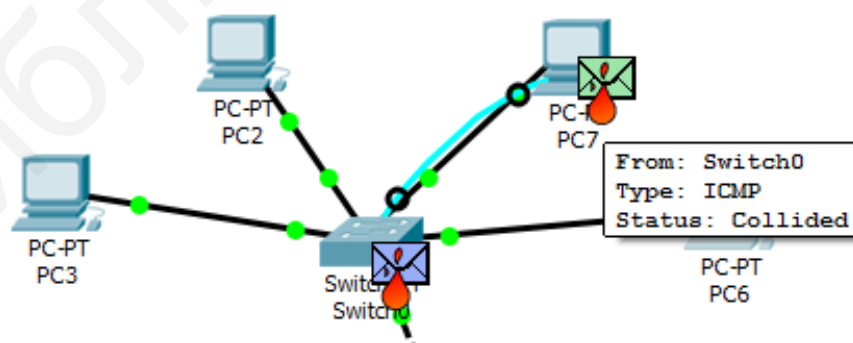


Рисунок 3.3 – Пример реализации коллизии в смоделированной сети

Способы контроля доступа к среде передачи на основе ассоциативного доступа не требуют наличия механизмов для отслеживания очередности доступа к среде; следовательно, они не обладают нагрузкой на ресурсы, присущей способам контролируемого доступа. Однако ассоциативные системы



не отличаются хорошей масштабируемостью в условиях сильной загруженности среды. По мере увеличения интенсивности нагрузки и количества узлов снижается вероятность получить доступ к среде без коллизий. Кроме того, пропускная способность среды также уменьшается, так как для исправления ошибок, вызванных такими коллизиями, требуется задействовать механизмы восстановления.

При обнаружении коллизий CSMA (CSMA/CD) устройство проверяет среду на наличие в ней сигнала данных. Его отсутствие указывает на то, что среда передачи не загружена, и тогда устройство передает данные. Передача данных прерывается и переносится на другое время, если обнаруживаются сигналы о том, что одновременно ее осуществляет другое устройство. Для использования этого метода были разработаны традиционные формы Ethernet.

В современных сетях широкое применение технологий коммутации позволило практически полностью исключить первоначальную потребность в CSMA/CD для локальных сетей. Почти все проводные соединения между устройствами в современных локальных сетях являются полнодуплексными, т. е. способными одновременно отправлять и принимать данные. Поэтому несмотря на то, что сети Ethernet разрабатывались с учетом использования технологии CSMA/CD, современные промежуточные устройства позволяют устранить коллизии, и процессы, обеспечиваемые CSMA/CD, в действительности уже не требуются.

Тем не менее для беспроводных соединений в среде локальной сети возможность возникновения таких коллизий все еще необходимо учитывать. Устройства в беспроводной локальной сети применяют метод доступа к среде передачи данных с контролем несущей и предотвращением коллизий (CSMA/CA).

При использовании CSMA/CA (контроль несущей и предотвращение коллизий) устройство проверяет среду передачи данных на наличие в ней сигнала данных. Если среда не загружена, данное устройство отправляет по среде уведомление о намерении использовать ее для передачи данных, затем отправляет данные. Этот способ используется беспроводными сетевыми технологиями стандарта 802.11.

Любой кадр длиной менее 64 байта считается «фрагментом коллизии», или «карликовым кадром», и автоматически отклоняется принимающими станциями.

Для доступа к настройкам сетевых устройств используется консольное подключение.

Консольный порт – это порт управления, обеспечивающий возможность внеполосного доступа к устройству Cisco, т. е. доступа через выделенный административный канал, который применяется исключительно в целях технического обслуживания устройства. Преимущество использования порта консоли состоит в том, что доступ к устройству возможен даже без настройки сетевых услуг, например, начальной конфигурации сетевого устройства. При выполнении начальной конфигурации компьютер подключается к порту

консоли устройства с помощью специального кабеля и запускается программа эмуляции терминала для настройки сетевого оборудования. Команды конфигурации для настройки коммутатора или маршрутизатора можно ввести на подключенном компьютере.

На рисунке 3.4 изображена схема подключения по консольному порту: на тыльной стороне 1 коммутатора расположены силовой разъем для подключения шнура питания 2 и консольный порт 3, обеспечивающий подключение к СОМ-порту компьютера администратора посредством кабеля RJ-45-to-DB-9.

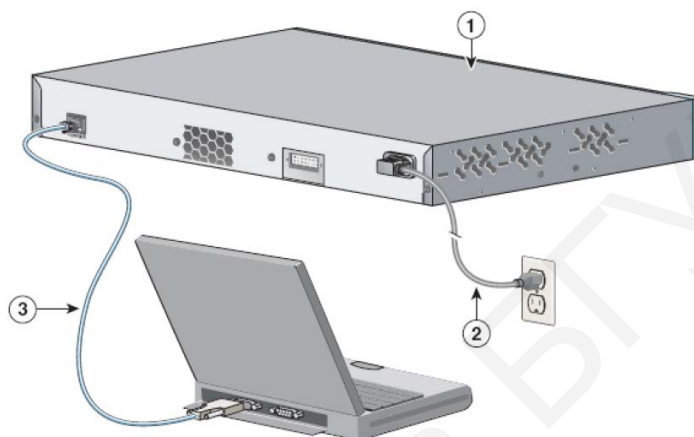


Рисунок 3.4 – Подключение по консольному кабелю к коммутатору

Для обеспечения безопасности устройств Cisco используются иерархические режимы настройки.

**Пользовательский режим (User Mode)** – стандартный режим первоначального доступа к операционной системе (ОС), в который ОС переходит автоматически при продолжительном отсутствии ввода в режиме администратора. В режиме пользователя доступны только простые команды, не влияющие на конфигурацию оборудования. Командная строка в этом режиме имеет следующий вид:  
Switch>

**Привилегированный режим (Privileged Mode)** открывается командой `enable`, введенной в режиме пользователя:  
Switch> enable

В привилегированном режиме доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии, а также команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации, поэтому вход в данный режим должен быть ограничен и безопасен. Командная строка будет иметь следующий вид:  
Switch#

**Режим глобальной конфигурации (Global Configuration Mode)** позволяет вносить изменения в конфигурацию устройства, активизируется следующей командой, введенной в административном режиме:  
Switch# configure terminal

Режимы специфической конфигурации являются подрежимами режима глобальной конфигурации. Например, при вводе в режиме глобальной конфигурации команды `interface FastEthernet 0/0` осуществляется переход в подрежим настройки соответствующего интерфейса (`config-if`). Множество режимов специфической конфигурации соответствует множеству разных ветвей глобальной конфигурации.

Для защиты доступа к привилегированному режиму используется команда `enable secret` пароль. Устаревшая, менее безопасная версия этой команды – `enable password` пароль. Хотя для настройки аутентификации перед доступом в привилегированный режим подходят обе эти команды, рекомендуется использовать `enable secret` пароль. Команда `enable secret` пароль обеспечивает более высокий уровень безопасности, поскольку пароль зашифрован.

Пример команды для установления паролей:

```
Switch(config)# enable secret пароль
```

Консольный порт сетевых устройств также необходимо защищать надежным паролем, что снижает вероятность доступа неавторизованных сотрудников. Чтобы установить пароль для консоли в режиме глобальной конфигурации, необходимо ввести следующие команды:

```
Switch(config)#line console 0
Switch(config-line)#password <пароль>
Switch(config-line)#login
Switch(config-line)#exec-timeout <время>
Switch(config-line)#exit
Switch(config)#exit
Switch#exit
```

В режиме глобальной конфигурации используется команда **line console 0**, чтобы войти в режим конфигурации строки для консоли. Ноль используется для обозначения первого интерфейса консоли.

Вторая команда `password` пароль определяет пароль для консоли строки.

Команда `login` настраивает коммутатор для аутентификации при входе в систему. Если включена процедура входа и настроен пароль, пользователь консоли должен будет ввести пароль, чтобы получить доступ к интерфейсу командной строки (CLI).

Также рекомендуется задавать значения тайм-аута с помощью команды `exec-timeout` время. Настройка тайм-аута сообщает устройству Cisco о необходимости отключения пользователей от линии, если они неактивны, в течение указанного периода времени.

Для удаленного доступа к коммутатору на его виртуальном интерфейсе нужно настроить IP-адрес и маску подсети, для этого используется последовательность команд:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
```

```
Switch(config-if)#description LAN
Switch(config-if)#no shutdown
```

В приведенных выше командах `interface vlan 1` – применяется для перехода в режим настройки интерфейса из режима глобальной конфигурации; `ip address 192.168.10.2 255.255.255.0` – настраивает IP-адрес и маску подсети для коммутатора; `description LAN` – задает краткое описание; `no shutdown` – активирует интерфейс.

Коммутаторы Cisco поддерживают три типа режима:

- full – полнодуплексный режим;
- half – полудуплексный режим;
- auto – автоматическое согласование дуплексного режима.

При включении автоматического согласования два порта связываются друг с другом, чтобы определить оптимальный режим работы.

Например, для настройки полудуплексного режима интерфейса используется следующая команда:

```
Switch(config-if)#interface fastEthernet 0/1
Switch(config-if)#duplex half
```

Файл текущей конфигурации отражает текущую конфигурацию, функционирующую на устройстве CISCO IOS. Изменения текущей конфигурации незамедлительно влияют на работу устройства Cisco. Файл текущей конфигурации хранится в рабочей памяти устройства или в оперативном запоминающем устройстве (ОЗУ). Это означает, что файл текущей конфигурации временно активен, когда устройство Cisco работает (подключено к питанию). Однако при отключении питания или перезапуске устройства все несохраненные изменения конфигурации будут потеряны. Поэтому каждый раз после завершения настройки сетевого устройства необходимо выполнить резервное копирование файла конфигурации в NVRAM и проверить, чтобы внесенные изменения не потерялись после перезагрузки системы и отключения питания.

Команду `show running-config` можно применять при просмотре файла текущей конфигурации. Когда изменения проверены, необходимо использовать команду для сохранения файла текущей конфигурации в файл загрузочной конфигурации:

```
Switch# copy running-config startup-config
```

После выполнения команды файл текущей конфигурации обновляет файл загрузочной конфигурации.

Если изменения, внесенные в ходе конфигурации, не принесли желаемого результата, возможно, понадобится восстановить предыдущую конфигурацию устройства. Лучше всего это осуществляется путем перезапуска устройства и ввода команды `reload` в командной строке привилегированного режима. Выполняя перезагрузку, система определит, что измененная конфигурация не была сохранена в файл начальной конфигурации.

Для просмотра таблицы MAC-адресов на коммутаторе используется следующая команда:

```
Switch#show mac-address-table
```

Команда `clear mac-address-table dynamic` применяется для очистки таблицы MAC-адресов.

### 3.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе №1. До начала выполнения необходимо открыть сохраненный файл с именем **lab1-2.pkt**, полученный в лабораторной работе №1, и проверить правильность соединений. В данной работе необходимо осуществить настройку всех коммутаторов в смоделированной сети, учитывая следующие указания.

1. Выбрать консольный кабель (раздел «Connections» → «Console») и подсоединить любой компьютер (порт RS232) к коммутатору (порт «Console»).

2. На данном компьютере зайти на вкладку «Desktop», выбрать приложение «Terminal», не изменяя параметры, нажать «Ok». Осуществиться подключение к настройкам коммутатора (рисунок 3.5).

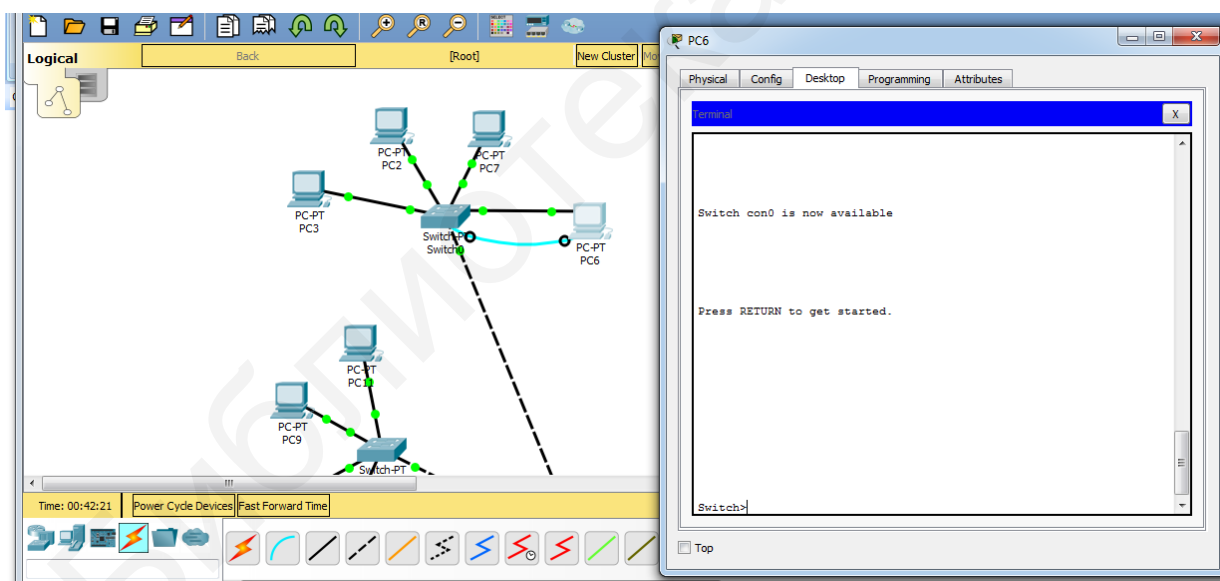


Рисунок 3.5 – Осуществление консольного подключения к коммутатору

3. В окне «Terminal» нажать «Enter». Произойдет автоматический переход в режим конфигурации. Используя команды из теоретической части, перейти в режим глобальной конфигурации. Настроить пароль и значение тайм-аута в соответствии с первой цифрой шифра из таблицы 3.1.

Таблица 3.1 – Данные для настройки пароля консольного подключения

Первая цифра шифра	Параметры для ограничения доступа к консоли		Пароль для доступа к привилегированному режиму
	Пароль	Значение тайм-аута, мин	
1	cisco1	2	cisco1cisco
2	cisco22	3	cisco22cisco
3	cisco333	4	cisco333cisco
4	admin45	1	admin45admin
5	console12	5	console12console
6	admin89	6	admin89admin
7	admin55	7	admin55admin
8	console11	9	console11console
9	cisco88	10	cisco88cisco
0	cisco66	11	cisco66cisco

4. Проверить правильность настройки пароля, осуществив подключение с другого компьютера по консоли. Проверить, что в файле текущей конфигурации коммутаторов присутствуют настройки пароля, используя команду `show running-config`.

5. Настроить виртуальные интерфейсы всех коммутаторов для удаленного доступа, используя не занятые в сети IP-адреса. Заполнить таблицу 3.2.

Таблица 3.2 – Таблица адресации устройств в смоделированной сети

Имя устройства	IP-адрес	Описание

6. Отобразить таблицу MAC-адресов коммутатора. Если в ней присутствуют какие-то адреса, очистить таблицу. Перейти в режим симуляции и отправить ICMP-пакет с помощью команды `ping` с любого компьютера. Зафиксировать в виде снимков экрана последовательность передачи пакетов и объяснить процесс заполнения таблицы MAC-адресов коммутатора по примеру рисунка 3.1. Просмотреть таблицу MAC-адресов коммутатора и заполнить таблицу 3.3.

Таблица 3.3 – Таблица MAC-адресов коммутатора

MAC-адрес	Тип/Порт	Имя подключенного к данному порту устройства

7. Просмотреть таблицу MAC-адресов на компьютере, с которого осуществлялась отправка ICMP-пакета. Представить таблицу MAC-адресов в отчете.

8. Осуществить настройку полудуплексного режима для портов, указанных в таблице 3.3. Реализовать коллизию, по примеру рисунка 3.3. Для этого в режиме симуляции одновременно отправить ICMP-пакеты с двух компьютеров, указанных в таблице 3.3. Представить в отчете пример коллизии.

9. Осуществить настройку полнодуплексного режима для портов, указанных в таблице 3.3.

10. В случае исправной работы всей сети скопировать в отчет содержание файла текущей конфигурации, для чего выполнить команду `show running-config`. Скопировать текущую конфигурацию коммутатора в загрузочную, используя команду `copy running-config startup-config`. Сохранить файл с именем **lab3.pkt**.

### 3.3 Содержание отчета

1. Цель работы, исходные данные из таблицы 3.1.
2. Результаты произведенных настроек (заполненные таблицы 3.2, 3.3, результаты выполнения команд из пунктов 6, 8, 10 подраздела 3.2), изображение смоделированной в данной работе сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

### 3.4 Контрольные вопросы и задания

1. Объяснить принцип работы коммутатора.
2. Перечислить типы режимов работы коммутатора, их отличия, достоинства и недостатки.
3. Пояснить сущность метода ассоциативного доступа.
4. Сформулировать особенности метод множественного доступа с контролем несущей.
5. Как можно предотвратить появление коллизий?
6. Назвать назначения и основные отличия методов CSMA/CA и CSMA/CD.
7. Объяснить назначение и особенности консольного подключения.
8. Каковы виды режимов конфигурации коммутатора?

## **ЛАБОРАТОРНАЯ РАБОТА №4**

### **БАЗОВАЯ НАСТРОЙКА МАРШРУТИЗАТОРА**

**Цель:** изучить структуру IP-протокола; овладеть навыками настройки проводных и беспроводных маршрутизаторов.

#### **4.1 Теоретическая часть**

Третий, сетевой, уровень модели OSI предоставляет сервисы, с помощью которых пакеты направляются к узлу назначения в другой сети. Для перемещения к другим сетям пакет должен быть обработан маршрутизатором, роль которого заключается в том, чтобы выбрать пути для пакетов и направить их к узлу назначения. Такой процесс называется маршрутизацией. До того как достигнуть узла назначения, пакет может пройти через несколько промежуточных устройств. Каждый маршрут на пути пакета к узлу назначения называется переходом.

Основной протокол сетевого уровня – протокол IP, который обеспечивает только функции, необходимые для доставки пакета от узла источника к узлу назначения по взаимосвязанной системе сетей. Этот протокол не предназначен для мониторинга и управления потоком пакетов. При необходимости эти функции выполняют другие протоколы на других уровнях.

Основные характеристики IP можно сформулировать следующим образом:

- не требуется предварительное установление соединения, т. е. перед отправкой пакетов данных соединение с узлом назначения не устанавливается;
- доставка пакетов не гарантируется;
- независимость от среды.

Главная роль сетевого протокола – пересылка пакетов между узлами при наименьшей нагрузке на сеть. Сетевой уровень не имеет отношения (и даже не обладает какой-либо информацией) к типу обмена данными, который содержится внутри пакета. IP является протоколом без установления соединения, а это означает, что перед отправкой данных выделенное сквозное соединение не устанавливается. По своей сути обмен данными без установления соединения аналогичен отправке письма без предварительного уведомления получателя.

Протокол IP не использует соединения и, следовательно, ему не требуется первоначальный обмен контрольной информацией для установления сквозного подключения до начала пересылки пакетов. IP также не нуждается в дополнительных полях в заголовке блока данных протокола (PDU) для поддержки установленного соединения. Этот процесс значительно снижает нагрузку IP. Тем не менее без предварительно установленного сквозного подключения отправителям неизвестно, имеются ли устройства-адресаты и способны ли они функционировать в момент отсылки



пакетов, а также получит ли пакет узел назначения и смогут ли устройства-адресаты получить доступ к пакету и прочитать его.

Протокол IP не способен контролировать не доставленные или поврежденные пакеты и восстанавливаться в случае их появления. Это связано с тем, что хотя отправляемые пакеты IP и содержат сведения о месте доставки, в них отсутствует информация, которую можно обработать, чтобы сообщить отправителю об успешно выполненной доставке. Заголовок пакета не содержит данных синхронизации для отслеживания очередности доставки пакетов. Также не предусмотрены подтверждения доставки пакетов по IP и отсутствуют данные контроля ошибок, с помощью которых можно отследить, доставлены ли пакеты без повреждений. Пакеты могут прибыть на узел назначения поврежденными или с нарушенным порядком либо не прибыть совсем. В случае возникновения таких ошибок информация, которая содержится в заголовке IP, не позволяет выполнить повторную пересылку пакетов.

Если отсутствие пакетов или несоблюдение очередности создает проблемы для приложений, использующих данные, сервисы верхнего уровня, например TCP, должны устранить эти проблемы. Это обеспечивает высокую эффективность работы протокола IP. Если нагрузки надежности были включены в IP, то процессы обмена данными, для которых не требуется подключение, или надежность могут пострадать от уменьшения пропускной способности и задержек, вызванных такими нагрузками. В пакете протоколов TCP/IP транспортный уровень может использовать либо TCP, либо UDP, в зависимости от необходимости обеспечения надежности передачи данных. Если решение об обеспечении надежности принимается на транспортном уровне, это позволяет IP быстрее адаптироваться к различным типам передачи данных.

Пакет IPv4 состоит из двух частей:

- заголовок IP определяет характеристики пакета;
- полезная нагрузка содержит информацию сегмента уровня 4 и фактические данные.

Как показано на рисунке 4.1, заголовок пакета IPv4 состоит из нескольких полей, включающих важную информацию о пакете. Эти поля содержат двоичные числа, которые анализируются процессом уровня 3. Двоичные значения каждого поля определяют различные параметры пакета IP.

Далее представлено описание наиболее важных полей в заголовке IPv4.

**Версия** включает в себя 4-битное двоичное значение, определяющее версию IP-пакета. Для пакетов IPv4 в этом поле всегда указано значение 0100.

**Дифференцированные сервисы (DS)** – это 8-битное поле, используемое для определения приоритета каждого пакета. Первые 6 бит определяют значение точки кода дифференцированных сервисов (DSCP), которое используется механизмом обеспечения качества обслуживания (QoS). Последние 2 бита определяют значение явного уведомления о перегрузке (ECN), которое можно использовать для предотвращения потери пакетов во время перегрузки сети.

Байт 1		Байт 2		Байт 3		Байт 4	
Версия	Длина заголовка Internet	Дифференциальные услуги (DS)		Общая длина			
		DSCP	ENC				
Идентификация				Флаг	Смещение фрагмента		
Время существования		Протокол		Контрольная сумма заголовка			
IP-адрес источника							
IP-адрес назначения							
Параметры (дополнительно)						Заполнитель	

Рисунок 4.1 – Формат заголовка IPv4

**Время существования (TTL)** содержит 8-битное двоичное значение, используемое для ограничения времени существования пакета. Оно указывается в секундах, но обычно подразумевает количество переходов. Отправитель пакета устанавливает начальное значение времени существования (TTL), которое уменьшается на единицу, или переход в процессе каждой обработки пакета маршрутизатором. Если значение в поле TTL уменьшается до нуля, маршрутизатор отбрасывает пакет и отправляет на IP-адрес источника сообщение о превышении времени протокола ICMP (управление сообщениями в сети). Команда **traceroute (tracert)** задействует это поле, чтобы определить маршруты, использованные между источником и назначением.

**Протокол** – 8-битное двоичное значение, указывающее тип полезной нагрузки данных, которые переносит пакет, что позволяет сетевому уровню пересылать данные на соответствующий протокол более высокого уровня. Часто встречаются значения ICMP (1), TCP (6) и UDP (17).

**IP-адрес источника** содержит 32-битное двоичное значение, которое представляет IP-адрес источника пакета.

**IP-адрес назначения** содержит 32-битное двоичное значение, которое представляет IP-адрес назначения пакета.

Два наиболее часто используемых поля, IP-адрес источника и IP-адрес назначения определяют, откуда поступил пакет и куда он направляется. Обычно в процессе передачи от узла источника к узлу назначения эти адреса не меняются.

Далее описаны поля, используемые для определения и проверки пакета.

**Длина заголовка Интернета (IHL)** содержит 4-битное значение, определяющее число 32-битных слов в заголовке. Значение IHL может

отличаться в зависимости от полей «Параметры» и «Заполнитель». Минимальное значение этого поля – 5 (т. е.  $5 \cdot 32 = 160$  бит = 20 байт), а максимальное значение – 15 (т. е.  $15 \cdot 32 = 480$  бит = 60 байт).

**Общая длина** – 16-битное поле, которое иногда называется длиной пакета. Определяет размер всего пакета (фрагмента), включая заголовок и данные и выражает его в байтах. Пакет минимальной длины составляет 20 байт (20-байтный заголовок + 0 байт данных), пакет максимальной длины – 65 535 байт.

**Контрольная сумма заголовка** – 16-битное поле, которое используется для проверки ошибок в заголовке IP. Контрольная сумма заголовка рассчитывается повторно и сравнивается со значением в поле контрольной суммы. Если значения не совпадают, то пакет отбрасывается.

Маршрутизатору может понадобиться выполнить фрагментацию пакета при его пересылке из одной среды передачи данных в другую с меньшим максимальным размером пакета. В этом случае выполняется фрагментация, а пакет IPv4 использует поля для отслеживания образовавшихся фрагментов, а именно:

- **идентификация** – 16-битное поле, которое однозначно определяет фрагмент исходного пакета IP;

- **флаги** – 3-битное поле, которое определяет способ фрагментации пакета и используется с полями «Смещение фрагмента» и «Идентификация» для упрощения восстановления фрагментов в исходный пакет;

- **смещение фрагмента** – 13-битное поле, определяющее порядок, в котором необходимо расположить фрагменты при восстановлении исходного нефрагментированного пакета.

Шлюз по умолчанию – это устройство, которое направляет трафик из локальной сети к устройствам в удаленных сетях. В домашних условиях или на малых предприятиях шлюз по умолчанию часто используется для подключения локальной сети к Интернету.

При отправке пакета устройству другой IP-сети узел должен пересылать его через промежуточное устройство к шлюзу по умолчанию, так как главное устройство не сохраняет информацию о маршрутизации за пределами локальной сети, чтобы достичь удаленных адресатов, а шлюз по умолчанию сохраняет. В роли шлюза по умолчанию чаще всего выступает маршрутизатор, который сохраняет таблицу маршрутизации.

Таблица маршрутизации – это файл данных в ОЗУ, используемый в целях хранения информации о маршрутах для сетей, подключенных напрямую, а также записей удаленных сетей, о которых стало известно устройству. Маршрутизатор использует информацию из таблицы маршрутизации, чтобы определить наилучший путь к узлам назначения.

На узлах должна храниться их собственная локальная таблица маршрутизации, чтобы пакеты сетевого уровня гарантированно направлялись

к нужной сети назначения. На узле для отображения таблицы маршрутизации узла можно использовать команду `netstat -r`.

После ввода команды `netstat -r` будут отображены следующие три раздела, относящиеся к текущим сетевым подключениям TCP/IP:

- **список интерфейсов** содержит адрес управления доступом к среде (MAC) и присвоенный номер интерфейса с поддержкой сети на узле, включая адаптеры Ethernet, Wi-Fi и Bluetooth;

- **таблица маршрутизации IPv4** содержит все известные маршруты, включая прямые подключения, локальные сети и локальные маршруты, используемые по умолчанию.

Таблица маршрутизации состоит из пяти столбцов, включающих следующие данные:

- **Network Destination** (Сеть назначения) – список достигаемых сетей;
- **Netmask** (Маска сети) – маска подсети, которая сообщает узлу, как следует определять сеть и узловые части IP-адреса;

- **Gateway** (Шлюз) – адрес, который используется локальным компьютером, чтобы достичь удаленного сетевого адресата; если узел назначения доступен напрямую, в этом столбце он будет отображен как «On-link» (Соединено);

- **Interface** (Интерфейс) – адрес физического интерфейса, который применяется для отправки пакета к шлюзу, используемому для достижения сетевого адресата;

- **Metric** (Метрика) – стоимость каждого маршрута для определения наилучшего маршрута к адресату.

Как правило, локальная таблица узла содержит следующую информацию:

- **прямое подключение** – маршрут к интерфейсу `loopback` (127.0.0.1);
- **маршрут локальной сети** – информация о сети, к которой подключен узел, автоматически добавляется в таблицу маршрутизации узла;

- **локальный маршрут по умолчанию** – это маршрут, который должны пройти пакеты, чтобы достичь всех удаленных сетевых адресов, и который создается в том случае, когда на узле имеется адрес шлюза по умолчанию;

- **адрес шлюза по умолчанию** – это IP-адрес сетевого интерфейса маршрутизатора, подключенного к локальной сети; его можно настроить на узле вручную либо получить динамически.

Важно отметить, что маршрут по умолчанию, а следовательно, и шлюз по умолчанию используется только в том случае, если узлу необходимо пересылать пакеты к удаленной сети. Он не требуется (и его можно даже не настраивать), если происходит только отправка пакетов устройствам в локальной сети.

Настройка маршрутизатора выполняется практически аналогично настройке коммутатора. При конфигурировании маршрутизатора также используются иерархические режимы настройки (пользовательский,

привилегированный, режим глобальной конфигурации, режимы специфической конфигурации).

Для настройки интерфейсов применяется команда `interface FastEthernet номер_интерфейса`, которая вводится в режиме глобальной конфигурации. Далее необходимо назначить IP-адрес для каждого интерфейса с помощью команды `ip address IP-адрес маска_подсети`. Обязательно необходимо ввести команду `no shutdown`, чтобы включить данный интерфейс. Команда `speed` используется для настройки скорости передачи (возможны режимы 10 Мбит/с, 100 Мбит/с, 1000 Мбит/с, автоматическая настройка скорости). Далее представлен пример настройки интерфейса `fastEthernet 0/1`.

```
router#configure terminal
router(config)#interface fastEthernet 0/1
router(config-if)#ip address 192.168.0.1 255.255.255.0
router(config-if)#speed 100
router(config-if)#description LAN1
router(config-if)#no shutdown
router(config-if)#exit
```

Настройка паролей происходит аналогично настройке паролей на коммутаторе (см. лабораторную работу №3).

Для просмотра таблицы маршрутизации используется команда `show ip route`. Команда `show ip interface` отображает информацию о настройках интерфейса. Краткую информацию о данных настройках можно получить с помощью команды `show ip interface brief`.

Для настройки маршрутизации при подсоединении построенной сети к другим сетям используются следующие команды:

```
Router (config)#router rip
Router (config-router)#version 2
Router (config-router)#network 192.168.83.0
Router (config-router)#no auto-summary
```

Команда `router rip` применяется для указания протокола маршрутизации RIP, также необходимо указать версию протокола с помощью команды `version 2`. IP-адрес для новой подключаемой сети указывается с помощью команды `network`. Команда `no auto-summary` отключает автоматические настройки маршрутизации.

Большинство маршрутизаторов предоставляют функции как проводной коммутации, так и беспроводного подключения, а также выполняют функцию точки доступа в беспроводной сети.

К беспроводным сетям применимы следующие стандарты передачи данных:

- **стандарт IEEE 802.11** – технология беспроводных локальных сетей (WLAN), которая чаще всего называется Wi-Fi и использует конкурирующую или недетерминированную систему с множественным доступом с контролем несущей (CSMA/CA);

- **стандарт IEEE 802.15** – стандарт беспроводной персональной сети, более известный как Bluetooth; для передачи данных на расстояниях от 1 до 100 м требует близкого расположения двух устройств.

Существуют следующие стандарты IEEE 802.11 в зависимости от диапазона частот и скорости передачи:

- **IEEE 802.11a**. Частотный диапазон – от 5 ГГц, скорость – до 54 Мбит/с. Поскольку этот стандарт работает на более высоких частотах, он имеет меньшую зону покрытия и менее эффективен внутри зданий. Устройства, работающие в соответствии с данным стандартом, несовместимы со стандартами 802.11b и 802.11g, описанными ниже.

- **IEEE 802.11b**. Частотный диапазон – от 2,4 ГГц, скорость – до 11 Мбит/с. Устройства, работающие в соответствии с этим стандартом, имеют больший диапазон и эффективнее работают внутри зданий по сравнению с устройствами стандарта 802.11a.

- **IEEE 802.11g**. Частотный диапазон – от 2,4 ГГц, скорость – до 54 Мбит/с. Устройства, функционирующие в соответствии с этим стандартом, работают с той же радиочастотой и диапазоном, что и устройства со стандартом 802.11b, но имеют пропускную способность стандарта 802.11a.

- **IEEE 802.11n**. Частотные диапазоны – 2,4 и 5 ГГц, скорость – от 150 до 600 Мбит/с, работает на расстоянии до 70 м. Этот стандарт обладает обратной совместимостью с устройствами стандартов 802.11a/b/g.

- **IEEE 802.11ac**. Полоса частот – 5 ГГц, скорость передачи данных – от 450 до 1300 Мбит/с (1,3 Гбит/с). Совместим с прежними версиями устройств 802.11a/n.

- **IEEE 802.11ad** (также называется «WiGig»). Этот стандарт использует связь Wi-Fi с тремя частотными диапазонами: 2,4, 5 и 60 ГГц, а также теоретически обеспечивает скорость передачи до 7 Гбит/с.

Беспроводное соединение устройств к локальной сети обеспечивает беспроводную передачу данных. Обычно для установления беспроводной локальной сети требуются следующие сетевые устройства:

- **беспроводные сетевые адаптеры** обеспечивают беспроводную связь для каждого сетевого узла;

- **точка беспроводного доступа (AP)**, которая концентрирует беспроводные сигналы от пользователей и с помощью медного кабеля подключается к имеющейся сетевой инфраструктуре, например к Ethernet. Беспроводные маршрутизаторы для дома и малых предприятий сочетают функции маршрутизатора, коммутатора и точки доступа в одном устройстве.

В Cisco Packet Tracer присутствует модель Wi-Fi маршрутизатора WRT300N, который находится в разделе «Wireless Devices» (рисунок 4.2). К данному маршрутизатору могут подключаться такие оконечные устройства, как персональный компьютер, ноутбук, мобильный телефон, планшет (расположенные в разделе «End devices»). При этом в ноутбуке следует установить интерфейсную плату для беспроводного соединения. Сначала в настройках устройства необходимо его выключить. Затем удалить интерфейсную карту,

которая установлена по умолчанию, и добавить карту WPC300N (рисунок 4.3). Включить устройство.

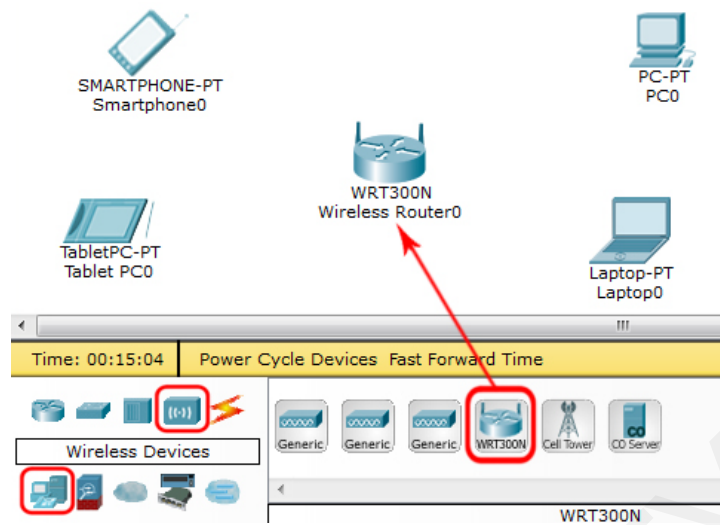


Рисунок 4.2 – Установка беспроводного маршрутизатора

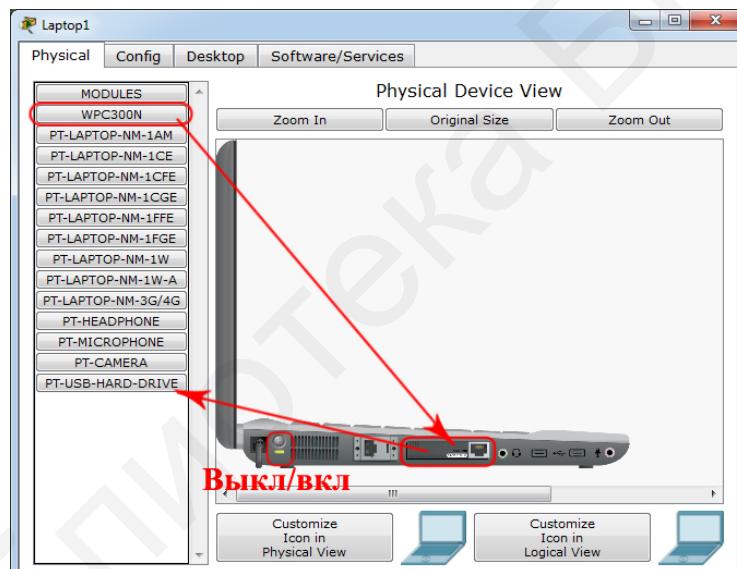


Рисунок 4.3 – Установка беспроводной интерфейсной платы в ноутбук

Для настройки беспроводного маршрутизатора необходимо соединить Ethernet-порты персонального компьютера и маршрутизатора. Когда идентификаторы подключения загорятся зеленым цветом, в настройках компьютера на вкладке «Desktop» выбрать «IP configuration» и установить «DHCP». В результате маршрутизатором компьютеру автоматически будет выдан IP-адрес. На этой же вкладке в веб-браузере «Web Browser» после ввода IP-адреса 192.168.0.1 осуществляется подключение к настройкам маршрутизатора (рисунок 4.4). Для входа в режим конфигурации необходимо ввести пароль и логин (по умолчанию и логин, и пароль – «admin»).

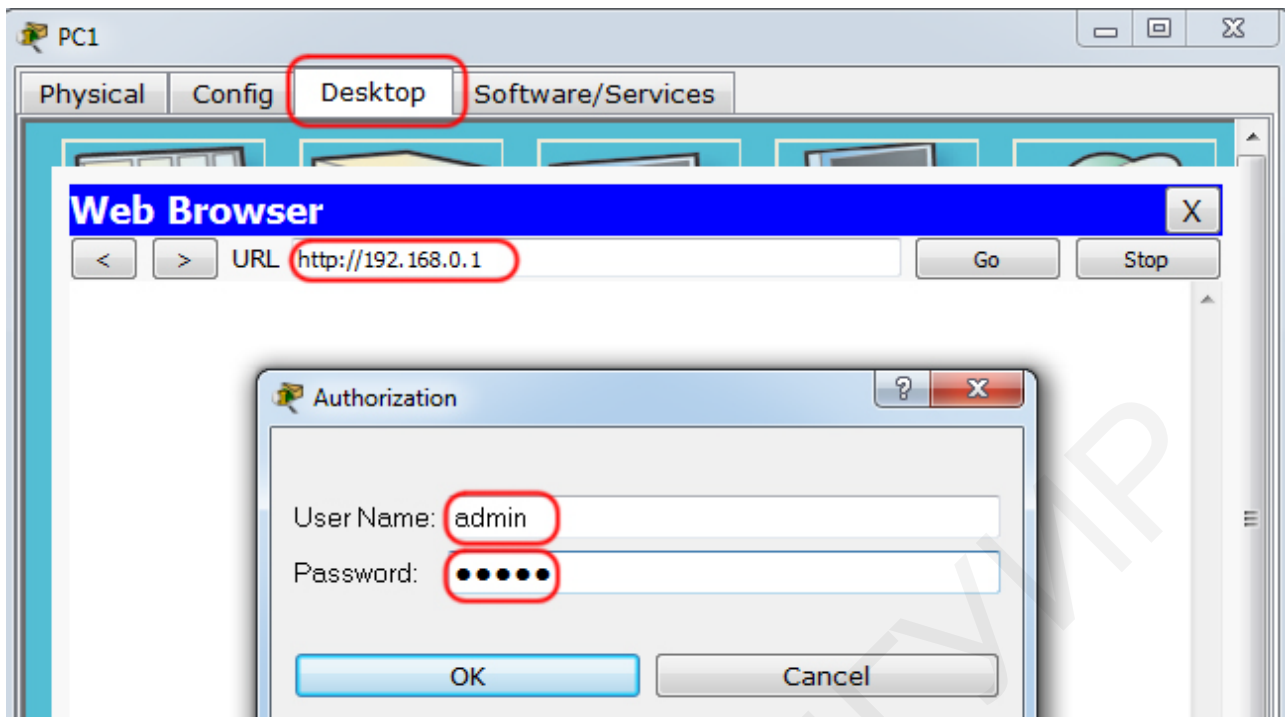


Рисунок 4.4 – Вход в конфигурацию беспроводного маршрутизатора

На рисунке 4.5 представлено окно настройки маршрутизатора. В области 1 настраивается публичный IP-адрес маршрутизатора для связи с Интернетом, в области 2 – частный IP-адрес маршрутизатора и маска подсети. В области 3 разрешается или запрещается автоматическая раздача IP-адресов, включение DHCP-сервера. После нажатия кнопки «DHCP Regervation» появляется окно резервирования IP-адресов (на рисунке 4.5 справа). В данном окне в области 5 показаны все IP-адреса подключенных устройств с указанием MAC-адресов. Их можно жестко закрепить, зарезервировать за устройствами, для чего необходимо поставить галочку в колонке «Select» для нужного устройства и нажать кнопку «Add client». Устройство будет добавлено в таблицу в области 7 и указанный IP-адрес будет закреплен за данным устройством. В области 6 можно вручную ввести имя устройства, его IP- и MAC-адрес и, нажав кнопку «Add», добавить в таблицу в области 7.

В области 4 указывается начальный IP-адрес для подключенных к беспроводной сети устройств и возможное максимальное количество подключаемых устройств. Автоматически будет показан диапазон используемых IP-адресов в организованной беспроводной сети. После внесенных изменений обязательно надо нажать кнопку «Save settings» в самом низу окна настроек маршрутизатора. После чего произойдет перезагрузка и возможно будет потеряно соединения. Если в области 2 был указан другой IP-адрес маршрутизатора, то для возврата в окно настроек его необходимо внести в адресную строку браузера.



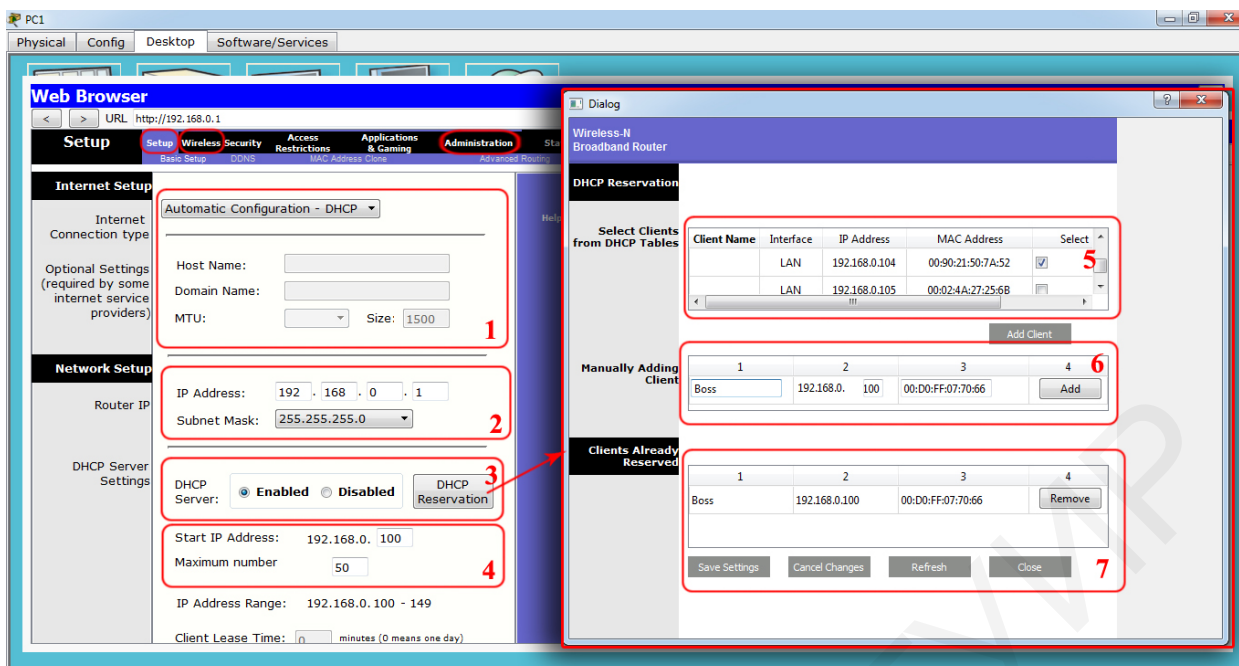


Рисунок 4.5 – Базовые настройки беспроводного маршрутизатора

Во вкладке «Wireless»→ «Basic Wireless Settings» (рисунок 4.6) задаются тип сети, идентификатор сети (SSID) диапазон частот (стандартный 20 МГц или широкий 40 МГц), номера каналов, также возможно включение или отключение широковещательной рассылки SSID. Для увеличения безопасности целесообразнее отключать широковещательную рассылку SSID, так злоумышленники не будут знать, что такая сеть существует, и не смогут к ней подключиться, не зная ее SSID. При этом пользователь для подключения к данной сети должен будет в настройках своего устройства задать вручную SSID.

Во вкладке «Wireless»→«Wireless Security» задаются тип и ключ шифрования, во вкладке «Wireless»→«Wireless MAC Filter» – MAC-адреса устройств, которым можно запретить (prevent) или разрешить (permit) доступ в беспроводную сеть. Так на рисунке 4.6 запрещен доступ в беспроводную сеть устройствам с MAC-адресами 00:00:0C:15:C5:1B, 00:0B:BE:87:1A:32 и др.

Самым главным действием по обеспечению безопасности беспроводной сети является изменение пароля на маршрутизаторе. Если этим пренебречь, то злоумышленник может получить доступ к настройкам маршрутизатора и ко всем данным, которые через него проходят. Во вкладке «Administration» (рисунок 4.7) вводится и повторяется новый пароль, во вкладке «Administration» → «Firmware upgrate» по нажатию кнопки «Browse» можно выбрать обновления для данного маршрутизатора, при нажатию «Save settings» обновление будет установлено.

В каждом устройстве во вкладке «Config» → «Wireless» необходимо указать SSID беспроводной сети, тип шифрования и ключ, а также установить DHCP (рисунок 4.8). Таким образом, всем устройствам будет присвоен IP-адрес, и они будут подключены к беспроводной сети, за исключением тех,

MAC-адреса которых указаны в таблице фильтрации (рисунок 4.9). Протестировать работу сети можно командой ping во вкладке «Desktop» → «Command prompt» любого оконечного устройства.

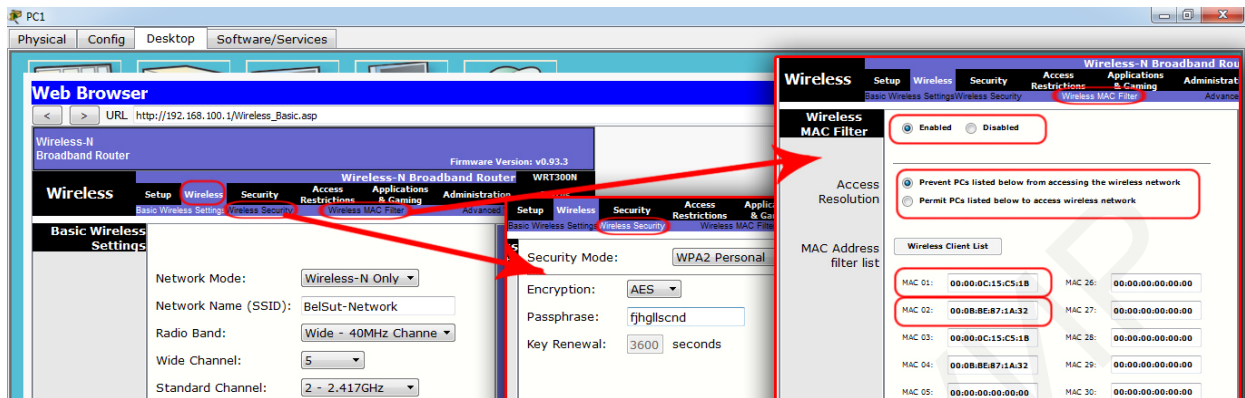


Рисунок 4.6 – Настройка названия и типа сети, шифрования и MAC-фильтрации

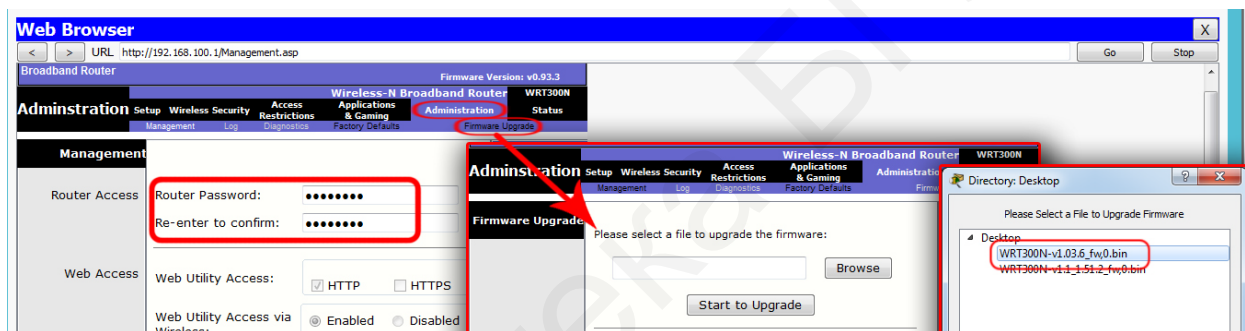


Рисунок 4.7 – Административная настройка маршрутизатора

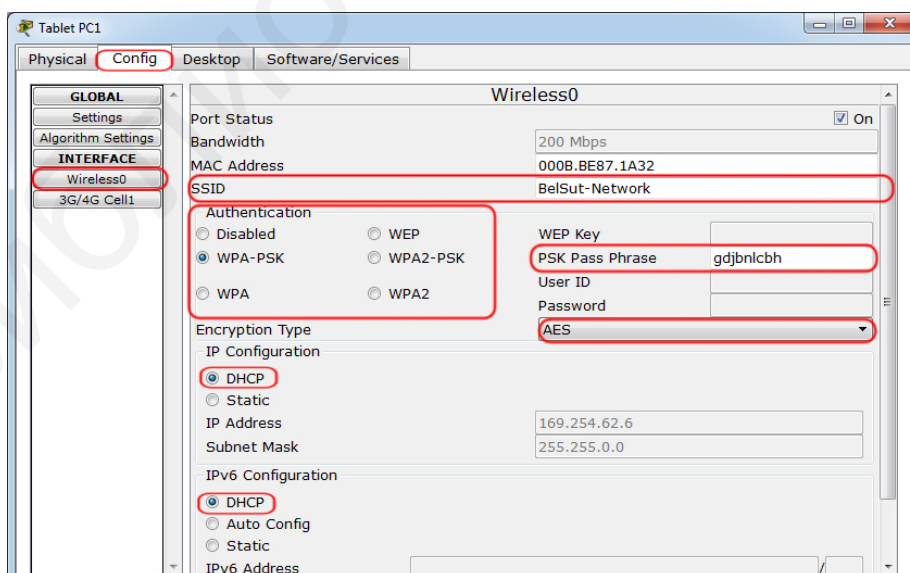


Рисунок 4.8 – Настройка беспроводной сети на оконечном устройстве

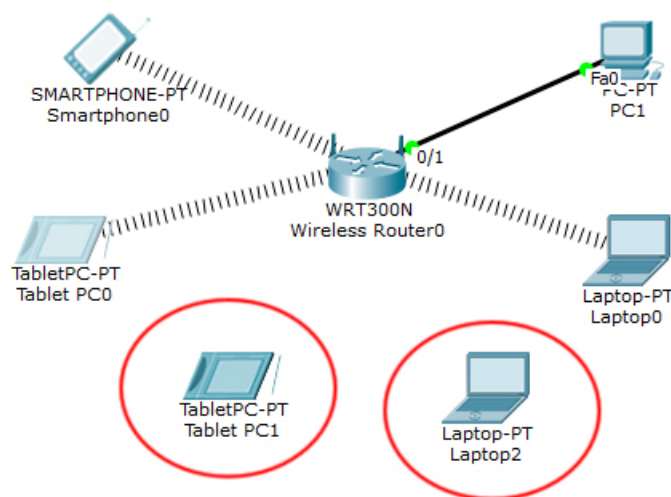


Рисунок 4.9 – Смоделированная беспроводная сеть

Для объединения беспроводной сети, представленной на рисунке 4.9, с другими сетями используется модем (Cable Modem), который находится в разделе «Network Devices» → «WAN Emulation». К данному модему с помощью витой пары подключается беспроводной маршрутизатор, с помощью коаксиального кабеля – облако (Cloud), находящееся в разделе «Network Devices» → «WAN Emulation». По такому принципу строятся домашние локальные сети (рисунки 4.10).

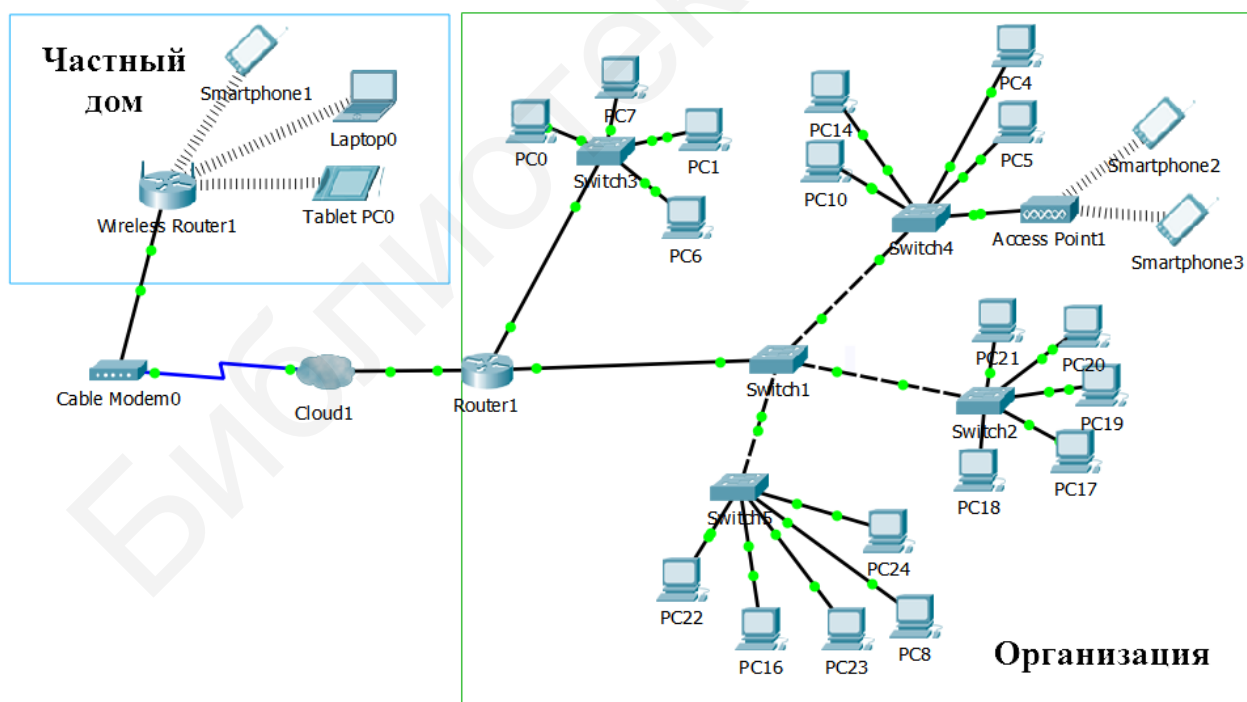


Рисунок 4.10 – Смоделированная сеть организации и частного дома

В настройках облака необходимо на закладке «Config» для интерфейса Ethernet указать тип сети провайдера «Cable». В кабельном соединении «Cable» выбрать типы портов, которые будут соединяться облаком, и нажать кнопку «Add». В сетях организации для создания беспроводных сетей (см. рисунок 4.11) используются точки доступа (AccessPoint), их можно выбрать в разделе «Network Devices»→«WAN Emulation». В настройках данного устройства на закладке «Config» для интерфейса Port 1 устанавливаются идентификатор сети SSID и ключ аутентификации.

## 4.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе №3. До начала выполнения необходимо открыть сохраненный файл с именем lab3.pkt, полученный в лабораторной работе №3, и проверить правильность соединений. В данной работе необходимо добавить маршрутизатор, учитывая следующие указания.

1. Осуществить подключение одного из коммутаторов построенной в лабораторной работе №3 сети к любому интерфейсу маршрутизатора 2811 (раздел «Routers» → «2811»). Пример сети представлен на рисунке 4.11.

2. Осуществить настройку интерфейса маршрутизатора в соответствии с IP-адресом построенной сети с помощью консольного подключения с любого компьютера. Настроить шлюз по умолчанию в сетевых настройках компьютеров в соответствии со второй цифрой шифра из таблицы 1.3 лабораторной работы №1. Настроить пароль и значение тайм-аута в соответствии с первой цифрой шифра из таблицы 3.1 лабораторной работы №3. Проверить правильность настройки пароля, осуществив подключение с другого компьютера по консоли и проверив файл текущей конфигурации маршрутизатора с помощью команды `show running-config`.

3. Построить еще одну сеть и подключить ее к другому интерфейсу маршрутизатора, осуществить настройку компьютеров и интерфейса маршрутизатора в соответствии с таблицей 4.1.

Таблица 4.1 – Настройка IP-адресации сети

Вторая цифра шифра	Количество компьютеров	IP-адрес	IP-адрес маршрутизатора
0	5	192.168.11.2–192.168.11.100	192.168.11.1
1	3	192.168.12.2–192.168.12.100	192.168.12.1
2	4	192.168.120.2–192.168.120.100	192.168.120.1
3	5	192.168.57.2–192.168.57.100	192.168.57.1
4	6	192.168.33.2–192.168.33.100	192.168.33.1
5	4	192.168.10.2–192.168.10.100	192.168.10.1
6	3	192.168.7.2–192.168.7.100	192.168.7.1
7	5	192.168.5.2–192.168.5.100	192.168.5.1
8	4	192.168.115.2–192.168.115.100	192.168.115.1
9	6	192.168.77.2–192.168.77.100	192.168.77.1

4. Просмотреть таблицу маршрутизации и краткую информацию о настройках интерфейса маршрутизатора, вставить в отчет.

5. Перейти в режим симуляции времени. Проверить правильность произведенных настроек с помощью отправки ICMP-сообщения из одной сети в другую. Отправить ICMP-пакет с любого компьютера, используя команду ping. Проследить прохождение пакета, нажимая кнопку «Capture/Forward», и заполнить таблицу 4.2. Проанализировать передачу сообщений и сделать вывод о разнице передачи данных в сети с маршрутизатором и без него (сравнить с таблицей 2.2 из лабораторной работы №2).

Таблица 4.2 – Последовательность действий в смоделированной сети при отправке ping-запроса

Номер шага	Отправитель	Получатель	Содержание уровня	Описание действий
1				
2				
3				

6. Проверить таблицу маршрутизации на компьютере, с которого осуществлялась отправка ICMP-сообщения, вставить в отчет.

7. Добавить беспроводной маршрутизатор WRT300N. Подключить к нему беспроводные устройства, количество и IP-адрес которых указаны в таблице 4.3. Настроить IP-адрес беспроводного маршрутизатора, DHCP, пароль администратора (состоит из фамилии студента на латинице и его шифра). Установить идентификатор беспроводной сети, состоящий из фамилии студента на латинице. Проверить правильность работы беспроводной сети с помощью отправки ICMP-пакета с любого устройства беспроводной сети в другую сеть. Результаты выполнения команд ping, ipconfig и netstat -r на данном устройстве вставить в отчет.

Таблица 4.3 – Настройка IP-адресации беспроводной сети

Вторая цифра шифра	Количество устройств	IP-адрес	IP-адрес маршрутизатора
0	4	192.168.10.2–192.168.10.100	192.168.10.1
1	7	192.168.11.2–192.168.11.100	192.168.11.1
2	5	192.168.121.2–192.168.121.100	192.168.121.1
3	6	192.168.56.2–192.168.56.100	192.168.56.1
4	4	192.168.31.2–192.168.31.100	192.168.31.1
5	6	192.168.11.2–192.168.11.100	192.168.11.1
6	7	192.168.6.2–192.168.6.100	192.168.6.1
7	6	192.168.7.2–192.168.7.100	192.168.7.1
8	5	192.168.116.2–192.168.116.100	192.168.116.1
9	4	192.168.78.2–192.168.78.100	192.168.78.1

8. Настроить MAC-фильтрацию на беспроводном маршрутизаторе. Запретить доступ в сеть любым двум беспроводным устройствам, остальным разрешить. Проверить правильность произведенных настроек фильтрации, отобразить в отчете.

9. Осуществить подключение беспроводной точки доступа «Wireless devices» → «AccessPoint-PT» к любому коммутатору. Пример подключения представлен на рисунке 4.11. Настроить идентификатор сети, состоящий из имени студента, тип и ключ шифрования, состоящие из имени студента и его шифра. Осуществить подключение пяти беспроводных устройств к данной точке доступа. Проверить соединение, отобразить правильность произведенных настроек в отчете.

10. В случае правильности произведенных настроек, вставить в отчет конфигурацию маршрутизатора. Сохранить файл под именем lab4.pkt.

### **4.3 Содержание отчета**

1. Цель работы, исходные данные из таблиц 4.1, 4.3.
2. Результаты произведенных настроек (заполненная таблица 4.2, результаты выполнения команд из пунктов 4, 6–10 подраздела 4.2), изображение смоделированной в данной работе сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

### **4.4 Контрольные вопросы и задания**

1. Назвать назначение и основные функции протокола IP.
2. Какие поля в заголовке пакета IPv4?
3. Объяснить назначение полей в пакете IPv4.
4. Пояснить необходимость настройки шлюза по умолчанию на компьютере.
5. Какая информация присутствует в таблице маршрутизации? Какие команды применяются для просмотра таблицы маршрутизации?
6. Перечислить стандарты передачи данных в беспроводных сетях. Объяснить их назначение.

## ЛАБОРАТОРНАЯ РАБОТА №5 НАСТРОЙКА СЕРВЕРОВ

**Цель:** изучить типы служб сервера и механизмы установления соединения «клиент – сервер»; овладеть навыками настройки различных типов сервисов сервера.

### 5.1 Теоретическая часть

**Сервер** – вычислительное устройство с установленным программным обеспечением, позволяющим предоставлять другим сетевым узлам информацию. Для работы каждой службы необходимо отдельное серверное программное обеспечение. Например, для веб-служб в сети на узле должно быть установлено ПО веб-сервера. В роли сервера может выступать компьютер с серверным программным обеспечением (несколько типов ПО), при этом он может одновременно обслуживать одного или несколько клиентов.

**Клиент** – компьютерный узел с установленным программным обеспечением, позволяющим запрашивать и отображать полученную с сервера информацию. Примером клиентского программного обеспечения является веб-браузер.

**HTTP-сервер** (HyperText Transfer Protocol, протокол передачи гипертекста, веб-сервер) – вычислительное устройство, которое принимает HTTP-запрос от клиента и возвращает HTTP-ответ, содержащий HTML-страницы с различной информацией: изображения, тексты, скрипты, файлы, медиаданные (видео и аудио) и многое другое.

**DNS-сервер** (Domain Name System, система доменных имен) обеспечивает разрешение имен с помощью программы для поддержки сервера имен доменов. Протокол DNS использует для работы TCP- или UDP-порт 53 для ответов на запросы. В сетях передачи данных устройства идентифицируются по числовым IP-адресам для отправки и получения информации. Большинство пользователей не в состоянии запомнить эти числовые адреса. Доменные имена были созданы для того, чтобы преобразовать числовой адрес в простое и легко запоминаемое имя. Служба доменных имен (DNS) была создана специально для их преобразования в адреса в таких сетях. Когда клиент выполняет запрос, сервер сначала ищет это имя в своих записях, чтобы разрешить его. Если имя не удалось найти по локальным записям, сервер обращается к другим серверам для разрешения имени. Запрос может пересылаться по нескольким серверам. Числовой адрес после нахождения возвращается исходному серверу, который определенное время хранит эту запись в своей кэш-памяти. При повторном запросе этого же имени первый сервер может вернуть адрес, используя значение, которое хранится в кэше имен.

**Сервер NTP** (Network Time Protocol, протокол сетевого времени) – сервер, поддерживающий сетевой протокол для синхронизации внутреннего

времени всех сетевых устройств. NTP для синхронизации использует протокол UDP и порт 123.

**Сервер DHCP** (Dynamic Host Configuration Protocol, протокол динамической настройки узла) – сервер, который автоматически присваивает IP-адрес каждому локальному узлу. Основное преимущество DHCP – автоматическое изменение конфигурации локальной сети при ее расширении, добавлении или удалении узлов. По умолчанию запросы от клиента делаются на порт 67 к серверу, сервер в свою очередь отвечает на порт 68 к клиенту, выдавая адрес IP и другую необходимую информацию, такую, как сетевая маска, маршрутизатор и серверы DNS.

**Сервер FTP** (File Transfer Protocol, протокол передачи файлов) поддерживают работу простых файловых менеджеров, обеспечивающих большие возможности управления подключения и совместного использования файлов. Стандартный порт управления FTP-соединением – 21.

**Сервер TFTP** (Trivial File Transfer Protocol, простой протокол передачи файлов) предназначен для автоматической передачи файлов между компьютерами через UDP-порт 69.

**Сервер электронной почты (Mail Server)** – выделенный узел для обработки почтовых приложений и централизованного управления внешней корреспонденцией, внутренней перепиской и документооборотом. Электронная почта – это набор средств для доставки, хранения и поиска электронных сообщений в сети. Данные сообщения хранятся на серверах электронной почты в базах данных.

Клиенты электронной почты для отправки и получения сообщений обращаются к серверам электронной почты, которые взаимодействуют с другими серверами для обмена сообщениями между доменами. Клиент не соединяется непосредственно с другим клиентом для отправки сообщения. Оба клиента должны доверить транспортировку сообщений серверу электронной почты.

Клиенты электронной почты отправляют сообщения на сервер, указанный в настройках приложения. Получив сообщение, сервер проверяет, присутствует ли указанный в нем домен получателя в локальной базе данных сервера. Если домен отсутствует, сервер отправляет запрос DNS, чтобы определить IP-адрес почтового сервера почты в домене получателя. Электронная почта затем пересылается на соответствующий сервер.

Для работы с электронной почтой применяется три отдельных протокола: SMTP, POP и IMAP. В процессе уровня приложений, при котором выполняется отправка почты, используется протокол SMTP. Это происходит при отправке сообщений от клиента на сервер, а также с одного сервера на другой. Когда клиент отправляет сообщение электронной почты, процесс SMTP-клиента подключается к процессу SMTP-сервера на широко известном порте 25. Установив соединение, клиент пытается отправить по нему сообщение электронной почты серверу. Когда сервер получает сообщение, он помещает



его в очередь сообщений локальной учетной записи или пересылает другому серверу, выполнив такой же процесс установки SMTP-соединения.

Целевой сервер электронной почты в момент доставки сообщения может оказаться недоступен или перегружен. На этот случай в SMTP предусмотрено временное хранение сообщений с последующей повторной отправкой. Периодически сервер проверяет очередь сообщений и пытается отправить их повторно. Если сообщение не удастся доставить в течение установленного времени, оно возвращается отправителю с уведомлением о невозможности доставки.

Получение электронной почты клиентом выполняется по одному из двух протоколов уровня приложений: POP или IMAP.

Протокол POP позволяет рабочим станциям получать сообщения с серверов электронной почты. При использовании протокола POP сообщения загружаются клиентом с сервера и удаляются на сервере.

Сетевой сервис POP на сервере пассивно ожидает запросы подключения клиентов к TCP-порту 110. Для использования этого сетевого сервиса клиент запрашивает TCP-соединение с сервером. После установки соединения сервер POP посылает приветствие. Затем клиент и сервер POP обмениваются командами и откликами, пока подключение не будет закрыто или прервано.

То, что сообщения электронной почты загружаются клиентом и удаляются с сервера, означает, что они не хранятся централизованно.

При подключении пользователя к серверу IMAP в клиентское приложение загружаются только копии сообщений. Исходные сообщения остаются на сервере до тех пор, пока они не будут удалены вручную. Пользователи просматривают копии в клиентах электронной почты. Портами IMAP по умолчанию являются: 143 – порт без шифрования, 993 – порт SSL/TLS (IMAPS, Internet Message Access Protocol).

После ввода в адресной строке веб-адреса или унифицированного указателя ресурса (URL-адрес) веб-браузер устанавливает соединение по протоколу HTTP с веб-сервисом. Унифицированные идентификаторы ресурсов (URL-адрес) – это названия, которые в большинстве случаев ассоциируются с веб-адресами.

Протокол HTTP основан на механизме «запрос – ответ», когда клиент отправляет запрос веб-серверу, а протокол HTTP определяет типы сообщений, используемые для этого взаимодействия.

Взаимодействие между сервером и клиентом происходит при участии ряда протоколов и стандартов в процессе обмена информацией между ними. Различные протоколы взаимодействуют друг с другом, чтобы гарантировать, что сообщения будут приняты и понятны обеим сторонам. Примером таких протоколов является протокол HTTP.

Протокол прикладного уровня HTTP (протокол передачи гипертекста) определяет, каким образом взаимодействуют веб-сервер и веб-клиент, содержание и формат запросов и ответов, которыми обмениваются клиент и сервер. Программное обеспечение и веб-клиента, и веб-сервера реализует

HTTP как часть приложения. Для управления процессом передачи сообщений между клиентом и сервером HTTP обращается к другим протоколам, например TCP.

Транспортный протокол TCP (протокол управления передачей) управляет отдельными сеансами связи между серверами и клиентами в Интернете. TCP делит сообщения HTTP на более мелкие части, называемые сегментами. Они передаются между веб-сервером и клиентскими процессами, запущенными на узле назначения. TCP также отвечает за управление размером и скоростью, с которой происходит обмен сообщениями между сервером и клиентом.

Если два узла взаимодействуют с использованием протокола TCP, соединение устанавливается до того, как обмен данными будет возможен. По завершении обмена данными все сеансы прекращаются, а соединение прерывается. Механизмы подключения и осуществления сеанса связи включают в себя функции TCP, обеспечивающие надежность. На рисунке 5.1 показаны этапы установления TCP-соединения.

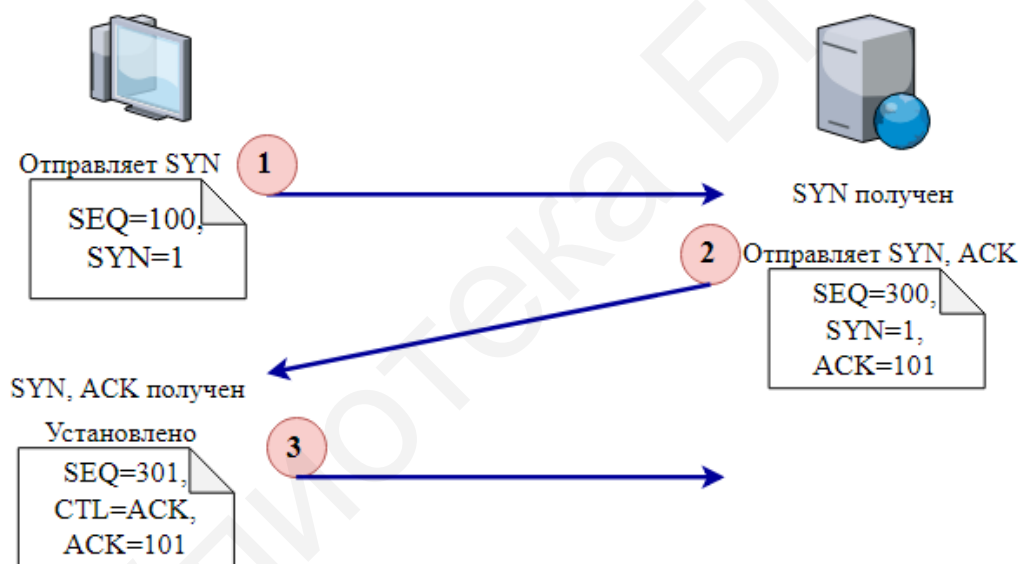


Рисунок 5.1 – Обмен сегментами при трехстороннем «рукопожатии» по протоколу TCP

Узлы отслеживают каждый сегмент данных, передаваемых во время сеанса, и обмениваются информацией о полученных данных с использованием сведений в заголовке TCP. Для установления связи узлы используют трехстороннее рукопожатие. Биты управления в заголовке TCP обозначают этап и состояние подключения. При трехстороннем рукопожатии выполняются следующие процессы:

- определяется присутствие устройства в сети;
- проверяется, имеется ли на устройстве назначения активный сервис и принимает ли он запросы на номер порта назначения, который клиент планирует использовать для сеанса;

- устройству назначения сообщается, что клиент источника планирует установить сеанс связи на этом номере порта.

При подключениях по протоколу TCP клиент узла устанавливает связь с сервером, для чего осуществляются следующие шаги:

- клиент запрашивает сеанс связи «клиент – сервер» с сервером;
- сервер подтверждает сеанс связи «клиент – сервер» и запрашивает сеанс связи «сервер – клиент»;
- клиент подтверждает сеанс связи «сервер – клиент».

При процессе трехстороннего рукопожатия узлы обмениваются различными значениями данных. Заголовок сегмента TCP содержит шесть однобитных полей (флагов) с контрольной информацией, которая используется для управления процессами TCP:

- **URG** – указатель важности;
- **ACK** – номер подтверждения;
- **PSH** – обозначает действие «протолкнуть данные»;
- **RST** – обозначает действие «оборвать соединение»;
- **SYN** – обозначает действие «синхронизировать порядковые номера»;
- **FIN** – обозначает сообщение «больше нет данных от отправителя».

**Запрос сеанса связи «клиент – сервер».** Клиент TCP начинает трехстороннее рукопожатие путем отправки сегмента с установленным управляющим флагом SYN (синхронизировать порядковые номера), который обозначает начальное значение в поле номера последовательности в заголовке. Это значение последовательности, называемое начальным порядковым номером (ISN), выбирается случайно и используется, чтобы начать отслеживание потока данных, которые пересылаются от клиента к серверу в этом сеансе. По мере продолжения сеанса обмена данными этот ISN-номер в заголовке каждого сегмента увеличивается на единицу для каждого байта данных, отправленного от клиента к серверу. Как показано на рисунке 5.1, передаваемая информация содержит управляющий флаг SYN и относительный порядковый номер. Управляющий флаг SYN установлен, а относительный порядковый номер равен 100.

**Подтверждение сеанса связи «клиент – сервер» и запрос сеанса связи «сервер – клиент».** Чтобы начать сеанс связи «клиент – сервер», TCP-сервер должен подтвердить получение сегмента SYN от клиента. Для этого он возвращает сегмент клиенту с установленным флагом подтверждения (ACK), указывая на то, что номер подтверждения задействован. В свою очередь клиент считает это подтверждением того, что сервер получил SYN от клиента TCP.

Значение в поле номера подтверждения равно номеру ISN плюс единица. Это позволяет установить сеанс связи «клиент – сервер». Для обеспечения сбалансированности сеанса флаг ACK остается установленным. Следует помнить, что сеанс связи между клиентом и сервером фактически представляет собой два односторонних сеанса: один «клиент – сервер», другой – «сервер – клиент». На втором шаге трехстороннего рукопожатия сервер должен инициировать ответ клиенту. Чтобы начать этот сеанс, сервер использует

флаг SYN точно так же, как это делал клиент. Он устанавливает управляющий флаг SYN в заголовке для установления сеанса типа «сервер – клиент». Флаг SYN указывает на то, что начальное значение поля порядкового номера указано в заголовке. Это значение используется для отслеживания в сеансе потока данных от сервера к клиенту. Как показано на рисунке 5.1, информация протоколов обозначает, что управляющие флаги ACK и SYN установлены, а последовательный номер и номер подтверждения – отображаются.

**Подтверждение сеанса связи «сервер – клиент».** Наконец, клиент TCP возвращает сегмент, содержащий ACK, т. е. ответ на TCP SYN, отправленный сервером. Пользовательские данные в этом сегменте отсутствуют. Значение в поле номера подтверждения на единицу больше, чем номер ISN, полученный от сервера. После того как между клиентом и сервером будут начаты оба сеанса, для всех дополнительных сегментов, которые пересылаются в этом процессе обмена данными, будут установлены флаги ACK. Как показано на рисунке 5.1, информация отображает установленный управляющий флаг ACK, а также последовательный номер и номер подтверждения.

Для обеспечения дополнительной безопасности в сети передачи данных можно выполнить следующие процедуры: отказ от установления TCP-сеансов, разрешение сеансов только для определенных сервисов, допуск трафика только в рамках уже установленных сеансов. Эти меры по обеспечению безопасности можно использовать как для всех, так и только для выбранных TCP-сеансов.

Для защищенного двухстороннего обмена данными с веб-серверами в Интернете применяется протокол HTTPS. По умолчанию HTTPS URL использует TCP-порт 443 (для незащищенного HTTP – 80). HTTPS применяет аутентификацию и шифрование для защиты данных, пересылаемых между клиентом и сервером. Протокол HTTPS определяет дополнительные правила передачи данных между уровнем приложения и транспортным уровнем. В протоколах HTTPS и HTTP процессы «запрос – ответ» аналогичны, но поток данных шифруется посредством SSL перед началом передачи по сети.

В Cisco Packet Tracer для настройки сервера необходимо перейти на закладку «Services» и выбрать нужный сервис. На рисунке 5.2 представлена настройка DHCP-сервера, в котором задается имя пула IP-адресов, адрес шлюза по умолчанию, DNS-сервер.

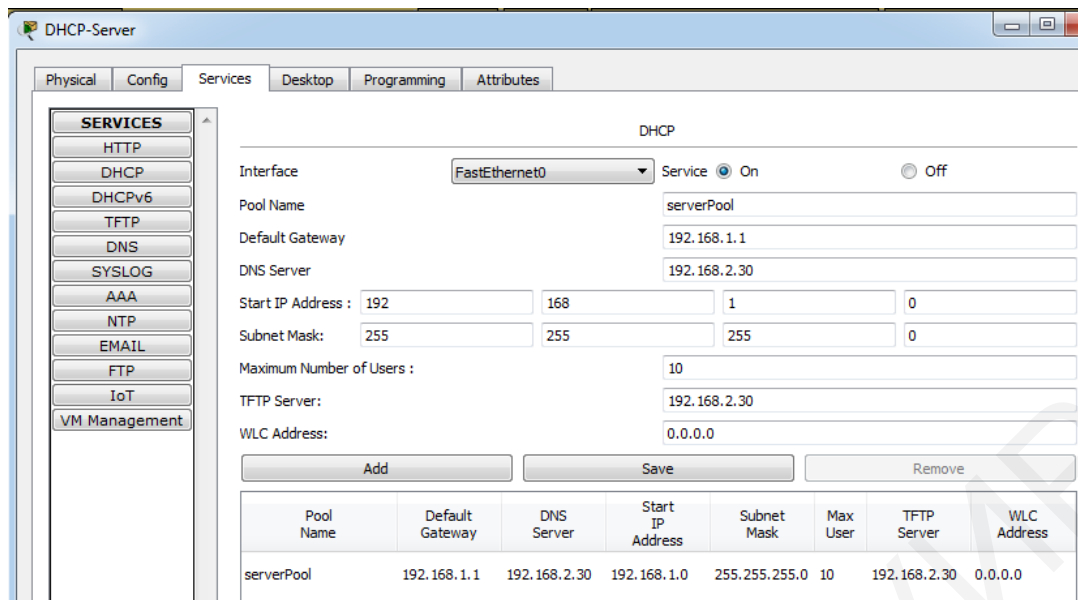


Рисунок 5.2 – Настройка DHCP

Для раздачи IP-адресов задается начальный IP-адрес, при его установке необходимо помнить, что адрес маршрутизатора и серверов не должен быть присвоен каким-либо другим устройствам в сети. Поэтому начальный IP-адрес необходимо задавать исходя из наличия устройств, у которых должен быть уникальный IP-адрес. На рисунке 5.3 представлена настройка DNS, в котором указывается доменное имя и соответствующий ему IP-адрес. Для настройки HTTP-сервера необходимо разместить на сервере файлы, содержащие HTML-код, с помощью которого осуществляется переход по страницам сайта (рисунок 5.4).

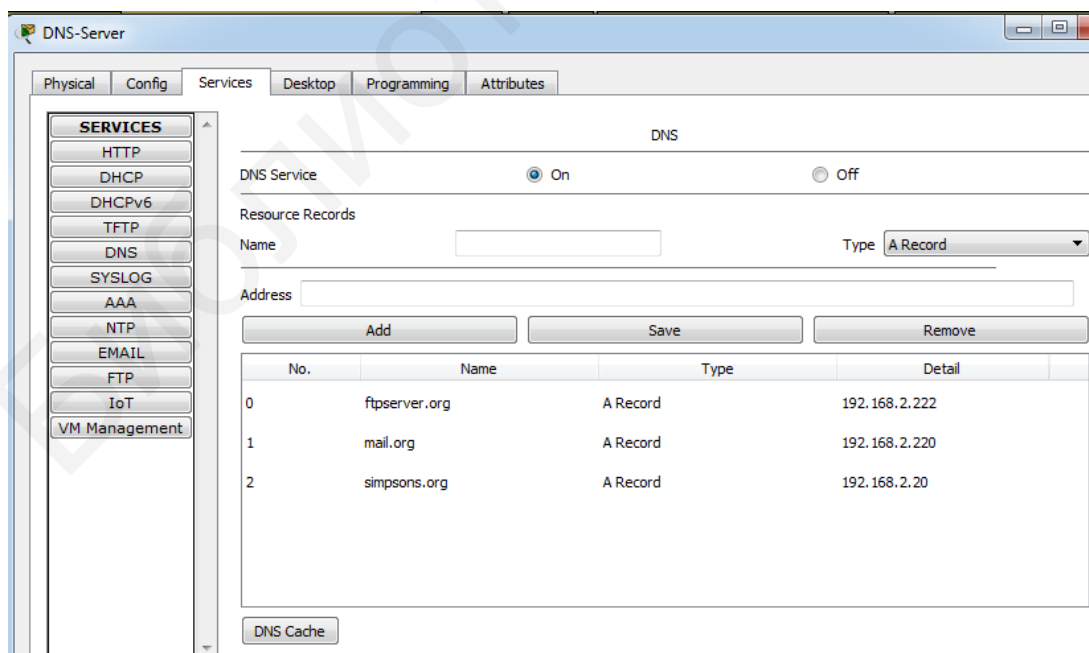


Рисунок 5.3 – Настройка DNS

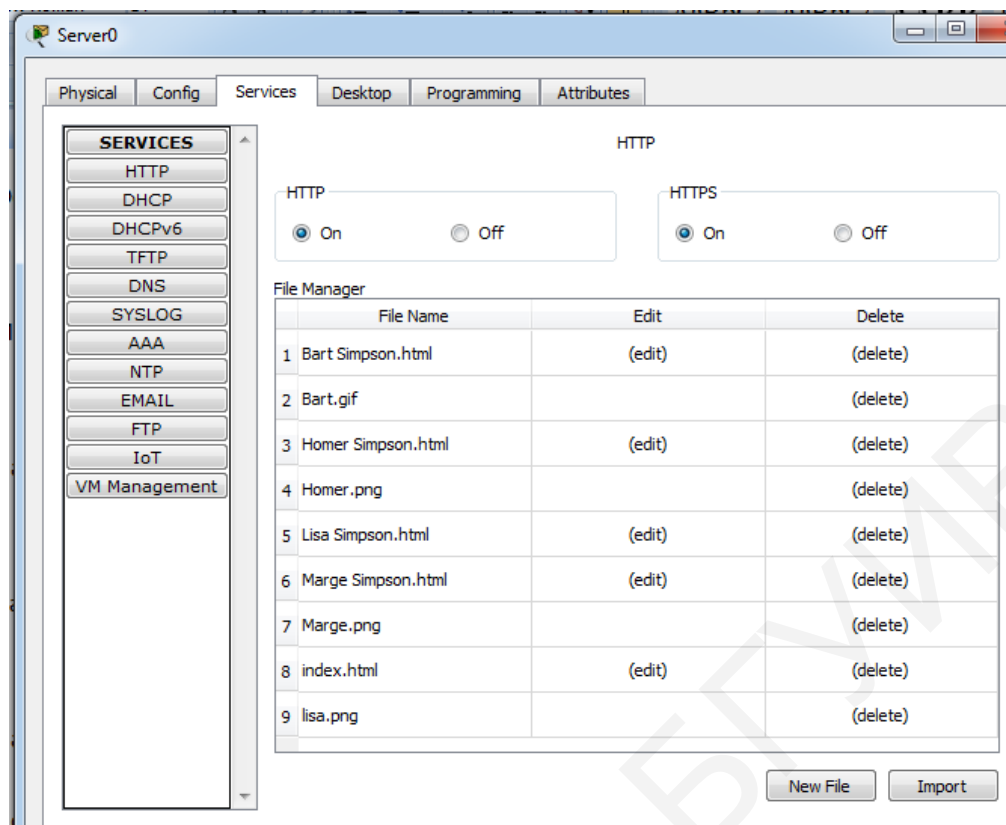


Рисунок 5.4 – Настройка HTTP-сервера

Например, на рисунке 5.5 представлен сайт организации с перечнем сотрудников, дополнительную информацию о которых можно получить, нажимая соответствующие ссылки. Простейший код для подобного сайта представлен ниже.

```

<html>
<head>
<title>Simpsons Corporation</title>
</head>
<body >
<center><font size='+2' color='blue'>Simpsons Corpora-
tion</font></center>
<hr>
<center><form method=?post? action=?tampil.php?>
<table border=?3px?>
<tr>
<td><a href="Homer Simpson.html">Homer Simpson</a>
</tr>
<tr>
<td><a href="Marge Simpson.html">Marge Simpson</a></td>
</tr>
<tr>
<td><a href="Bart Simpson.html">Bart Simpson</a></td>
</tr>

```

```

<tr>
<td><a href="Lisa Simpson.html">Lisa Simpson</a></td>
</tr>
</table>
</form></center>
<hr>
</body>
</html>

```

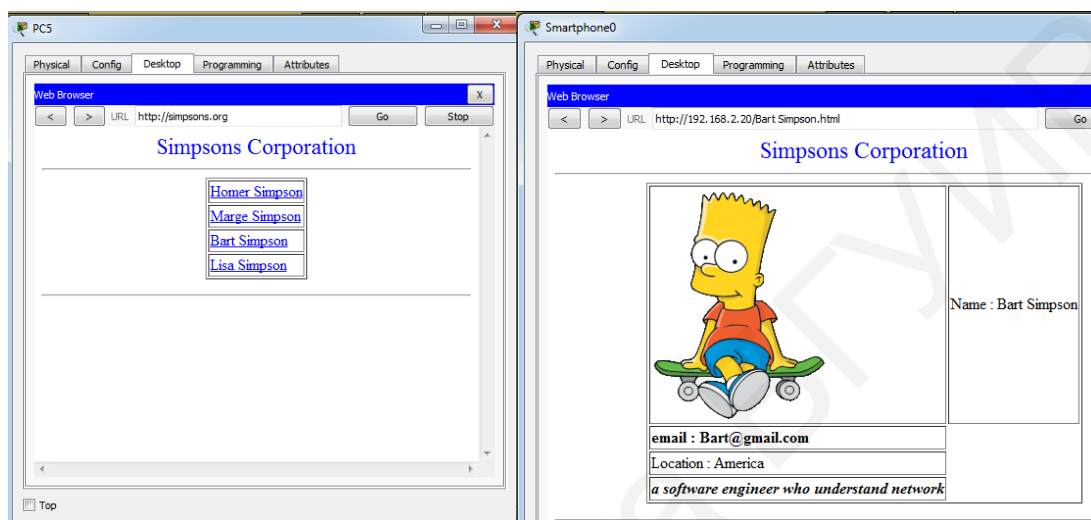


Рисунок 5.5 – Пример простейшего содержания HTTP-сервера

Для отображения текущего времени на маршрутизаторе применяется команда `show clock`. Чтобы осуществить синхронизацию времени маршрутизатора с сервером NTP, используются следующие команды:

```

Router(config)#ntp authentication-key значение_ключа md5 пароль
Router(config)#ntp trusted-key значение_ключа
Router(config)#ntp server IP-адрес key значение_ключа
Router(config)#ntp update-calendar

```

Команды `ntp authentication-key` и `ntp trusted-key` используются в целях указания ключа для безопасного соединения с сервером. Для получения информации о синхронизации сетевого времени на устройстве применяется команда `show ntp status`.

При включении FTP-службы необходимо задать имена и пароли пользователей (рисунок 5.6). Для подключения к FTP-серверу в командной строке вводится `ftp IP-адрес_или_имя_сервера` (рисунок 5.7, а), затем – имя и пароль пользователя. Для отображения файловой системы сервера применяется команда `dir`, для копирования файла на сервер – `put название_файла`, для копирования файла с сервера – `get название_файла` (рисунок 5.7, б). Команда `quit` используется для закрытия соединения FTP.

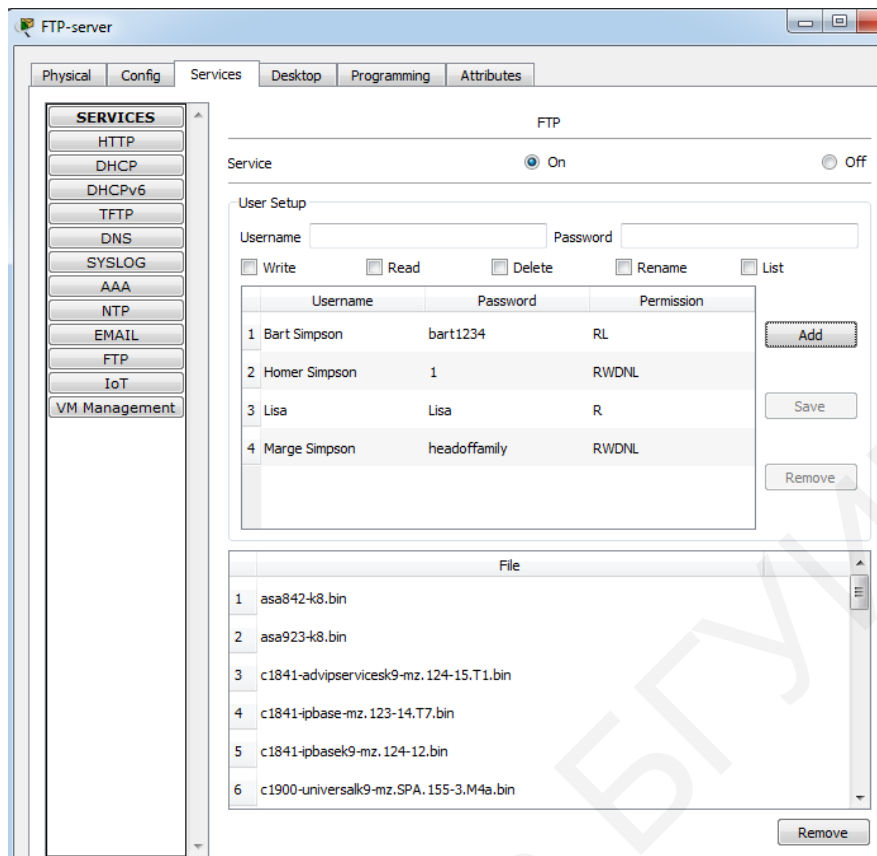
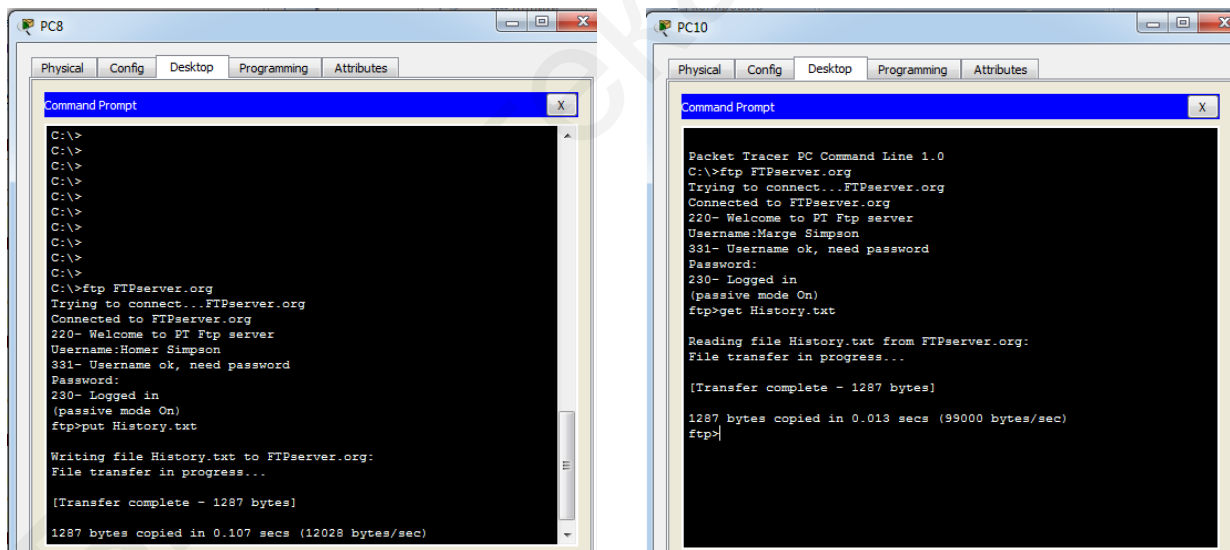


Рисунок 5.6 – Настройка FTP



а – процесс загрузки файла на FTP-сервер;  
 б – процесс копирования файла с FTP-сервера

Рисунок 5.7 – Установка соединения с FTP-сервером

В Cisco Packet Tracer для создания файла используется приложение «Desktop Text editor», которое можно найти на закладке «Desktop» компьютера. На рисунке 5.7, а представлен процесс авторизации пользователя на FTP-сервере с доменным именем FTPserver.org, затем пользователь вводит имя



Homer Simpson и загружает файл History.txt. На рисунке 5.7, б другой пользователь (Marge Simpson) осуществляет копирование данного файла. При этом у пользователей должны быть права доступа на запись и чтение файла для осуществления данных действий, которые устанавливаются на FTP-сервере (см. рисунок 5.6).

**Резервное копирование файлов конфигурации.** Для восстановления файлов конфигурации из резервной копии данных, а также последующего выполнения резервного копирования может использоваться TFTP-сервер. Для загрузки резервной копии на сервер применяется команда `copy running-config tftp:`, далее необходимо указать IP-адрес сервера. Для восстановления резервной копии используется команда `copy tftp: running-config`. Для установки соединения сетевого устройства с FTP-сервером необходимо внести в конфигурацию имя и пароль пользователя при помощи следующих команд:

```
Router(config)#ip ftp username cisco
Router(config)#ip ftp password cisco
Router#copy running-config ftp:
```

Для резервного копирования и восстановления файлов конфигурации применяются такие же команды, как и для TFTP-соединения.

Для настройки почтового сервера необходимо указывать доменное имя, например, «Mail.org» (рисунок 5.8), а также создавать пользователей. Для проверки соединения с почтовым сервером на устройстве пользователя в приложение «Email» на закладке «Desktop» вносятся настройки сервера, имя и пароль пользователя (рисунок 5.9, а). Создание, отправка и получение письма происходит по аналогии с другими почтовыми приложениями (рисунок 5.9, б).

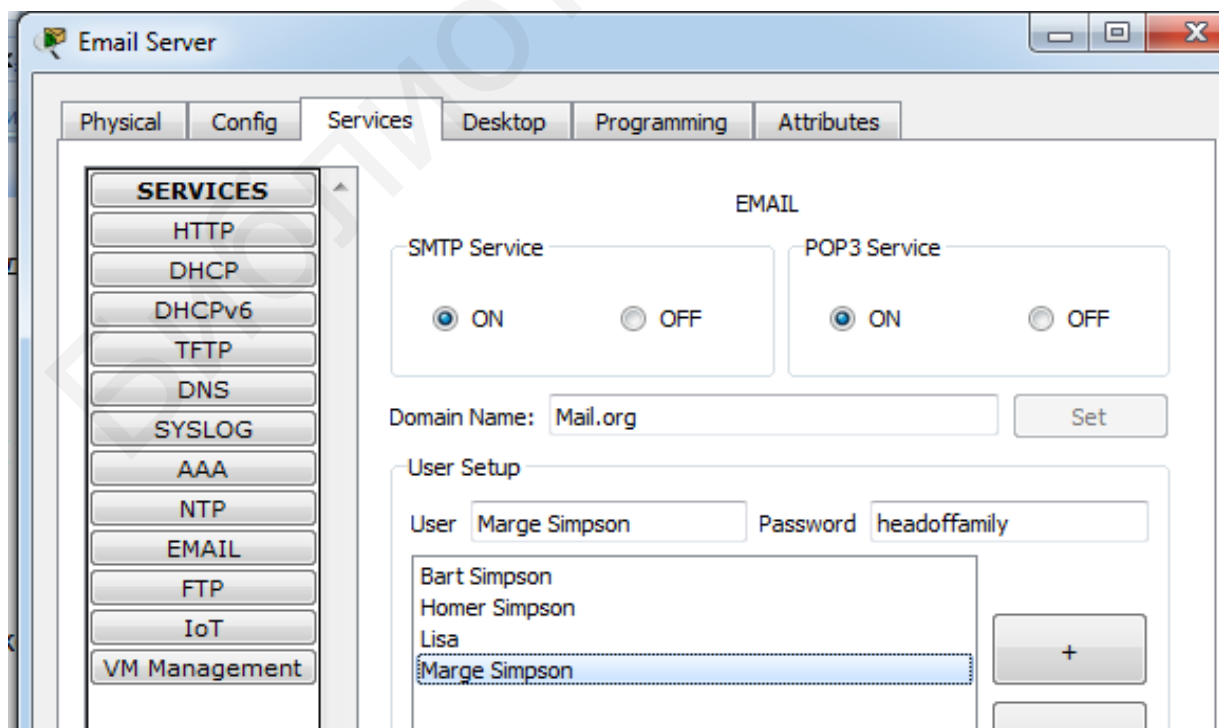
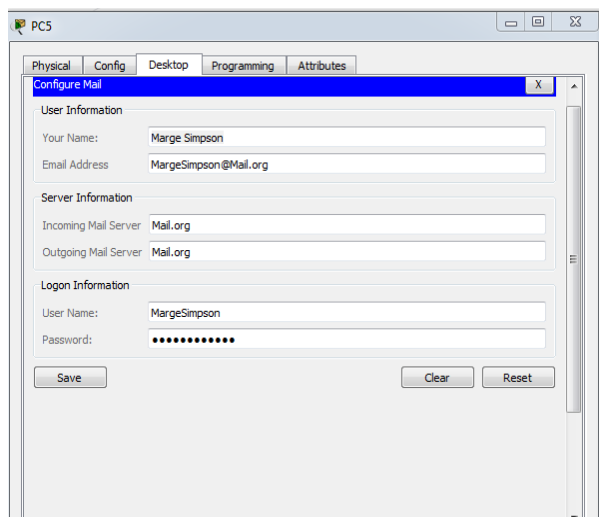
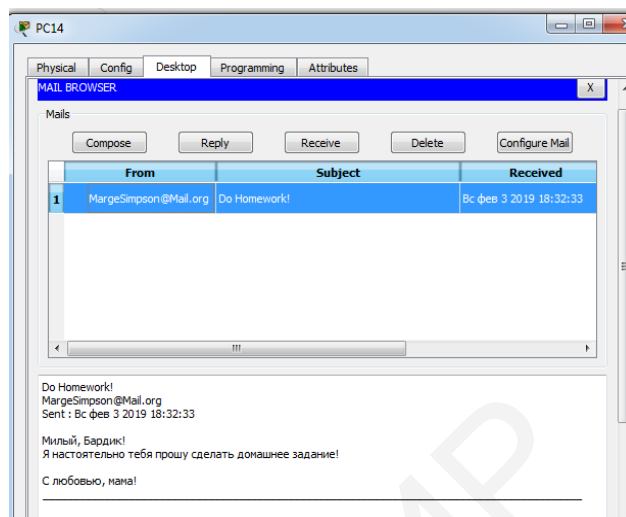


Рисунок 5.8 – Конфигурация почтового сервера



*а*



*б*

*а* – авторизация пользователя на почтовом сервере;  
*б* – результат получения почтового сообщения

Рисунок 5.9 – Соединение с почтовым сервером

## 5.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе №4. До начала выполнения необходимо открыть сохраненный файл с именем lab4.pkt, полученный в лабораторной работе №4, и проверить правильность соединений. В данной работе необходимо добавить и настроить пять серверов, каждый из которых будет отвечать за определенные типы служб в соответствии с таблицей 5.1. Для настройки серверов необходимо выполнить следующие задания.

1. Добавить и подключить по усмотрению студента пять серверов из раздела «End Devices» → «Server-PT». Пример подключения представлен на рисунке 5.10. Осуществить настройку IP-адресации данных серверов. Проверить правильность подключения.

Таблица 5.1 – Параметры и типы настраиваемых серверов

Номер сервера	Тип поддерживаемой службы	Параметр
1	DHCP	Диапазон IP-адресов выставляется в соответствии с моделированной сетью
2	HTTP	Имя сервера соответствует фамилии студента
3	E-mail	Имя сервера соответствует фамилии студента+слово «mail», например, IvanovMail, не менее четырех пользователей
4	FTP, TFTP	Не менее четырех пользователей
5	DNS, NTP	DNS-сервер включает названия HTTP, E-mail и FTP-серверов; NTP-сервер должен содержать ключ, состоящий из шифра студента; пароль – фамилия студента

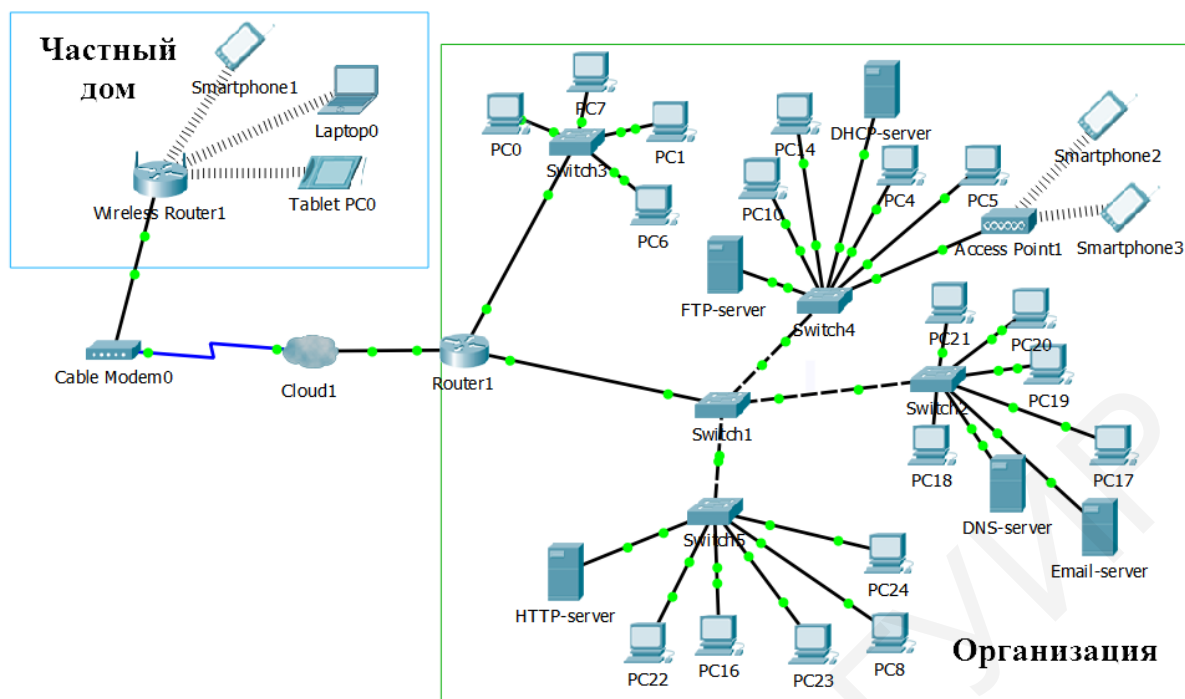


Рисунок 5.10 – Пример смоделированной сети

2. Осуществить настройку DHCP-сервера. Предусмотреть, чтобы IP-адрес основного шлюза (маршрутизатора) был исключен из раздаваемых адресов. Количество подключаемых пользователей не менее 10. Указать IP-адреса DNS- и TFTP-серверов. Проверить работоспособность данного сервера, установив DHCP на компьютерах. Отобразить результат работы в отчете.

3. Осуществить настройку HTTP-сервера. Сконфигурировать сайт организации, на котором должно быть не менее четырех картинок, не менее четырех ссылок и не менее четырех страниц HTML, взаимосвязанных друг с другом. Не использовать сайт, созданный по умолчанию в Cisco Packet Tracer. Проверить работоспособность данного сервера, установив соединение и проверив все страницы. Отобразить результат работы в отчете.

4. Осуществить настройку сервера E-mail. Добавить не менее четырех пользователей. Осуществить отправку и получение сообщения E-mail. Проверить правильность работы, отобразить результат в отчете.

5. Настроить FTP-сервер. Добавить не менее четырех пользователей и распределить их права. Указать имена, пароли и права пользователей в таблице 5.2.

Таблица 5.2 – Данные пользователей для доступа к FTP-серверу

Имя	Пароль	Права доступа

6. Создать файл с расширением \*.txt в Text Editor с любым содержанием, сохранить его под фамилией студента и загрузить на FTP-сервер, используя имя и пароль одного из зарегистрированных пользователей. Проверить правильность настройки прав пользователей, попытаться скачать данный файл с другого компьютера под именем другого пользователя. Отобразить результаты в отчете.

7. Настроить на всех сетевых устройствах возможность подключения и копирования конфигурации на FTP-сервер. Проверить возможность резервного копирования и восстановления с помощью FTP-сервера. Отобразить результат в отчете.

8. Осуществить настройку TFTP-сервера. Проверить возможность резервного копирования и восстановления конфигурации любого сетевого устройства с помощью TFTP-сервера. Отобразить результат в отчете.

9. Осуществить настройку NTP-сервера. Установить ключ и пароль в соответствии с рекомендациями из таблицы 5.1. Осуществить настройки протокола NTP на всех сетевых устройствах. Проверить правильность работы, результат отобразить в отчете.

10. Настроить DNS-сервер, который должен содержать IP-адреса и имена серверов в соответствии с рекомендациями из таблицы 5.1. Проверить возможность использования для установки соединения имен НТТР, E-mail и FTP-серверов вместо IP-адресов, результат отобразить в отчете. Сохранить файл под именем lab5.pkt.

11. Перейти в режим симуляции и отправить НТТР-пакет с любого компьютера. Проследить прохождение пакетов DNS, TCP и НТТР, заполнить таблицу 5.3, в которой указать состояния флагов при установке соединения и номеров портов.

Таблица 5.3 – Установление соединения НТТР

Номер шага	Отправитель	Получатель	Тип пакета	Содержание пакета
1				
2				
3				
4				

### 5.3 Содержание отчета

1. Цель работы, исходные данные из таблицы 5.1.
2. Результаты произведенных настроек (заполненные таблицы 5.2, 5.3, результаты выполнения команд из пунктов 2, 3, 6–10 подраздела 5.2), изображение смоделированной в данной работе сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

## 5.4 Контрольные вопросы и задания

1. Дать определение сервера и клиента, перечислить типы серверов.
2. Описать процесс установки соединения по протоколу DNS.
3. Привести соответствие протоколов HTTP, HTTPS, DNS, DHCP, FTP, TFTP, SNTP, POP, IMAP и используемых портов.
4. В чем заключаются отличия протоколов FTP и TFTP, IMAP и POP, HTTP и HTTPS?
5. Пояснить процесс установки соединения с сервером электронной почты.
6. Перечислить основные этапы процесса трехстороннего рукопожатия.
7. В чем заключается назначение флагов в процессе рукопожатия? Каков механизм их изменения?

## ЛАБОРАТОРНАЯ РАБОТА №6 ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

**Цель:** изучить назначение, принципы организации и настройки виртуальных локальных сетей; овладеть навыками настройки сетевых устройств при организации виртуальных локальных сетей.

### 6.1 Теоретическая часть

VLAN (Virtual Local Area Network) – логическая (виртуальная) локальная компьютерная сеть, представляющая собой группу устройств с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Может быть настроена на коммутаторах, маршрутизаторах, других сетевых устройствах.

Преимущества использования VLAN:

- облегчается перемещение, добавление устройств и изменение их соединений друг с другом;

- достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на третьем уровне;

- уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена;

- сокращается непроизводительное использование CPU за счет сокращения пересылки широковещательных сообщений;

- предотвращаются широковещательные штормы и петли.

Протокол 802.1Q повсеместно используется во всех современных сетях. Суть его состоит в том, что он слегка расширяет Ethernet-кадр (рисунок 6.1), добавляя туда несколько полей (в частности, поле VLAN Identifier, VID). На основании данного поля коммутатор способен определить, какой группе портов адресован тот или иной кадр.

Ethernet IEEE 802.3 (Ethernet II)						
8 байт	6 байт	6 байт	4 байта	2 байта	46–1500 байт	4 байта
Преамбула	Адрес назначения	Адрес источника	Маркер 802.1Q VLAN	Тип	Данные	Контрольная последовательность кадра

Рисунок 6.1 – Формат Ethernet-кадра в сетях VLAN

Благодаря полю VID, к одному коммутатору можно подключить клиентов из нескольких разных подсетей, тем самым ограничив

широковещательный домен. Также появляется возможность объединить клиентов, подключенных к разным коммутаторам, в одну логическую сеть.

Процесс передачи кадра в сети с протоколом 802.1Q включает следующие этапы (рисунок 6.2):

- компьютер 1 подключен к access-порту fa2/1 коммутатора 1 во VLAN10; это означает, что при попадании кадра на порт коммутатора 1 в него будет добавлен 802.1Q header с информацией о принадлежности к VLAN10;

- коммутатор 1 пересылает тегированный кадр на коммутатор 2 через trunk-порт;

- коммутатор 2 получает кадр, смотрит в свою CAM-таблицу и отправляет кадр в соответствующий access-порт, заголовок 802.1Q снимается.

Особенности процесса передачи кадра:

- пользователи ничего не знают о своей принадлежности к определенному VLAN и работают с нетегированными кадрами, заголовок 802.1Q появляется только при прохождении кадра через access-порт;

- порт может быть нетегирован (access) только в одном VLAN (верно для коммутаторов Cisco);

- через тегированный (trunk) порт можно передавать кадры, принадлежащие к разным VLAN;

- существует так называемый native VLAN – при попадании на trunk-порт кадра без тега он автоматически будет причислен к native VLAN. Как правило, к native VLAN по умолчанию относится VLAN1.

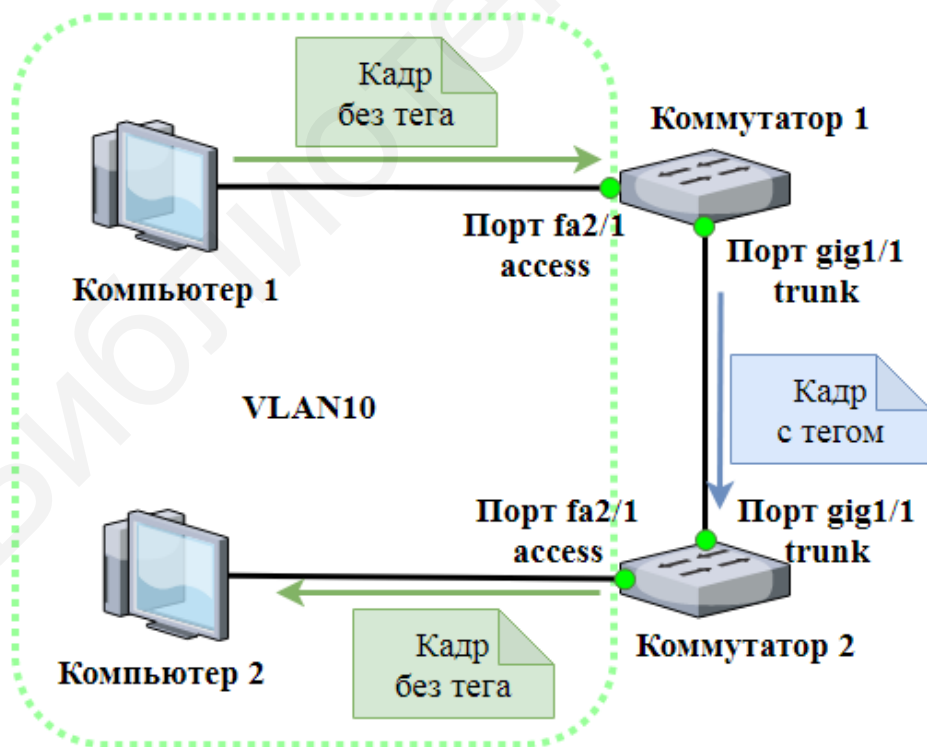


Рисунок 6.2 – Процесс передачи кадра в сети с протоколом 802.1Q

При этом кадры, принадлежащие native VLAN и попавшие в access-порт, будут передаваться через trunk-порт без тега.

Коммутаторы имеют возможность автоматически согласовывать тип порта (рисунок 6.3). Для этого применяется проприетарный протокол DTP (Dynamic Trunking Protocol) компании Cisco. При его использовании (а он включен по умолчанию) возможны следующие состояния порта: dynamic auto, dynamic desirable, static access, static trunk.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Ограниченное подключение
Access	Access	Access	Ограниченное подключение	Access

Рисунок 6.3 – Возможные состояния портов

При определенных условиях в режимах dynamic auto и dynamic desirable порт коммутатора может согласовать свою работу в режиме trunk. Это значит, что если атакующее устройство будет настроено как порт в режиме desirable, оно согласует на себя trunk-порт и получит доступ к трафику всех VLAN.

В настоящее время рекомендуются следующие принципы создания и настройки защищенных компьютерных сетей.

1. Не использовать для распространения информации о применяемых VLAN в компьютерной сети протокол VTP (включать режим transparent).

2. В качестве протокола инкапсуляции использовать протокол IEEE 802.1Q.

3. Запретить передавать кадры VLAN по магистральным каналам. В качестве native VLAN использовать специально для этого выделенную VLAN, не применяемую ни для каких других целей.

4. Не использовать стандартную VLAN1 ни для каких целей, особенно для управления сетевым оборудованием.

5. На магистральных портах использовать только необходимые VLAN, все другие запрещать.

6. Не использовать одинаковые VLAN на разных коммутаторах.

7. Все неиспользуемые порты коммутатора переводить в режим shutdown и назначать их в специально созданную для этого немаршрутизируемую и изолированную VLAN.

8. На портах доступа отключать использование протокола DTP. Для минимизации времени восстановления функционирования системы при подключении канала на магистральных портах устанавливать протокол DTP в режиме Nonegotiate (отключать согласование).



Рассмотрим пример настройки VLAN для сети, представленной на рисунке 6.4.

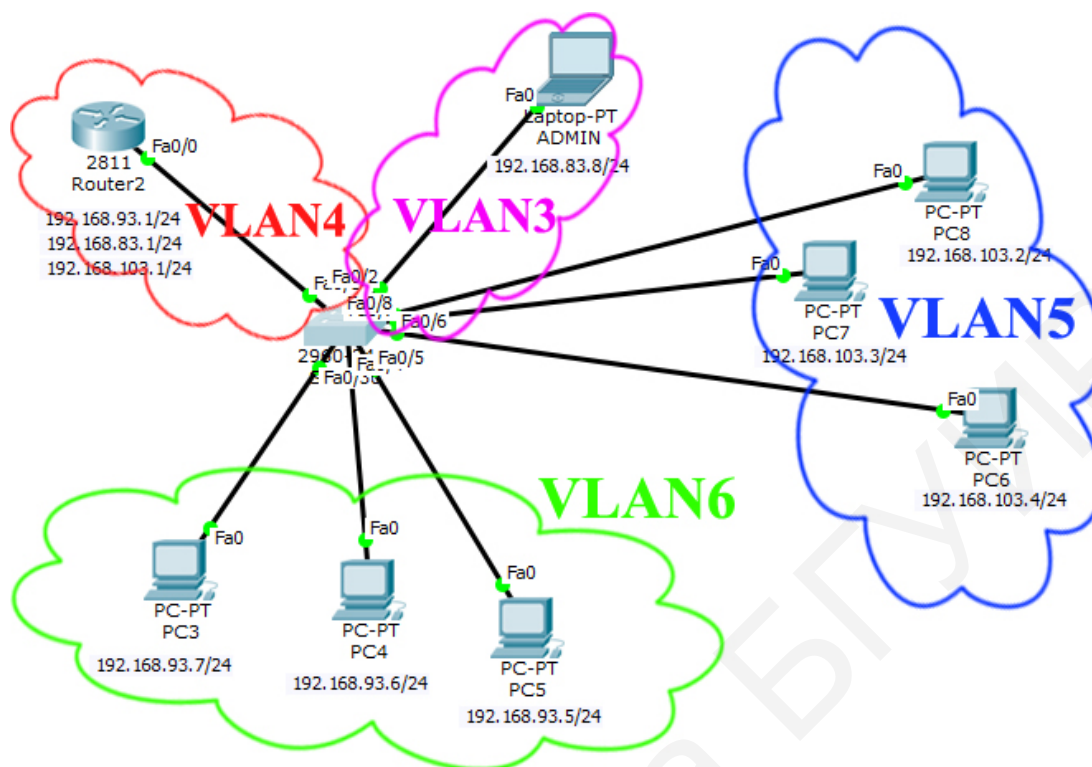


Рисунок 6.4 – Пример виртуальных локальных сетей

Сети VLAN – это определенные внутри коммутаторов широковещательные домены, позволяющие внутри устройства второго уровня управлять широковещательными, групповыми, одноадресными рассылками, а также одноадресными рассылками с неизвестным получателем. Каждая сеть VLAN создается в локальной базе данных используемого коммутатора. Если в коммутаторе отсутствуют сведения о какой-либо VLAN-сети, то он не может передавать трафик для этой сети через свои порты. VLAN-сети создаются по номерам, при этом существует два диапазона, пригодных для использования VLAN-номеров: обычный – 1–1000 и расширенный – 1025–4096. При создании VLAN-сети можно также назначить ей определенные атрибуты, такие как имя, тип и операционное состояние. По умолчанию на коммутаторе существуют предопределенные VLAN, которые нельзя удалить или переименовать. Все физические порты устройства по умолчанию находятся во VLAN1, называемой стандартной сетью VLAN (default VLAN), поэтому ее в целях безопасности и не рекомендуют использовать. При создании новой сети не рекомендуется применять VLAN1.

Для получения краткой информации о VLAN на коммутаторе (рисунок 6.5) вводится команда `Switch#show vlan brief`

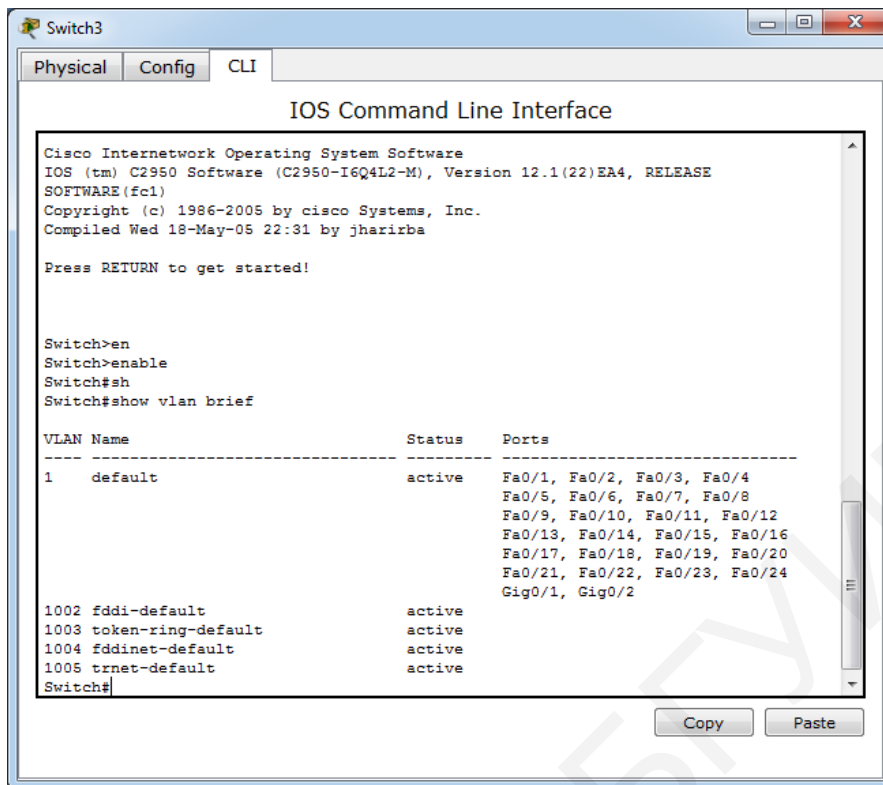


Рисунок 6.5 – Просмотр информации о VLAN на коммутаторе

В результате выполнения команды на экране появится следующая информация:

- номера VLAN – первый столбец;
- название VLAN – второй столбец;
- состояние VLAN (включен или выключен) – третий столбец;
- порты, принадлежащие к данному VLAN, – четвертый столбец.

По умолчанию на коммутаторе существует пять VLAN (1, 1002, 1003, 1004, 1005), все порты принадлежат VLAN1. Порты, принадлежащие VLAN 1002–1005, являются служебными и используются не очень часто. В целях безопасности порты, которые относятся к VLAN1, необходимо или отключить, или перевести в другие VLAN.

Процесс создания статических VLAN-сетей включает в себя несколько этапов.

1. В режиме глобального конфигурирования необходимо установить протокол VTP в прозрачный режим функционирования для защиты от VLAN-hopping атаки:

```
Switch#configure terminal
Switch(config)#vtp mode transparent
```

2. Создать все сети VLAN и указать их имена с помощью последовательности команд:

```
Switch(config)#vlan <номер>
Switch(config-vlan)#name <имя>
Switch(config-vlan)#exit
```

В таблице 6.1 представлено соответствие VLAN и IP-адресов компьютеров, номера портов маршрутизатора и коммутатора, за которым они закреплены сети, представленной на рисунке 6.4.

Таблица 6.1 – Настройка виртуальных локальных сетей

Номер VLAN	IP-адреса устройств, входящих во VLAN	Номер интерфейса коммутатора, подключенного к VLAN	Имя интерфейса коммутатора, подключенного к VLAN	Номер и IP-адрес интерфейса маршрутизатора
3	192.168.83.8 (admin)	Fa0/2	Admin	Fa0/0.3
4	192.168.83.1 192.168.93.1 192.168.103.1 (маршрутизатор)	Fa0/1	Main	Fa0/0.4
5	192.168.103.2 192.168.103.3 192.168.103.4	Fa0/6, Fa0/7, Fa0/8	Office1	Fa0/0.5
6	192.168.93.5 192.168.93.6 192.168.93.7	Fa0/3, Fa0/4, Fa0/5	Office2	Fa0/0.6

Сеть VLAN 5 будет настроена на коммутаторе следующим образом:

```
Switch(config)#vlan 5
Switch(config-vlan)#name Office1
```

3. Назначить в созданные VLAN-сети физические порты коммутатора, для чего перейти в режим конфигурирования выбранного интерфейса, а затем перевести его в режим доступа, используя команду `switchport mode access`, и назначить его в соответствующую VLAN-сеть командой `switchport access vlan 6`. Например, для рисунка 6.4 и таблицы 6.1 порт FastEthernet 0/3, к которому подключен PC3, назначается во VLAN с номером 6 с помощью следующих команд:

```
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 6
```

Таким же образом VLAN настраивается на всех остальных интерфейсах.

Для выполнения некоторой последовательности команд одновременно для нескольких портов коммутатора можно использовать выбор диапазона портов, осуществляемый с помощью команды

```
Switch(config)#interface range FastEthernet 0/3-5
```

Порт Fa0/1, соединяющий коммутатор с маршрутизатором (см. рисунок 6.4), является транковым. Это означает, что через него будет передаваться информация от трех остальных VLAN. Поэтому на данном интерфейсе включение режима транкинга осуществляется с помощью команды `switchport mode trunk`. Далее указывается номер VLAN с помощью

команды `switchport trunk native vlan номер`. Конфигурация интерфейса Fa0/1 осуществляется с помощью следующих команд:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 4
```

На маршрутизаторе следует настроить sub-интерфейсы на порту Fa0/0, поэтому сначала необходимо удалить установленный IP-адрес командой `no ip address`. Далее осуществляется переход в режим настройки sub-интерфейса командой `interface fa0/0.номер`, номера sub-интерфейсов могут соответствовать номерам VLAN. В целях указания номера VLAN для данного sub-интерфейса используется команда `encapsulation dot1q номер_VLAN`, которая включает инкапсуляцию по протоколу IEEE 802.1Q. Обязательно настраивается IP-адрес sub-интерфейса и сервера. Последовательность команд для настройки sub-интерфейса Fa0/0.3, который соединяется с VLAN3 на рисунке 6.4, представлена ниже:

```
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#no ip address
Router(config)# interface fa0/0.3
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 192.168.83.1 255.255.255.0
Router(config-if)#ip helper-address 192.168.10.10
Router(config-subif)#no shutdown
```

Аналогично осуществляется настройка sub-интерфейсов для других VLAN. Проверку наличия VLAN в таблице маршрутизации маршрутизатора можно осуществить с помощью команды `show ip route`. В результате будут показаны сети, которые подключены к маршрутизатору (рисунок 6.6).

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

Gateway of last resort is not set

C    192.168.83.0/24 is directly connected, FastEthernet0/0.2
C    192.168.93.0/24 is directly connected, FastEthernet0/0.1
C    192.168.103.0/24 is directly connected, FastEthernet0/0.3
```

Рисунок 6.6 – Результат выполнения команды `show ip route`

При соединении внешней сети необходимо настроить маршрутизацию с помощью следующих команд:

```
Router (config)#router rip
Router (config-router)#version 2
Router (config-router)#network 192.168.83.0
Router (config-router)#network 192.168.93.0
Router (config-router)#network 192.168.103.0
```

```
Router (config-router)#no auto-summary
```

Команда `router rip` применяется для включения протокола маршрутизации RIP, команда `version 2` – для установки версии протокола маршрутизации RIP, команды `network 192.168.83.0`, `network 192.168.93.0`, `network 192.168.103.0` – для указания подключения сетей VLAN3, VLAN6, VLAN5 к маршрутизатору, команда `no auto-summary` – для отключения автоматических настроек маршрутизации.

Если к данному маршрутизатору будет впоследствии подключена еще одна сеть, ее также необходимо внести в список сетей протокола маршрутизации. Так, например, при подключении локальной сети ее адрес необходимо внести в таблицу маршрутизации.

## 6.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе №5. До начала выполнения необходимо открыть сохраненный файл с именем `lab5.pkt`, полученный в лабораторной работе №5, и проверить правильность соединений.

1. Осуществить разделение всех устройств в смоделированной сети на пять сетей VLAN: сеть VLAN, содержащая серверы; три сети VLAN с компьютерами, сеть VLAN с беспроводными устройствами. Пример сети представлен на рисунке 6.7. Номера VLAN задаются согласно таблице 6.3 в соответствии со второй цифрой шифра. Заполнить таблицу 6.4 по аналогии с таблицей 6.1.

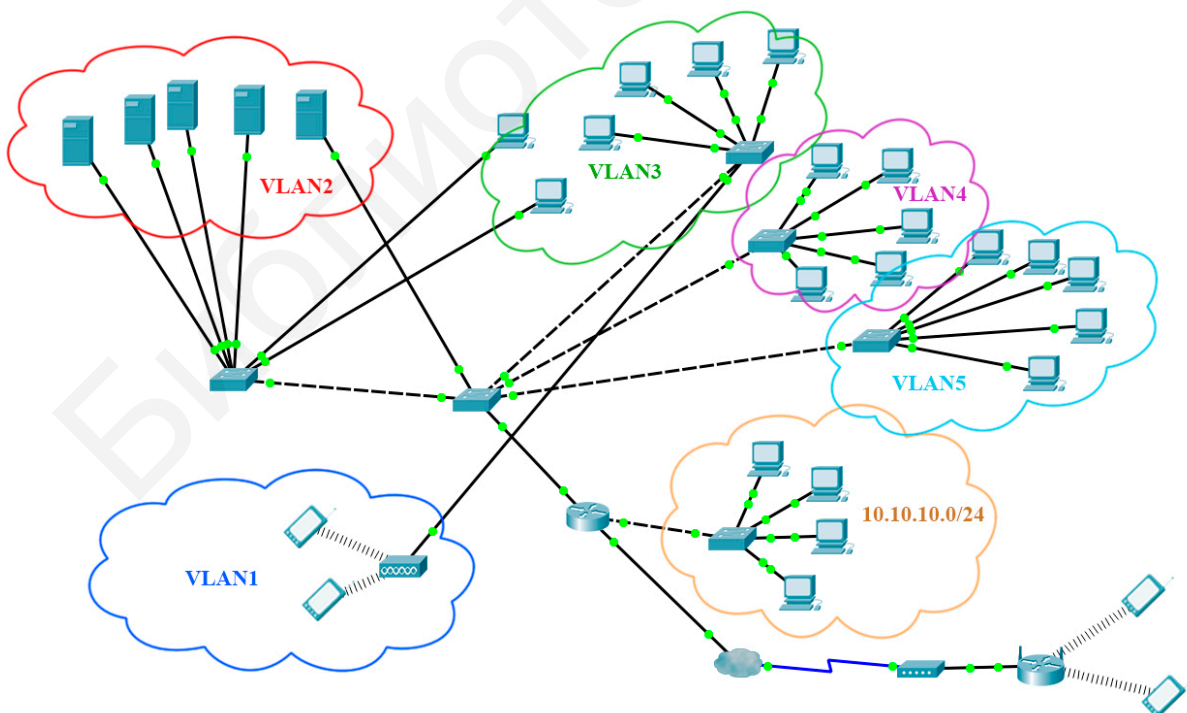


Рисунок 6.7 – Пример соединения локальных сетей

Таблица 6.3 – Исходные данные для создания VLAN

Вторая цифра шифра	Номер VLAN	IP-адресация во VLAN
0	116	192.168.11.2–192.168.11.250
	216	192.168.10.2–192.168.10.250
	316	192.168.12.2–192.168.12.250
1	184	192.168.14.2–192.168.14.250
	186	192.168.13.2–192.168.13.250
	185	192.168.11.2–192.168.11.250
2	938	192.168.121.2–192.168.121.250
	838	192.168.120.2–192.168.120.250
	738	192.168.122.2–192.168.122.250
3	554	192.168.55.2–192.168.55.250
	454	192.168.56.2–192.168.56.250
	354	192.168.57.2–192.168.57.250
4	863	192.168.32.2–192.168.32.250
	865	192.168.33.2–192.168.33.250
	867	192.168.34.2–192.168.34.250
5	192	192.168.10.2–192.168.10.250
	294	192.168.11.2–192.168.11.250
	396	192.168.9.2–192.168.9.250
6	855	192.168.6.2–192.168.6.250
	756	192.168.7.2–192.168.7.250
	657	192.168.8.2–192.168.8.250
7	145	192.168.5.2–192.168.5.250
	335	192.168.4.2–192.168.4.250
	426	192.168.3.2–192.168.3.250
8	23	192.168.114.2–192.168.114.250
	33	192.168.115.2–192.168.115.250
	13	192.168.116.2–192.168.116.250
9	187	192.168.75.2–192.168.75.250
	377	192.168.76.2–192.168.76.250
	897	192.168.77.2–192.168.77.250

Таблица 6.4 – IP-адресация устройств в смоделированной сети

Номер VLAN	Название устройства	IP-адреса устройств, входящих во VLAN	Номер интерфейса коммутатора, подключенного к VLAN	Имя интерфейса коммутатора, подключенного к VLAN	Номер и IP-адрес интерфейса маршрутизатора

2. Осуществить конфигурацию сетей VLAN. С помощью команды `ping` проверить соединение всех компьютеров в сети. С помощью команды `show vlan brief` получить информацию о настроенных VLAN на коммутаторе,

с помощью команды `show ip route` – о сетях, подключенных к маршрутизатору, и настроить маршрутизацию. Результаты выполнения вышеприведенных команд отобразить в отчете.

3. Создать локальную сеть с адресом 10.10.10.0/255.255.255.0, в которой к коммутатору подключено четыре компьютера со статической IP-адресацией. Подключить данную сеть к маршрутизатору. Для примера сети использовать рисунок 6.7. Дополнить таблицу 6.4 информацией о подключенных устройствах.

5. Проверить наличие связи между устройствами локальных сетей и всеми VLAN с помощью команды `ping`. Скопировать в отчет результат выполнения команды `show ip route`.

6. В случае исправной работы всей сети сохранить текущую конфигурацию настроек маршрутизатора и коммутатора, для чего выполнить команду `copy running-config startup-config`. В отчете представить конфигурацию маршрутизатора. Сохранить файл под именем lab6.pkt.

### **6.3 Содержание отчета**

1. Цель работы, исходные данные в соответствии с заданным вариантом из таблиц 6.2 и 6.3.

2. Результаты произведенных настроек (заполненная таблица 6.4, результаты выполнения команд из пунктов 2–6 подраздела 6.2), изображение смоделированной сети.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

### **6.4 Контрольные вопросы и задания**

1. Каково назначение виртуальных локальных сетей? Перечислить достоинства и недостатки виртуальных локальных сетей.

2. Описать процесс передачи кадра в виртуальных локальных сетях.

3. Представить формат Ethernet-кадра в сетях VLAN и процесс его передачи.

4. В чем заключается согласование состояния портов коммутаторов?

5. Объяснить принципы настройки виртуальных локальных сетей.

## ЛАБОРАТОРНАЯ РАБОТА №7 VOIP-ТЕЛЕФОНИЯ

**Цель:** изучить принципы работы VoIP-телефонии; овладеть навыками конфигурации маршрутизаторов и коммутаторов для VoIP-телефонии.

### 7.1 Теоретическая часть

VoIP (Voice over Internet Protocol) – технология IP-телефонии, которая основана на пакетной коммутации сообщений для передачи голоса в режиме реального времени по протоколу IP.

Основным устройством IP-телефонии кроме телефонов является шлюз, Gateway, который соединяет телефонную сеть с сетью IP (рисунок 7.1). Основными функциями шлюза являются ответ на сигнал вызывающего абонента, установление соединения с удаленным шлюзом и вызываемым абонентом, сжатие, пакетирование и восстановление голоса (рисунок 7.2). Для подключения системы IP-телефонии к телефонной сети общего пользования (ТфОП) используются голосовые шлюзы на базе маршрутизаторов, при этом выбор конкретной модели шлюза зависит от типа и количества интерфейсов, применяемых для стыковки с ТфОП (возможно использование как аналоговых, так и цифровых интерфейсов). Шлюзы также нужны в случае необходимости подключения системы IP-телефонии к установленной ранее офисной АТС.

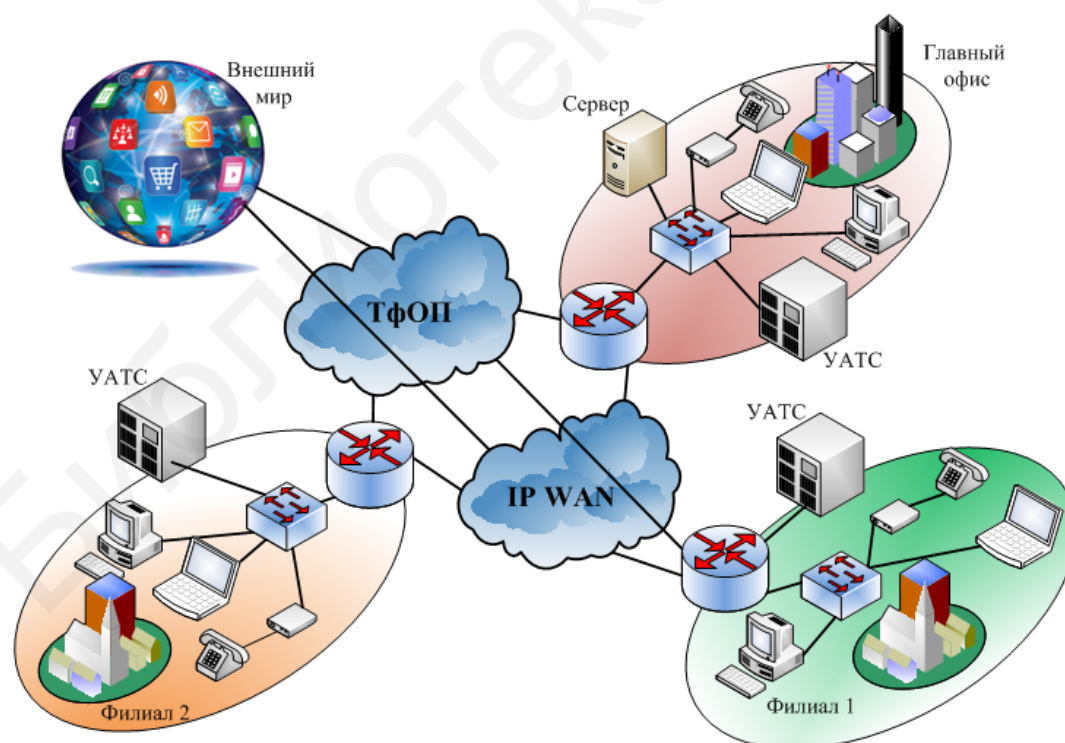


Рисунок 7.1 – Структурная схема сети IP-телефонии





Рисунок 7.2 – Сценарий IP-телефонии «компьютер – компьютер»

Пользовательские IP-телефоны так же, как и серверы, подключаются к коммутаторам локальной сети. Многие модели телефонов оснащены встроенным двухпортовым коммутатором Ethernet, позволяющим подключить персональный компьютер абонента к корпоративной сети.

Для управления сетью IP-телефонии необходим сервер управления звонками, который размещается в пределах локальной сети. Общий принцип действия телефонных серверов, связанных с телефонными линиями и сетью Интернет, заключается в получении стандартного телефонного сигнала, оцифровке, сжатии, разделении на пакеты и отправке с использованием протокола TCP/IP. Для пакетов, получаемых из локальной сети на телефонный сервер и отправляемых в телефонную линию, операция происходит в обратном порядке.

**На физическом уровне** модели OSI VoIP-телефония полностью опирается на существующую инфраструктуру сети. В качестве среды передачи информации используются, как правило, витая пара, одномодовое или многомодовое оптическое волокно.

На рисунке 7.3 представлен фрагмент сети, изображенный на рисунке 6.7, с добавлением IP-телефонов и аналоговых телефонов. Для подключения к сети IP-телефона используется витая пара, для подключения аналогового телефона – телефонный кабель и VoIP-шлюз, который в свою очередь подключается к коммутатору с использованием витой пары.

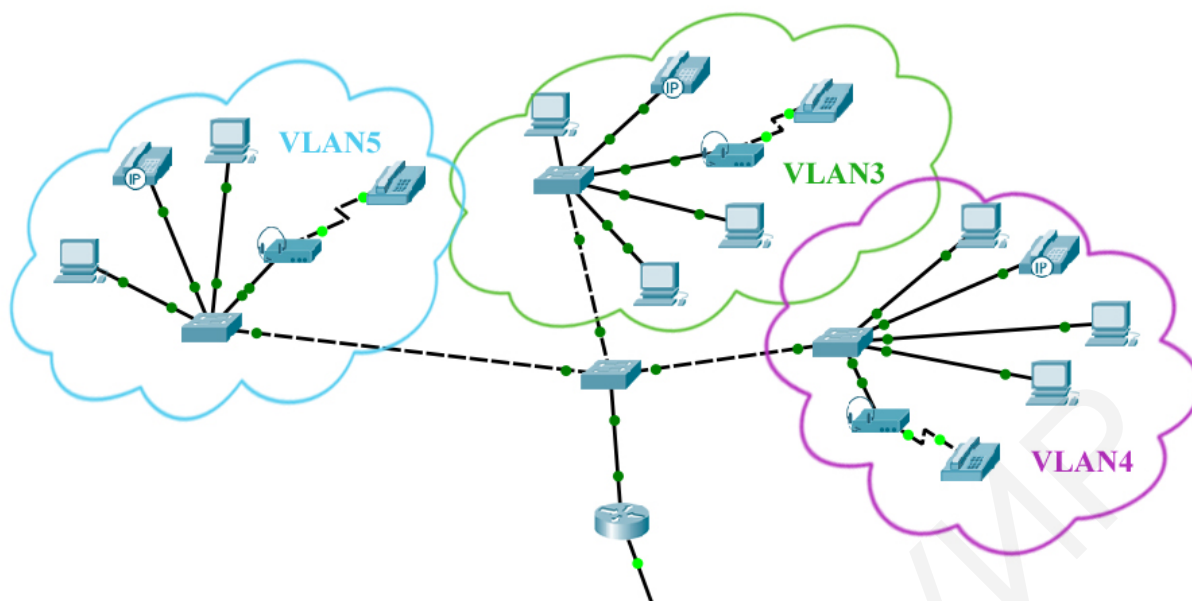


Рисунок 7.3 – Пример локальной сети с VoIP-телефонией

На канальном уровне в VoIP-телефонии используются коммутаторы, обеспечивающие соединение нескольких узлов компьютерной сети и распределение фреймов между устройствами на основе MAC-адресов. При проектировании VLAN для IP-телефонии создается отдельная Voice VLAN для изоляции голосового трафика, генерируемого IP-телефонами, от других данных. Ее использование целесообразно по двум причинам:

- создание отдельной VLAN для IP-телефонии уменьшает вероятность перехвата и анализа голосовых пакетов;
- создание отдельной VLAN позволяет задать повышенный приоритет голосовым пакетам и улучшить качество связи.

В сети на рисунке 7.3 настроены VLAN3, VLAN4, VLAN5. В целях добавления VLAN для IP-телефонии используются следующие команды в настройках интерфейсов с подключенными телефонными аппаратами.

```
Switch(config)#interface fastEthernet 5/1
Switch(config-if)#switchport voice vlan 10
```

На сетевом уровне происходит маршрутизация. Соответственно, основными устройствами сетевого уровня являются маршрутизаторы. Основной протокол, используемый на этом уровне, – IP, на основе которого и построена IP-телефония. У каждого телефонного аппарата должен быть IP-адрес. Аналоговым телефонным аппаратам IP-адрес не может быть присвоен, поэтому он присваивается VoIP-шлюзу. Для IP-адресации используется DHCP-сервер, который можно настроить на сервере или маршрутизаторе. Настройка DHCP-сервера на маршрутизаторе производится следующим образом:

```
Router(config)#ip dhcp pool Telephony
Router(dhcp-config)#network 192.168.80.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.80.1
Router(dhcp-config)#option 150 ip 192.168.80.1
```

Сначала с помощью команды `ip dhcp pool` имя осуществляется переход в режим настройки DHCP с заданным именем. Далее с помощью команды `network` IP-адрес маска\_подсети производится настройка IP-адреса сети, в которой находятся телефонные аппараты. Командой `default-router` задается IP-адрес маршрутизатора. Команда `option` количество ip IP-адрес указывает количество адресов, которое будет раздаваться, и IP-адрес маршрутизатора, который является сервером DHCP. Также необходимо исключить IP-адрес маршрутизатора из пула IP-адресов, используя команду `Router(config)#ip dhcp excluded-address 192.168.100.10`

В настройках VoIP-шлюза указывается адрес DHCP-сервера (рисунок 7.4).

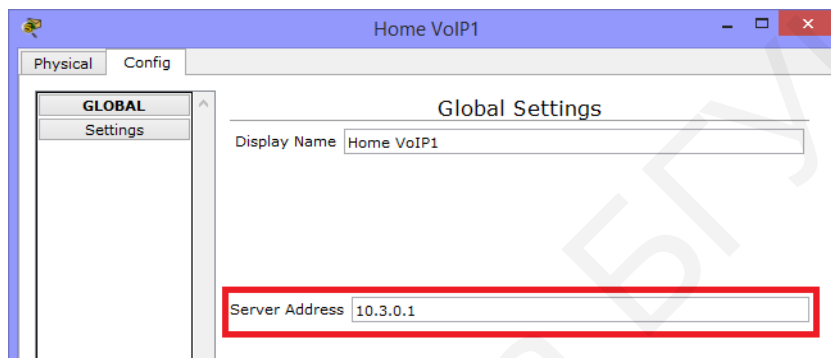


Рисунок 7.4 – Настройка VoIP-шлюза

Маршрутизатор может выступать в роли сервера управления. Для настройки сервиса телефонии используется команда `telephony-service`, затем настраивается максимальное количество подключаемых телефонных аппаратов и выделяемых телефонных линий командами `max-ephones` и `max-dn` соответственно. Команда `ip source-address` IP-адрес port номер задает интерфейс и порт, на которые будут приниматься пакеты IP-телефонии. Для маршрутизатора, приведенного на рисунке 7.3, сервис телефонии настраивается следующим образом.

```
Router(config)#telephony-service
Router(config-telephony)#max-ephones 10
Router(config-telephony)#max-dn 10
Router(config-telephony)#ip source-address 192.168.80.145 port 2000
```

Для присвоения телефонного номера необходимо создать телефонные линии командой `ephone-dn` номер и задать телефонный номер командой `number` номер. Для сети, изображенной на рисунке 7.3, необходимо создать 14 телефонных линий для все устройств, в том числе и компьютеров. Далее представлены команды для создания трех телефонных линий с номерами 801, 802, 803 соответственно:

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 801
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 802
```

```
Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 803
```

Для закрепления конкретного телефонного номера за определенным устройством необходимо внести это устройство в базу данных маршрутизатора, используя команду `ephone номер`, и указать MAC-адрес устройства командой `mac-address MAC-адрес`. Также указывается тип устройства командой `TYPE ТИП`. Существуют следующие типы устройств:

- АТА – тип аналогового телефона;
- 7960 – тип VoIP-телефона;
- CIPC – тип ПО CIPC для компьютера.

Для цифрового и аналогового телефона и компьютера, изображенного на рисунке 7.3, настройка телефонного номера осуществляется следующим образом:

```
Router(config)#ephone 1
Router(config-ephone)#mac-address 000A.F39B.1B01
Router(config-ephone)#TYPE ATA
Router(config-ephone)#button 1:1
Router(config)#ephone 2
Router(config-ephone)#mac-address 0060.5C17.D09A
Router(config-ephone)#type 7960
Router(config-ephone)#button 1:2
Router(config)#ephone 3
Router(config-ephone)#mac-address 000.D367.B233
Router(config-ephone)#type CIPC
Router(config-ephone)#button 1:3
```

Из представленных выше команд видно, что аналоговому телефону присваивается номер 801, так как команда `button 1:1` означает, что за телефонной линией под номером 1 с телефонным номером 801 закрепляется одно устройство типа АТА. По аналогии цифровому телефону присваивается номер 802, компьютеру 803.

Основные протоколы транспортного уровня – TCP (Transmission Control Protocol), UDP (User Datagram Protocol), RTP (Real-time Transport Protocol). Непосредственно в IP-телефонии используются протоколы UDP и RTP, причем основное их отличие от TCP заключается в том, что они не обеспечивают надежность доставки данных. Это является более приемлемым вариантом, чем осуществление контроля за доставкой (TCP), так как телефонная связь чрезвычайно зависима от задержек передачи, но менее чувствительна к потерям пакетов.

Протокол UDP является упрощенным транспортным протоколом, который выполняет сегментацию, как и протокол TCP, но при этом не обеспечивает надежность и управление потоком. К основным особенностям протокола UDP относятся следующие:

- не устанавливает соединение между узлами до того, как станут возможными отправка и получение данных;

- не использует процессы, которые требуют от отправителя повторной передачи потерянных или поврежденных данных;

- не предусматривает средства для повторной сборки данных в их исходной последовательности;

- не имеет механизмы управления объемами данных, которые пересылаются источником, для предотвращения перегрузок на устройстве назначения.

Источник отправляет данные. В случае чрезмерного использования ресурсов на узле назначения он, скорее всего, будет отклонять отправленные данные до тех пор, пока ресурсы не станут доступными. В отличие от TCP, протокол UDP не обладает механизмами повторной автоматической передачи отклоненных данных.

Протокол RTP обеспечивает сквозную передачу в реальном времени мультимедийных данных, таких как интерактивное аудио и видео. Этот протокол реализует распознавание типа трафика, нумерацию последовательности пакетов, работу с метками времени и контроль передачи.

Действие протокола RTP сводится к присваиванию каждому исходящему пакету временных меток. На приемной стороне временные метки пакетов указывают последовательность и задержки, с которыми их необходимо воспроизводить. Поддержка RTP позволяет принимающему узлу располагать принимаемые пакеты в надлежащем порядке, снижать влияние неравномерности времени задержки пакетов в сети на качество сигнала и восстанавливать синхронизацию между аудио и видео, чтобы поступающая информация могла правильно прослушиваться и просматриваться пользователями. Порядковые номера, включенные в RTP, позволяют получателю восстанавливать последовательность пакетов отправителя.

На трех последних уровнях модели OSI используются протоколы H.323, SIP, SCCP.

Протокол H.323 – самый первый протокол для IP-телефонии, разработанный Международным союзом электросвязи (ITU) в 1996 г. На сегодняшний день данный протокол используется довольно редко.

Протокол SIP – протокол сигнализации, предназначенный для организации, изменения и завершения сеансов связи. Данный протокол независим от транспортных технологий, однако при установлении соединения использует протокол UDP. Для передачи голосовой и видеoinформации применяется протокол RTP, но возможно использование других протоколов.

В протоколе SIP два типа сигнальных сообщений: запрос и ответ, которые могут быть со следующими флагами:

- INVITE – приглашение пользователя принять участие в сеансе связи (установление нового соединения);

- BYE – завершение соединения между двумя пользователями;

- OPTIONS – данные, которые используются для передачи информации о поддерживаемых характеристиках;

- ACK – подтверждение получения сообщения или положительного ответа на команду INVITE;
- CANCEL – отмена поиска пользователя;
- REGISTER – информация о местоположении пользователя.

Протокол SCCP (Skinny Client Control Protocol) предназначен для построения корпоративных телефонных сетей на основе оборудования Cisco. Данный протокол имеет гораздо более простую структуру и требует меньше компьютерных ресурсов для обработки своих сообщений. Как и большинство VoIP-протоколов, SCCP предназначен для обмена сигнальными сообщениями между клиентом и сервером в процессе установления и завершения звонка.

В процессе передачи речевых данных протокол SCCP использует RTP. Для передачи сообщений SCCP используется протокол TCP с портом 2000. По заголовку сообщения SCCP можно однозначно определить, в каком статусе находится текущее соединение. Данный протокол имеет большое разнообразие сообщений и отправляет их на сервер, ожидая руководства к дальнейшим действиям. Каждое событие фиксируется вплоть до получения сервером сообщения о том, что телефонная трубка снова в исходном положении.

Сообщения SCCP отправляются как в сторону клиента, так и в сторону сервера, поэтому для определения источника сообщения используются следующие идентификаторы: StationInit – если источником является клиент, StationIniD – если источником является сервер телефонии. Таким образом, появляется возможность в мельчайших деталях отследить любой звонок, совершенный внутри корпоративной сети.

Процесс обмена сообщениями можно пояснить следующим образом:

- IP-телефон (StationInit): снятие телефонной трубки;
- сервер (StationD): включение зуммера;
- сервер (StationD): выведение на дисплей сообщения «Введите номер»;
- IP-телефон (StationInit): начало вызова абонента, первая цифра его номера – «4»;
- IP-телефон (StationInit): вторая цифра – «7» и т. д.

## **7.2 Лабораторное задание**

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе №6. До начала выполнения необходимо открыть сохраненный файл с именем lab6.pkt, полученный в лабораторной работе №6, и проверить правильность соединений. В данной работе необходимо реализовать IP-телефонию в смоделированной в прошлых лабораторных работах локальной сети.

1. В смоделированную сеть добавить следующие устройства:

- аналоговый телефон (раздел «End devices» → «Phone»), который будет подключен к коммутатору через VoIP-шлюз (раздел «End devices» → «VoIP device»);

- IP-телефон 7960 (раздел «End devices» → «IP-Phone»).

Клиентские компьютеры будут осуществлять звонки при помощи ПО Cisco IP Communicator.

Для IP-телефона необходимо подключить адаптер питания.

Количество аналоговых и IP-телефонов выбирается в соответствии с третьей цифрой шифра из таблицы 7.1.

Таблица 7.1 – Количество телефонных аппаратов в сети

Третья цифра шифра	Количество аналоговых телефонов	Количество IP-телефонов	Номер голосового VLAN
0	5	1	100
1	4	2	200
2	3	3	300
3	2	4	400
4	1	5	500
5	3	3	600
6	4	2	700
7	5	1	800
8	2	4	900
9	1	5	10

2. Осуществить подключение добавленных устройств к разным коммутаторам. Для соединения устройств использовать прямой кабель Ethernet и телефонный кабель. Пример соединения представлен на рисунке 7.3.

3. Произвести настройку IP-адресации. В соответствии со второй цифрой шифра из таблицы 7.2 выбрать IP-адреса и телефонные номера для всех устройств и заполнить таблицу 7.3, в которой должны присутствовать не только телефоны, но и компьютеры.

Таблица 7.2 – IP-адреса для оконечных устройств

Вторая цифра шифра	Диапазон телефонных номеров	IP-адреса
0	550–560	192.168.13.2–192.168.13.250
1	840–850	192.168.12.2–192.168.12.250
2	120–130	192.168.123.2–192.168.123.250
3	950–960	192.168.58.2–192.168.58.250
4	230–240	192.168.35.2–192.168.35.250
5	480–490	192.168.8.2–192.168.8.250
6	330–340	192.168.5.2–192.168.5.250
7	770–780	192.168.7.2–192.168.7.250
8	660–670	192.168.113.2–192.168.113.250
9	200–210	192.168.74.2–192.168.74.250

Таблица 7.3 – Таблица адресации

Наименование устройства	IP-адрес	Маска подсети	MAC-адрес	Телефонный номер
		255.255.255.0		

В таблицу 7.3 необходимо внести MAC-адреса VoIP-шлюза, IP-телефона и других устройств. Для определения MAC-адресов IP-телефонов и шлюза необходимо просто навести на него курсор мыши (рисунок 7.5).

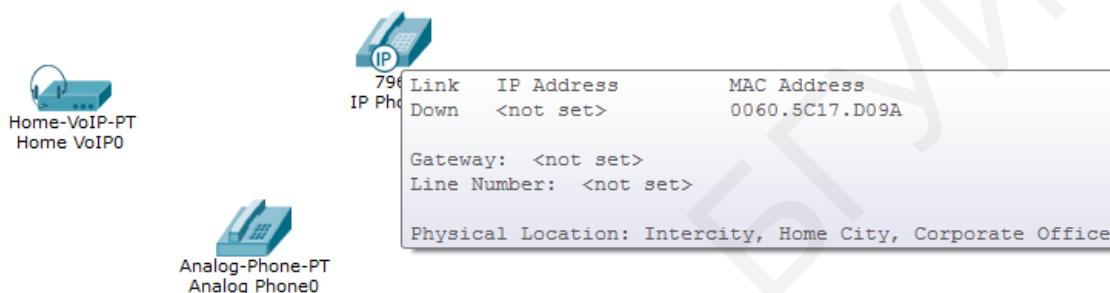


Рисунок 7.5 – Определение MAC-адреса IP-телефона

4. Настроить коммутаторы. На всех интерфейсах всех коммутаторов добавить VLAN для IP-телефонии. В отчете представить результат выполнения команды `show vlan brief` двух любых коммутаторов.

5. Настроить DHCP-сервер на маршрутизаторе для IP-телефонии. Настроить VoIP-шлюзы всех аналоговых телефонов. Проверить, что телефонные аппараты получили IP-адреса. Результаты выполнения команды `show ip dhcp pool имя` представить в отчете.

6. Осуществить настройку сервиса телефонии на маршрутизаторе. Создать необходимое количество линий и присвоить телефонные номера всем оконечным устройствам в сети.

7. Получить адреса и настроить SIPС на устройствах. Проверить, что телефоны получили телефонные номера. Для этого во вкладке «GUI» настроек телефонных аппаратов в правом верхнем углу должен появиться полученный номер телефона (рисунок 7.6, а). Для проверки телефонного номера на компьютерах необходимо перейти на вкладку «Desktop» и выбрать «Cisco IP Communicator». Номер должен отображаться в правом верхнем углу.

8. Проверить работоспособность. Осуществить телефонный звонок с аналогового телефона на компьютер, с компьютера на аналоговый телефон, с компьютера на IP-телефон, с IP-телефона на аналоговый телефон. Для этого набрать телефонный номер во вкладке «GUI» настроек телефонных аппаратов и нажать на телефонную трубку. На телефоне назначения должен быть зафик-



сирован звонок. Для звонка с компьютера также необходимо ввести номер вызываемого абонента и нажать клавишу «Dial».



*а* – IP-телефон; *б* – приложение Cisco IP Communicator

Рисунок 7.6 – Проверка присвоения телефонных номеров оконечным устройствам

9. В случае исправной работы всей сети сохранить текущую конфигурацию настроек маршрутизатора и коммутатора, для чего выполнить команду `copy running-config startup-config`. В отчете представить конфигурацию маршрутизатора. Сохранить файл под именем **lab7.pkt**.

### 7.3 Содержание отчета

1. Цель работы, исходные данные в соответствии с заданным вариантом из таблиц 7.1 и 7.2.
2. Результаты произведенных настроек (заполненная таблица 7.3, результаты выполнения команд из пунктов 4, 5, 9 подраздела 7.2), изображение смоделированной сети (см. пример на рисунке 7.3).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

### 7.4 Контрольные вопросы и задания

1. Представить структуру сети VoIP.
2. Каковы особенности канального уровня в VoIP-телефонии?
3. Описать особенность сетевого уровня модели OSI для VoIP-телефонии.
4. Перечислить протоколы транспортного уровня для VoIP, дать их краткую характеристику.
5. В чем заключается процесс передачи данных VoIP в соответствии с моделью OSI?
6. Описать отличия протоколов SIP и SCCP.

## ЛАБОРАТОРНАЯ РАБОТА №8 ТЕХНОЛОГИЯ IOT

**Цель:** изучить принципы построения сетей на основе технологии IoT; овладеть навыками настройки оборудования для управления и сбора информации с устройств.

### 8.1 Теоретическая часть

Интернет вещей (Internet of Things, IoT) – концепция вычислительной сети физических предметов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой без вмешательства со стороны человека с использованием протокола IP.

Реализация IoT возможна только при одновременной работе многочисленных компонентов:

- приложения и взаимодействие с пользователями;
- облачные вычислительные системы/платформы, способные обрабатывать данные и выполнять другие аналитические операции в режиме реального времени, хранение и доставка;
- сеть, доступ в Интернет (беспроводной/проводной, Wi-Fi, Bluetooth, сети поколения 3G/4G и др.);
- стандарты и протоколы связи для подключения датчиков к единой сети;
- физические объекты и устройства: датчики (преобразование информации об окружающей физической среде в сигнал), исполнительные механизмы (включение по сигналу датчика и выполнение необходимого действия).

Для преобразования информации о внешней среде в код, понятный машине, применяются различные средства измерения, играющие важную роль для IoT, наполняющие вычислительную среду приоритетной информацией.

Среди таких средств различные датчики (освещенности, температуры, влажности), приборы учета (интеллектуальные счетчики) и другие системы, включая сложные интегрированные измерительные комплексы. Измерительные средства объединены в сети, например сети беспроводных датчиков, из которых строятся целые системы взаимодействия.

Даже если вещь не имеет встроенного средства связи, она может иметь на себе идентификатор. В качестве идентификатора может служить штрихкод, QR-код или код Data Matrix. А для вещей, подключаемых к сетям, идентификатором является MAC-адрес адаптера, при помощи которого устройство идентифицируется на канальном уровне.

Архитектура IoT предполагает наличие следующих функциональных уровней: сеть датчиков, шлюз, управление, приложение (рисунок 8.1). Поскольку нижний уровень состоит из датчиков, сенсоров, то сразу же возникает необходимость в протоколах для обеспечения взаимодействия этих устройств друг с другом и верхними уровнями. Стандартные прикладные

протоколы не подходят ввиду их неприспособленности к условиям концепции IoT. Датчик, обычно миниатюрный, с небольшой памятью измеряет физические параметры в режиме реального времени, чаще всего в условиях низкого энергообеспечения. Результаты измерений обрабатываются сенсорным узлом и передаются на сервер. Объем информации, формируемый одним сенсорным узлом, сравнительно небольшой, однако большинство сервисов IoT построено на принципе обработки информации от множества узлов, что принципиально отличается от архитектур, принятых в классических сетях.

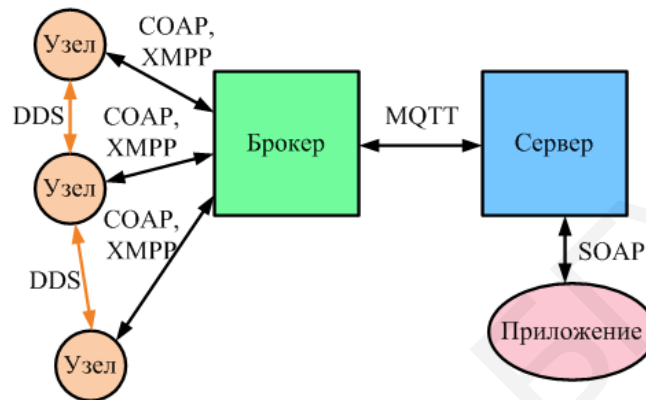


Рисунок 8.1 – Топология IoT

Представленная на рисунке 8.1 топология соответствует передаче сообщений по сценарию «издатель – подписчик» (Publisher – Subscriber, или pub/sub). В такой схеме вводится понятие издателя – источника информации – и подписчика – ее получателя. Термин «подписка» обозначает определенные операции, выполняемые участниками с целью получения информации подписчиком от конкретного издателя, а также упорядочивания сбора информации – параметров периодичности получения.

В данном случае рассматривается ситуация, когда сенсорный узел (Node) объединяет информацию от нескольких датчиков (например, данные телеметрической системы) и направляет ее согласно параметрам подписки либо по запросу, либо самостоятельно с определенным интервалом времени или по происшествии какого-либо события на сервер. Обычно сами датчики достаточно примитивны, их задачи сводятся к постоянной передаче информации о контролируемом параметре. Поэтому появляется необходимость объединять датчики в узлы, оснащенные микроконтроллерами, которые будут отвечать за считывание измеряемых данных и отправку их по заранее определенным алгоритмам на сервер. Чаще всего для взаимодействия клиента с системой необходимо клиентское приложение (Application), установленное на персональном устройстве, служащее для графического представления получаемой с датчиков или уже обработанной сервером информации и управления системой. Такая топология рассчитана на включение брокера (Broker).

Брокер – это сервер, который принимает информацию от издателей и передает ее соответствующим подписчикам, в сложных системах также может выполнять различные операции, связанные с анализом и обработкой поступивших данных, устанавливать приоритеты сообщениям и формировать очереди для передачи сообщений. Таким образом, брокер организует пересылку сообщений, их хранение и фильтрацию. Под очередью сообщений понимается контейнер, или блок, в котором хранятся сообщения в процессе их пересылки. При недостаточном ресурсе канала связи или если получатель недоступен во время отправки сообщения, очередь хранит сообщение до тех пор, пока оно не будет доставлено.

На участке между сенсорными узлами (участок 1) выполняется ряд задач, заключающихся в распределении информации между сенсорными узлами для временного хранения или перенаправления. Для обеспечения связи между сенсорными узлами/датчиками используется протокол DDS (Data Distribution Service), который распределяет данные между устройствами. Протокол DDS реализует многоадресную систему, используя протокол UDP, при этом передача сообщений производится с использованием метода «запрос – ответ». Операции, выполняемые протоколом, задаются тринадцатью классами (Entity Class, WaitSet Class, Condition Class, Publisher Class, DataWriter Class, Subscriber Class, DataReader Class, ReadCondition Class, QueryCondition Class и др.). Протокол DDS реализует две основные операции – чтения и записи, используя соответствующие классы.

Операция чтения (Read) осуществляется на всех доступных устройствах. В результате этой операции данные не удаляются из локального кеша DDS и могут быть прочтены снова при указании специальных параметров. Получение данных осуществляется тремя следующими способами:

- опрос (Polling) – приложение периодически запрашивает данные DDS для информирования о смене состояния;
- списки ожидания (WaitSets) – приложение регистрирует списки ожидания и ждет, пока одно из переданных событий не произойдет;
- слушатели (Listeners) – приложение регистрирует специальные классы-слушатели, которые будут информированы при наступлении этих событий.

На участке узел – брокер реализуется несколько задач, например такие, как регистрация сенсорного узла, конфигурация и настройки узлов, передача и распределение информации и т.д. На этом сегменте сети могут использоваться протоколы XMPP и COAP.

XMPP (Extensible Messaging and Presence Protocol) – протокол обмена сообщениями и информацией о присутствии. Применительно к IoT XMPP обеспечивает простой способ адресации устройств. Для идентификации пользователей используются запоминающиеся идентификаторы (JID), по формату похожие на адреса электронной почты (например, username@yandex.ru). В протоколе XMPP применяется текстовый формат XML. В качестве транспортного протокола используется протокол TCP.

XMPP поддерживает различные коммуникационные модели («запрос – ответ», «публикация – подписка» и др.).

Адресация XMPP особенно удобна в случаях, когда данные передаются между отдаленными, чаще всего независимыми точками, например, при взаимодействии двух абонентов. С помощью XMPP, например, возможно подключение домашнего термостата к веб-серверу для получения к нему доступа с телефона. Сильными сторонами этого протокола являются также безопасность и масштабируемость, что делает его идеальным для приложений IoT с ориентацией на потребителя.

COAP (Constrained Application Protocol) – это специализированный протокол передачи, созданный для сетей и устройств с ограниченными ресурсами. Его можно рассматривать как дополнение к HTTP, но в отличие от HTTP протокол COAP нацелен на применение в устройствах с определенными ограничениями. COAP использует транспортный протокол UDP.

Сообщения, применяемые протоколом COAP, основаны на механизме «запрос – ответ»: GET, PUT, HEAD, POST, DELETE, CONNECT. Клиенты используют сообщения для управления и наблюдения за ресурсом. По запросу устанавливается флаг наблюдения, и сервер продолжает отвечать после того, как первоначальное сообщение было передано. Это позволяет серверам организовывать потоковую передачу изменений состояний датчиков.

На участке сети брокер – сервер можно выделить следующие задачи: сбор и агрегация данных; организация очередей сообщений; распределение и хранение информации.

Протокол MQTT (Message Queue Telemetry Transport) предназначен для телеметрии и дистанционного мониторинга. Используется для обмена сообщениями между устройствами по принципу «издатель – подписчик», позволяет устройствам посылать и получать данные при возникновении некоторого события. Данный протокол является бинарным: основан на публикации или подписке, работающих с применением транспортного протокола TCP. Протокол использует 14 сообщений, предполагающих запрос и ответ: CONNECT, CONNACK, PUBLISH, PUBACK, PUBREC, PUBREL, PUBCOMP, SUBSCRIBE, SUBACK, UNSUBSCRIBE, UNSUBACK, PINGREQ, PINGRESP, DISCONNECT. Протокол MQTT подходит для загруженных сетей с большим количеством устройств, так как снижает нагрузку на канал за счет организации очередей.

Для сетей, использующих оборудование различных платформ и допускающих применение простого протокола передачи сообщений, можно использовать STOMP.

STOMP (Simple (или Streaming) Text Oriented Message Protocol) – простой протокол обмена сообщениями, предполагающий широкое взаимодействие со многими языками, платформами и брокерами. Данный протокол подходит под шаблон «издатель – подписчик» и с помощью сообщений SEND, SUBSCRIBE, UNSUBSCRIBE, BEGIN, COMMIT, ABORT, ACK, NACK, DISCONNECT организует связь с брокером по методу «запрос – ответ».

Протокол в целом похож на HTTP, использует транспортный протокол TCP, является простым текстовым, что позволяет клиентам STOMP общаться с любым брокером сообщений, поддерживающим данный протокол. Таким образом, это способ взаимодействия, разработанный для обмена сообщениями между платформой, описываемой на одном языке программирования, и клиентом, программное обеспечение которого разработано на другом языке.

Заключительным участком топологии, представленной на рисунке 8.1, является сегмент, ориентированный на взаимодействие сервера с приложением пользователя. На данном участке выполняются задачи, связанные с взаимодействием пользователя и системы: получение информации с сервера (возможно, с участием сервера-посредника, поскольку информация может быть распределена); конфигурация пользователем параметров (частота получения информации, активация/деактивация датчиков и узлов и т. д.).

Для распределенной вычислительной среды, для веб-сервисов наиболее часто используемым является протокол SOAP, так как у него выделен механизм доступа RPC (Remote Procedure Call), который отвечает за удаленный вызов функций.

SOAP (Simple Object Access Protocol) – протокол обмена структурированными и произвольными сообщениями формата XML в распределенной вычислительной среде. SOAP использует базовую модель соединения, обеспечивающую согласованную передачу сообщения от отправителя к получателю, потенциально допускающую наличие посредников, которые могут обрабатывать часть сообщения или добавлять к нему дополнительные элементы. SOAP поддерживает два механизма доступа – SOAP RPC и SOAP Message.

SOAP RPC представляет собой простой протокол «запрос – ответ», который основывается на объекте Call. Этот объект (и некоторые низкоуровневые методы для создания и отсылки сообщений) используется для синхронного удаленного вызова процедур с помощью XML.

SOAP Message – это протокол для отсылки и обработки SOAP-сообщений, который может использоваться для асинхронных коммуникаций и подразумевает немедленный или отложенный ответ на запрос.

Благодаря всего нескольким сообщениям (Get, SOAPAction, SOAPAction-Response), подразумевающим «запрос – ответ», протокол может использоваться с любым протоколом прикладного уровня: SMTP, FTP, HTTP, HTTPS.

Для организации технологии IoT в Cisco Packet Tracer имеется шлюз управления DLC100, к которому осуществляется как проводное, так и беспроводное подключение устройств. На рисунке 8.2 представлен пример технологии IoT, в котором к локальной сети организации подключается шлюз управления (порт Internet). Так как планируется подключение к нему большого числа устройств IoT, к порту Ethernet шлюза управления подключается коммутатор.

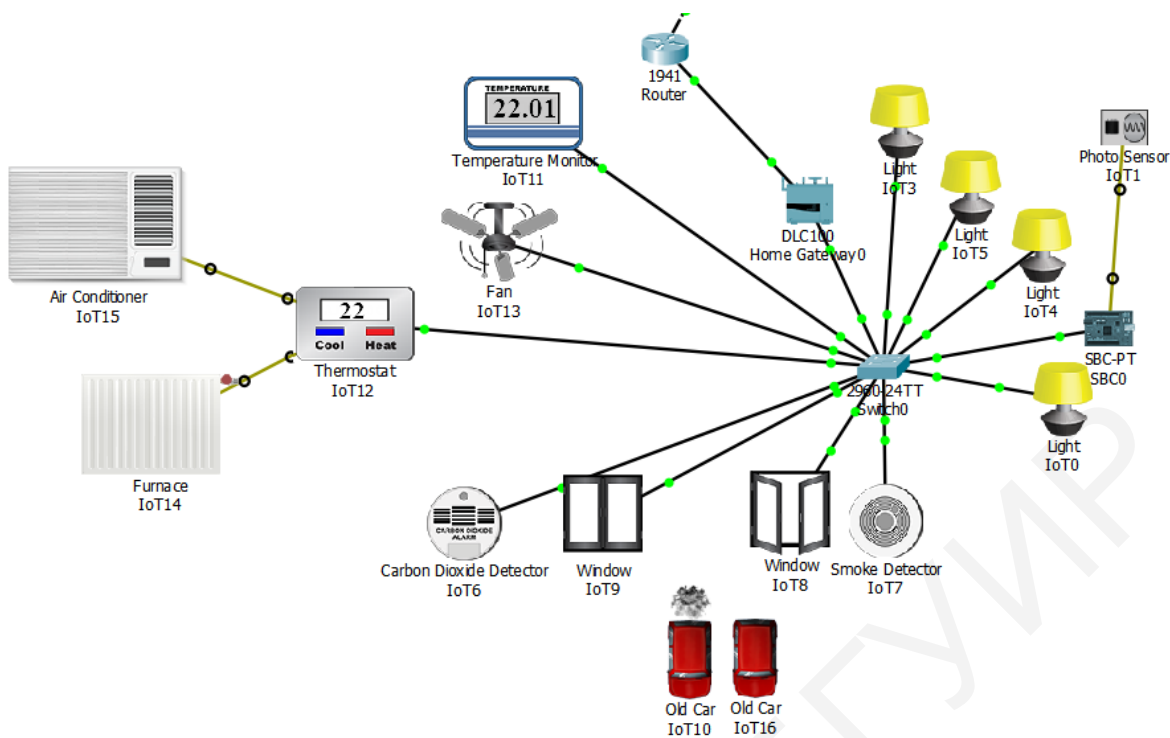


Рисунок 8.2 – Пример подключения устройств в технологии IoT

В настройках шлюза управления на закладке «Config» осуществляется настройка соединения с провайдером (Internet) и беспроводное соединение (Wireless). Возможно использование различных датчиков и устройств IoT, список которых представлен в таблице 8.1. Более подробное описание устройств можно получить в настройках устройства на вкладке «Specifications».

В Cisco Packet Tracer реализовано динамическое управление средой (температура, газ, давление, свет и др.), чтобы сделать моделирование устройств IoT более реалистичным. В правом верхнем углу главного рабочего окна Cisco Packet Tracer есть кнопка «Environment», при нажатии которой открывается окно состояния параметров окружающей среды (рисунок 8.3). Многие устройства или вещи влияют на окружающую среду или реагируют на нее. Например, при нажатии «Old Car» (Alt + щелчок кнопкой мыши) увеличивается содержание различных газов (например, углекислого) в окружающей среде, что может быть зафиксировано детектором дыма и/или углекислого газа, и затем дан сигнал тревоги. В данном окне доступно только изменение текущего времени, в результате чего меняются остальные параметры среды, зависящие от времени суток (уровень видимого света).

Для сбора информации с устройств и удаленного управления ими используется сервис IoT, который может быть активирован на сервере. Для доступа к мониторингу за устройствами в браузере любого компьютера необходимо ввести IP-адрес сервера и авторизоваться (рисунок 8.4, а), в результате отображается список всех подключенных устройств и их состояние (рисунок 8.4, б).

Таблица 8.1 – Список устройств, доступных для IoT в Cisco Packet Tracer

Название устройства		Свойства
Детектор углекислого газа	Carbon Dioxide Detector	Определяет уровень углекислого газа
Детектор дыма	Smoke Detector	Определяет уровень дыма
Светильник	Light	Изменяет уровень видимого света
Старая машина	Old Car	Увеличивает уровень углекислого газа, угарного газа, дыма
Окно	Window	При закрытом/открытом окне уменьшается/увеличивается уровень углекислого газа и дыма
Фотосенсор	Photo Sensor	Определяет уровень света
Монитор температуры	Temperature Monitor	Собирает данные о температуре окружающей среды
Термостат	Thermostat	Осуществляет регулировку обогревателя и кондиционера
Обогреватель	Furnace	Повышает температуру окружающей среды, обычно подключается к порту D1 термостата
Кондиционер	Air Conditioner	Понижает температуру окружающей среды, обычно подключается к порту D2 термостата
Вентилятор	Fan	Имеет два режима вращения (быстрый и медленный)

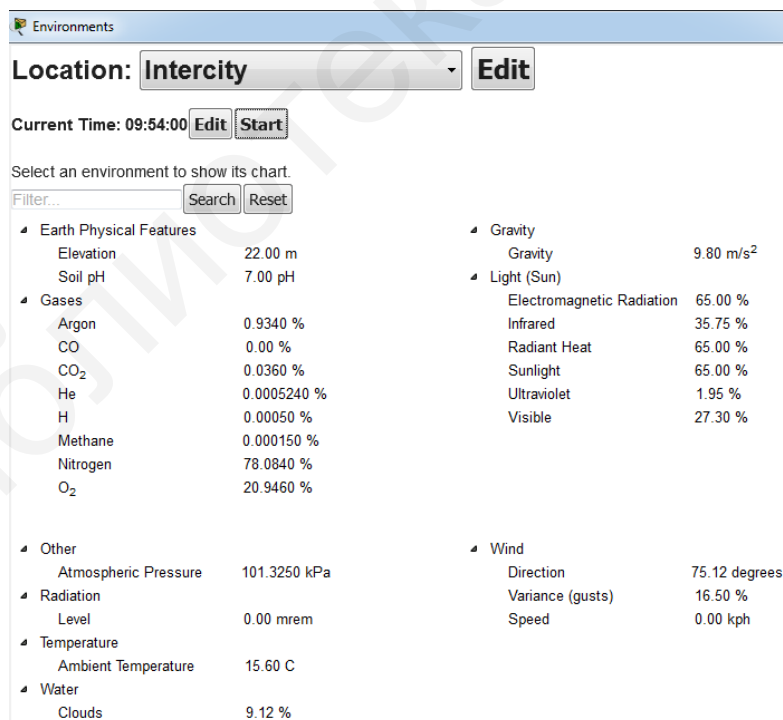
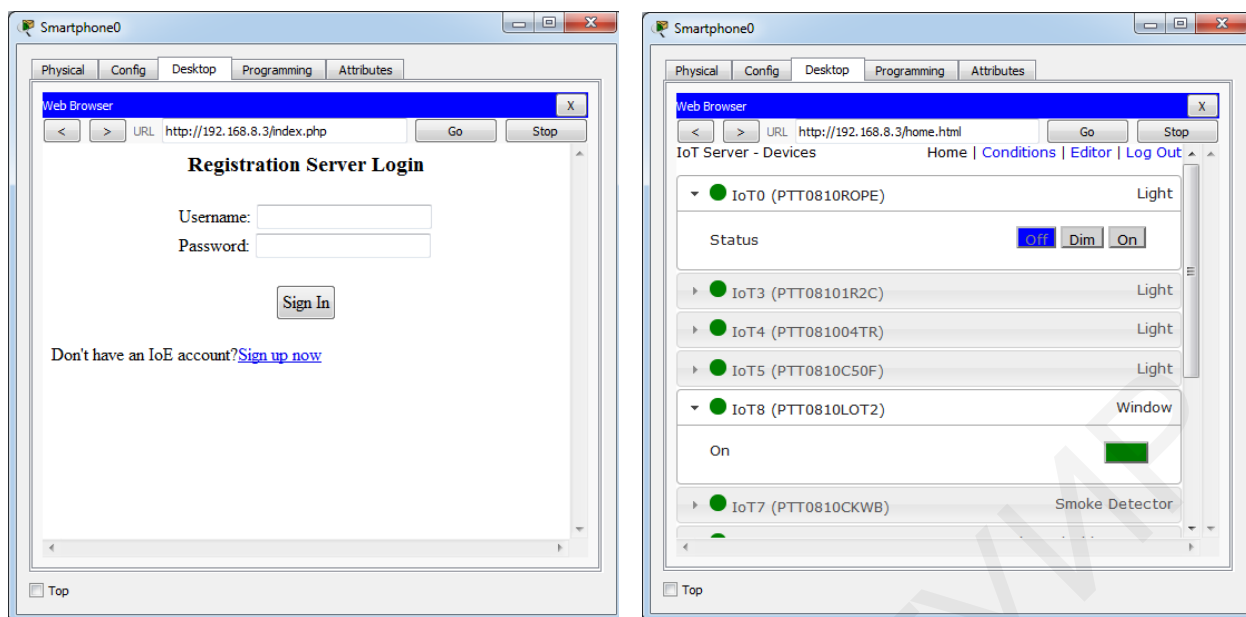


Рисунок 8.3 – Окно динамического наблюдения за изменением параметров окружающей среды





*a*

*б*

*a* – окно авторизации на сервере; *б* – окно мониторинга устройств IoT

Рисунок 8.4 – Сервер IoT

На закладке «Conditions» можно создавать условия включения или отключения устройств. На рисунке 8.5 представлен пример добавления условия закрытия окон (IoT8 и IoT9) при увеличении уровня угарного газа, передаваемого детектором углекислого газа и детектором дыма (IoT6 и IoT7), выше 1. Для открытия окон необходимо добавить обратное условие. Условие сохраняется после нажатия кнопки «Ok».

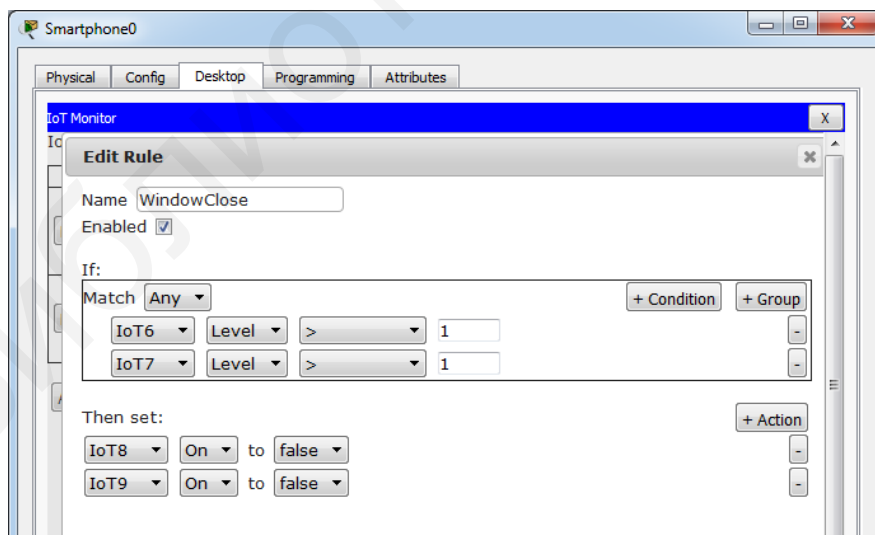
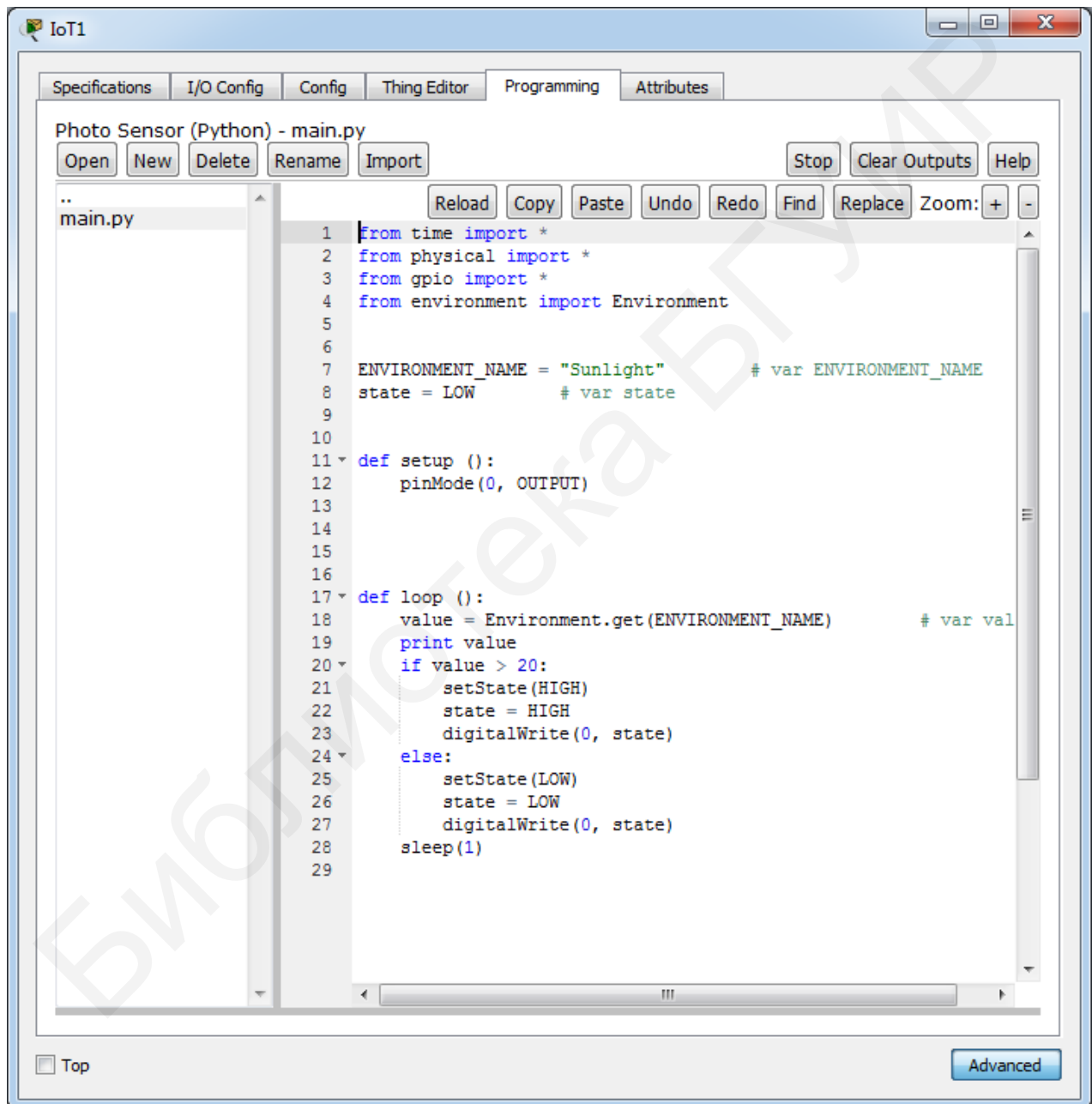


Рисунок 8.5 – Добавление условия закрытия окон

Датчики или сенсоры подключаются к микроконтроллеру (MCU-PT) или компьютерам с одиночной платой (SBC-PT). Они, как правило, не имеют сетевого интерфейса и полагаются на MCU-PT или SBC-PT для доступа к сети. Это простые устройства, которые общаются только через свои аналоговые

или цифровые слоты. Например, для подключения фотодатчика к плате SBC-PT применяется IoT-кабель (IoT Custom Cable). Плата может использовать порт Ethernet для подключения к сетевым устройствам. Возможно изменение кода работы любого устройства, для чего необходимо перейти на вкладку «Promting», для ее отображения необходимо нажать кнопку «Advansed» в окне настройки устройства. На рисунке 8.6 представлен пример изменения кода фотосенсора. Код работы платы, к которой подключается фотосенсор, представлен на рисунке 8.7.



```
Photo Sensor (Python) - main.py
Open New Delete Rename Import Stop Clear Outputs Help
Reload Copy Paste Undo Redo Find Replace Zoom: + -
..
main.py
1 from time import *
2 from physical import *
3 from gpio import *
4 from environment import Environment
5
6
7 ENVIRONMENT_NAME = "Sunlight" # var ENVIRONMENT_NAME
8 state = LOW # var state
9
10
11 def setup ():
12     pinMode(0, OUTPUT)
13
14
15
16
17 def loop ():
18     value = Environment.get(ENVIRONMENT_NAME) # var val
19     print value
20     if value > 20:
21         setState(HIGH)
22         state = HIGH
23         digitalWrite(0, state)
24     else:
25         setState(LOW)
26         state = LOW
27         digitalWrite(0, state)
28     sleep(1)
29
```

Top Advanced

Рисунок 8.6 – Код работы фотосенсора

```
..
main.py
1 from gpio import *
2 from time import *
3 from ioeclient import *
4
5 state = LOW
6
7 def detect():
8     global state
9     newState = digitalRead(0)
10    if (newState != state):
11        state = newState
12        sendReport('1' if newState == HIGH else '0')
13
14 def main():
15     pinMode(1, OUT)
16     state = 0
17     newState = 0
18
19     IoEClient.setup({
20         'type': 'Server',
21         'states': [{
22             'name': 'Light Status',
23             'type': 'options',
24             'options': {
25                 '0': 'off',
26                 '1': 'on'
27             },
28             'controllable': False
29         }]
30     })
31     sendReport(str(newState))
32     add_event_detect(0, detect)
33
34     while True:
35         delay(1000)
36
37
38 def sendReport(input):
39     IoEClient.reportStates(input)
40
41 if __name__ == "__main__":
42     main()
```

Рисунок 8.7 – Код работы платы для регулировки освещения

## 8.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе №7. До начала выполнения необходимо открыть сохраненный файл с именем lab7.pkt, полученный в лабораторной работе №7, и проверить правильность соединений. В данной работе необходимо создать простейшую сеть по технологии IoT, исходя из следующих заданий.

1. Добавить и подключить к маршрутизатору шлюз управления (DLC100) из раздела «Network devices» → «Wireless devices», к которому в свою очередь подключить коммутатор 2960-24TT. Настроить шлюз управления:

- настроить получение IP-адреса шлюзом управления по протоколу DHCP;
- настроить локальное беспроводное соединение для подключаемых к шлюзу устройств, назначить SSID, пароль для WPA2-PSK, которые должны содержать фамилию студента.

2. Активировать на любом сервере сервис IoT на закладке «Services». Добавить двух пользователей (из ранее созданных в других лабораторных работах) для удаленного доступа к серверу IoT. Используя браузер любого компьютера, осуществить подключение к серверу и авторизацию под именем любого пользователя.

3. Проконтролировать снижение уровня дыма и углекислого газа в помещении:

- добавить на рабочую область Old Car, активировать ее и с помощью мониторинга окружающей среды установить, какие параметры изменяются и насколько;

- добавить детектор дыма и детектор углекислого газа, а также не менее двух окон из раздела «End devices» → «Home», осуществить их подключение к коммутатору шлюза управления;

- добавить условия на сервере, которые предусматривают закрытие окон, если уровень дыма и углекислого газа увеличивается; критический уровень газа, при котором происходит закрытие окон, выбрать самостоятельно; если уровень меньше критического – открыть окна;

- проверить правильность работы установленного условия, отобразить результат в отчете.

4. Установить автоматическое регулирование света в помещении:

- добавить не менее четырех светильников, фотосенсор и SBC-плату из раздела «Componets» → «Boards», осуществить соединение светильников с коммутатором шлюза управления, фотосенсор подключить к SBC-плате, а плату к коммутатору;

- изменить код фотосенсора в соответствии с рисунком 8.6; а код SBC-платы – в соответствии с рисунком 8.7;

- добавить условия на сервере, которые предусматривают включение светильников при уменьшении уровня света на 20 %;

- проверить правильность работы установленного условия, отобразить результат в отчете.

5. Установить автоматическое регулирование температуры в помещении:

- добавить устройство мониторинга температуры, термостат, обогреватель, кондиционер и вентилятор, осуществить подключение устройства мониторинга температуры, термостата и вентилятора к коммутатору шлюза управления, кондиционер и вентилятор подключить к необходимым портам термостата.

- обеспечить постоянную температуру в помещении (20–22 °С), добавить необходимые условия на сервер;

- проверить правильность работы установленного условия, отобразить результат в отчете.

6. Перейти в режим симуляции времени и определить, какие типы пакетов передаются при увеличении уровня углекислого газа. Заполнить таблицу 8.2.

Таблица 8.2 – Процесс обмена информацией в сети IoT

Номер шага	Отправитель	Получатель	Тип пакета	Содержание пакета
1				
2				
3				

### 8.3 Содержание отчета

1. Цель работы.
2. Результаты произведенных настроек (см. пункты 3, 4, 5 подраздела 8.2), заполненная таблица 8.2, изображение смоделированной сети (см. пример на рисунке 8.2).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

### 8.4 Контрольные вопросы и задания

1. Перечислить основные функции IoT и условия его реализации.
2. Изобразить топологию IoT, основные элементы. Перечислить их функции.
3. Пояснить процесс взаимодействия между сенсорными узлами.
4. В чем заключаются отличия протоколов XMPP и SOAP?
5. Объяснить процесс обмена информацией на участке сети «брокер – сервер».
6. Пояснить процесс взаимодействия сервера IoT с приложением пользователя.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Яницкая, Т. С. Учебно-методический комплекс по дисциплине «Сети и телекоммуникации» / Т. С. Яницкая. – Тольятти : ПВГУС, 2016. – 228 с.
2. Руденков, Н. А. Основы сетевых технологий : учебник / Н. А. Руденков, Л. И. Долинер. – Екатеринбург : Изд-во Уральского федерального ун-та, 2011. – 300 с.
3. Гойхман, В. Аналитический обзор протоколов Интернета вещей / В. Гойхман, А. Савельева // Технологии и средства связи. – №4. – 2016. – С. 32–37.
4. IP-телефония в компьютерных сетях : учеб. пособие / И. В. Баскаков [и др.]. – М. : Интернет-Университет Информационных Технологий ; БИНОМ. Лаборатория знаний, 2008. – 184 с.
5. Воронин, А. А. Вычислительные сети : учеб. пособие / А. А. Воронин. – Владимир : Изд-во Владим. гос. ун-та, 2011. – 88 с.
6. Скуднев, Д. М. Компьютерные коммуникации и сети. Лабораторный практикум. Ч. 1 / Д. М. Скуднев, В. Р. Субботин, С. В. Ананьев. – Липецк : ЛГПУ, 2011. – 145 с.
7. Компьютерные сети. Лабораторный практикум : пособие / В. Н. Комличенко [и др.]. – Минск : БГУИР, 2013. – 76 с.
8. Амато, В. Основы организации сетей Cisco. Т. 1 / В. Амато ; пер. с англ. ; А. А. Голубенко. – М. : Изд. дом «Вильямс», 2002. – 512 с.

*Учебное издание*

**Белоусова Елена Сергеевна**

**ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ.  
ЛАБОРАТОРНЫЙ ПРАКТИКУМ**  
**УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ**

Редактор *М. А. Зайцева*

Корректор *Е. Н. Батурчик*

Компьютерная правка, оригинал-макет *М. В. Касабуцкий*

Подписано в печать 04.05.2020. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».  
Отпечатано на ризографе. Усл. печ. л. 6,16. Уч.-изд. л. 6,5. Тираж 35 экз. Заказ 19.

Издатель и полиграфическое исполнение: учреждение образования  
«Белорусский государственный университет информатики и радиоэлектроники».  
Свидетельство о государственной регистрации издателя, изготовителя,  
распространителя печатных изданий №1/238 от 24.03.2014,  
№2/113 от 07.04.2014, №3/615 от 07.04.2014.  
Ул. П. Бровки, 6, 220013, г. Минск