Федеральное агентство связи
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

И. Г. Квиткова

Методические указания к лабораторным работам по дисциплине «Математические основы моделирования сетей связи»

для студентов очной и заочной форм обучения,
обучающихся по направлению
11.03.02 «Инфокоммуникационные технологии и системы связи»,
профиль «Сети связи и системы коммутации»

Новосибирск - 2018

УДК 004.71:004.72:004.738

Квиткова И.Г. Методические указания к лабораторным работам по дисциплине «Математические основы моделирования сетей связи» / И.Г. Квиткова. – Новосибирск: СибГУТИ, 2018. – 28 с.

В методических указаниях описаны способы построения локальных сетей с применением программных пакетов моделирования, в частности, эмулятора сетей NetEmul. Эмулятор позволяет моделировать TCP/IP сети различной топологии, производить настройки сетевых интерфейсов используемого оборудования, отслеживать движение пакетов по сети.

Выполнение лабораторных работ позволит изучить ряд основных сетевых протоколов (TCP, IP, ARP, DHCP, протоколы динамической маршрутизации), приобрести навыки по настройке сетевого оборудования.

Предназначено для студентов очной и заочной форм, обучающихся по направлению 11.03.02 – Инфокоммуникационные технологии и системы связи.

Кафедра передачи дискретных сообщений и метрологии

Ил. 20, табл. 8, список лит. – 7 наименований.

Рецензент:

Утверждено редакционно-издательским советом СибГУТИ в качестве методических указаний.

Оглавление

1. Описание интерфейса программного эмулятора NetEmul

Лабораторные работы выполняются с применением программного эмулятора компьютерных сетей NetEmul и направлены на закрепление базовых знаний по построению локальных сетей.

Программа NetEmul предназначена для моделирования компьютерных сетей, предоставляя возможность создавать, конфигурировать сети и проверять их доступность.

Интерфейс программы NetEmul изображен на рисунке 1.

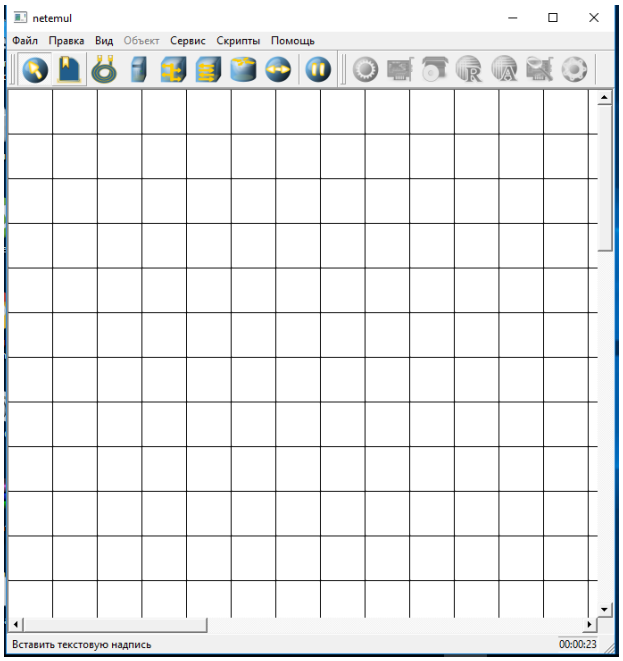

Рисунок 1 – Интерфейс программы NetEmul

Интерфейс включает в себя главное меню программы, панель устройств, панель инструментов и рабочую область программы.

Главное меню представлено на рисунке 2.

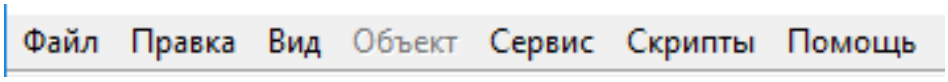

Рисунок 2 – Главное меню программы NetEmul

Файл - для создания нового или открытия старого проекта, сохранения, печати проекта, предпросмотра получившейся модели сети;

Правка – отменить/вернуть действие пользователя;

Вид - настройка видимости панелей программы;

Объект - для настройки выделенного устройства;

Сервис - просмотреть статистику всей сети; изменить количество портов устройств; настройка языка и скорости анимации;

Скрипты – примеры готовых моделей сетей;

Помощь - справка по использованию программы.

Вкладка **Сервис** имеет всплывающее меню: Статистика и Настройки. Меню настройки изображено на рис. 3. Здесь можно установить язык интерфейса

программы, а также изменить скорость анимации. Здесь также можно изменить количество портов устройств по умолчанию и стандартные параметры.

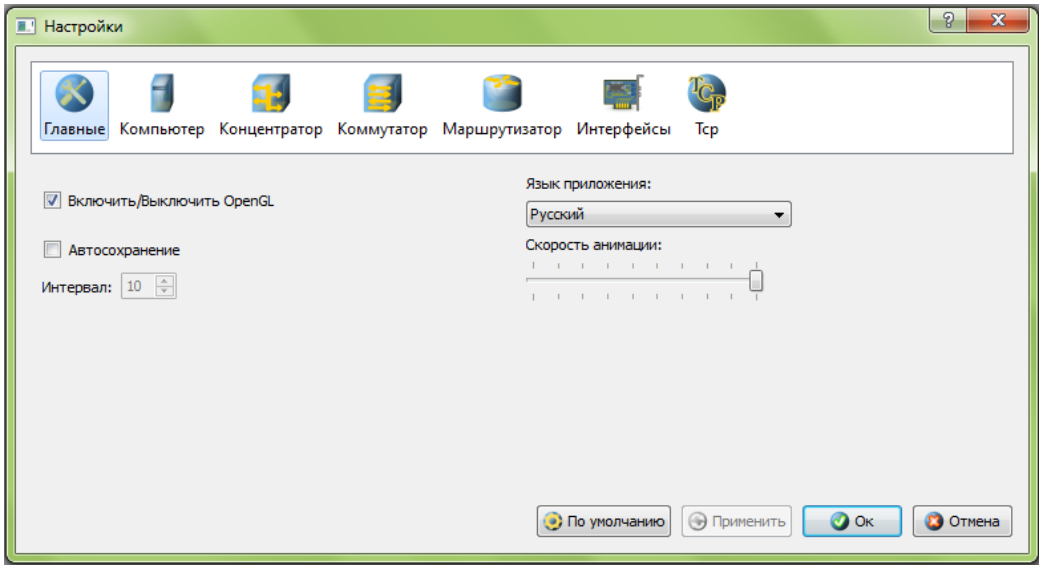

Рисунок 3 – Окно Настройки **Сервиса**

Панель устройств изображена на рисунке 4.

Рисунок 4 – Панель устройств

Описание панели устройств слева направо:

1) перемещение объектов - для перемещения устройств;
2) вставить текстовую надпись - для добавления текста – комментария;
3) создать соединение - для соединения устройств;
4) добавить компьютер;
5) добавить концентратор;
6) добавить коммутатор;
7) добавить маршрутизатор;
8) отправить данные – для проверки работоспособности сети;
9) остановить – прекращает передачу данных.

Панель параметров (рис. 5) появляется при выборе какого-либо устройства сети. Для каждого сетевого устройства применяются собственные настройки, поэтому не всегда все пункты доступны.

Рисунок 5 – Панель инструментов

Описание панели инструментов слева направо:

1) показать свойства – отображает свойства сетевого устройства

(для компьютера – шлюз и вкл./выкл. маршрутизации, для концентратора и маршрутизатора – количество портов и MAC-адрес, для маршрутизатора – количество портов и вкл./выкл. маршрутизации);

2) редактировать интерфейсы – задаются IP-адрес и маска подсети (для компьютера и маршрутизатора);
3) установленные программы - установка программ (RIP, DHCP-client, DHCP-server) на компьютер или маршрутизатор;
4) таблица маршрутизации – выбор правил маршрутизации;
5) ARP-таблица – создает соответствие между MAC-адресами и IP-адресами;
6) показать журнал устройства – отображение пакетов, проходящих через сетевое устройство.

2. Правила оформления отчёта

При выполнении лабораторной работы необходимо оформить отчёт, включающий в себя основные результаты моделирования. Отчёт может быть оформлен как в рукописном, так и в печатном виде.

1. Титульный лист отчёта должен иметь вид:

Федеральное агентство связи
СибГУТИ

Кафедра ПДСиМ

Отчёт по лабораторной работе № 1
Построение простых моделей компьютерных сетей в NetEmul

Группа:_____

Выполнил:_____

Новосибирск 20__

2. Отчёт должен содержать:

- цель лабораторной работы;
- ответы на контрольные вопросы (с указанием ссылок на источники, со списком использованных источников);
- исходные данные;
- выкладки по определению диапазона IP-адресов и количества узлов заданной сети;
- по каждому пункту необходимо привести схему модели сети с указанием IP-адресов и номеров интерфейсов;
- по каждому пункту должны быть приведены выводы по работе.

3. Определение количества хостов и подсетей на основе IP-адреса и маски

Понятие IP-адреса. IP-адрес (сокращение от англ. Internet Protocol Address) — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

Протокол IP является ненадежным протоколом без установления соединения. Это означает, что протокол IP не подтверждает доставку данных, не контролирует целостность полученных данных и не производит операцию квитирования (handshaking) - обмена служебными сообщениями, подтверждающими установку соединения с узлом назначения и его готовность к приему данных. Протокол IP обрабатывает каждый пакет (дейтаграмму) как независимую единицу, не имеющую связи ни с какими другими пакетами (дейтаграммами) в сети Интернет. После того, как пакет (дейтаграмма) отправляется в сеть, его дальнейшая судьба никак не контролируется отправителем (на уровне протокола IP). Если пакет (дейтаграмма) не может быть доставлен, он уничтожается. Узел, уничтоживший пакет (дейтаграмму), может оправить по обратному адресу ICMP-сообщение о причине сбоя. Гарантию правильной передачи данных предоставляют протоколы вышестоящего уровня (например, протокол TCP), которые имеют для этого необходимые механизмы.

Одна из основных задач, решаемых протоколом IP, - маршрутизация пакетов данных, т.е. определение пути следования пакетов от одного узла сети к другому на основании адреса получателя.

IP-адреса используются для идентификации устройств в сети. Для взаимодействия с другими устройствами по сети IP-адрес должен быть назначен каждому сетевому устройству (в том числе компьютерам, серверам, маршрутизаторам, принтерам и т.д.). Такие устройства в сети называют хостами.

Адреса IPv4 делятся на пять классов, предназначенных для дифференциации сегментов доступного адресного пространства IPv4. Однако такой способ деления адресного пространства имеет недостатки, связанные с нехваткой адресов для сетей некоторых классов. В соответствии со спецификацией стандарта RFC1519 разработана система бесклассовой адресации CIDR (Classless Inter-Domain Routing) в качестве альтернативы традиционным подсетям. CIDR использует методы деления на подсети переменных размеров.

IP-адрес версии протокола IPv4 состоит из четырех частей, записанных в виде десятичных чисел с точками (например, 192.168.1.1). Каждую из этих четырех частей называют октетом. Октет представляет собой восемь двоичных цифр (например, 11000000, или 192 в десятичном виде).

Таким образом, каждый октет может принимать в двоичном виде значения от 00000000 до 11111111, или от 0 до 255 в десятичном виде.

Часть IP-адреса определена как номер сети (подсети) и идентифицирует сеть (подсеть), а другая часть – номер узла (хоста) сети. Количество двоичных цифр в IP-адресе, которые приходятся на номер сети, и количество цифр в адресе, приходящееся на идентификатор хоста, могут быть различными в зависимости от маски подсети.

Маска сети (подсети). Маска сети (подсети) используется для определения того, какие биты IP-адреса являются частью номера сети, а какие – частью идентификатора хоста.

Маска сети (подсети) всегда состоит из серии последовательных единиц, начиная с самого левого бита маски, за которой следует серия последовательных нулей, составляющих в общей сложности 32 бита

Если бит в маске равен "1", то соответствующий бит IP-адреса является частью номера сети. Если бит в маске равен "0", то соответствующий бит IP-адреса является частью номера узла (хоста). Маску можно определить, как количество бит в адресе, представляющих номер сети (количество бит со значением "1"). Например, "8-битной маской" называют маску, в которой 8 бит – единичные, а остальные 24 бита – нулевые. В этом случае после адреса сети через "/" указывается числовой идентификатор сети (префикс). Например, адрес 192.1.1.0/8 представляет собой адрес 192.1.1.0 с маской 255.0.0.0 (8 единичных бит в маске подсети).

Используя маску, легко найти адрес сети, в которой находится хост с указанным адресом. Для этого достаточно произвести операцию поразрядной конъюнкции (логическое «И»), сложив двоичный IP-адрес хоста с двоичной маской (таблица 1).

Таблица 1 – Пример определения адреса сети

IP-адрес хоста	192	168	1	2
Маска сети	255	255	254	0
IP-адрес (двоичный)	**11000000**	**10101000**	**00000001**	**00000010**
Маска сети (двоичная)	**11111111**	**11111111**	**11111110**	**00000000**
Адрес сети (двоичный)	**11000000**	**10101000**	**00000000**	**00000000**
Адрес сети	192	168	0	0

С помощью маски определяется максимально возможное число хостов в конкретной сети. Помимо этого, она позволяет разделить одну сеть на несколько подсетей.

Определение максимального количества хостов сети. Максимально возможное количество хостов в сети определяется как $\mathbf{2^N-2}$, где $\boldsymbol{N}$ – количество нулей в двоичной маске подсети. Количество хостов конкретной сети на 2 меньше, чем общее количество IP-адресов этой сети. Это связано с тем, что первый адрес из диапазона IP-адресов определён как адрес самой сети, а последний адрес является широковещательным адресом данной сети (broadcasting address). Например, для сети 192.168.0.0/23 адрес сети – 192.168.0.0, широковещательный адрес – 192.168.1.255. Маска сети 23-битная. Это значит, что в двоичной маске 23 бита – «1» и 32-23 = 9 бит – «0». Количество адресов в данной сети 2^9 = 512, количество хостов – 2^9-2 = 510. В таблице 2 приведён пример определения диапазона адресов заданной сети.

Таблица 2 – Пример определения диапазона IP-адресов хостов сети

Адрес сети	192	168	0	0
Адрес сети (двоичный)	11000000	10101000	00000000	00000000
Маска сети (двоичная)	**11111111**	**11111111**	**1111111**0	00000000
Неизменная часть адреса	11000000	10101000	0000000_	
Наименьший адрес из диапазона (адрес сети)	11000000	10101000	0000000**0**	**00000000**
	192	168	0	0
Наибольший адрес из диапазона (broadcasting address)	**11000000**	**10101000**	0000000**1**	**11111111**
	192	168	1	255
Диапазон адресов хостов	192.168.0.1 – 192.168.1.254			

Формирование подсетей. С помощью подсетей одну сеть можно разделить на несколько. Например, чтобы разделить сеть 192.168.1.0/24 на две отдельные подсети, можно "позаимствовать" один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128). В каждой подсети $2^{32-25} = 2^7 = 128$ адресов. Адреса подсетей в этом случае: 192.168.1.0/25 и 192.168.1.128/25.

Адреса подсетей и количество хостов в них можно также определить, разделив число адресов сети на число подсетей. Например, в сети 192.168.1.0/24 $2^{32-24} = 2^8 = 256$ адресов. При делении сети на две подсети количество адресов в каждой подсети 256:2 = 128. Диапазон адресов первой подсети 192.168.1.0 – 192.168.1.127 (192.168.1.0 – адрес сети, 192.168.1.127 – широковещательный адрес), второй подсети - 192.168.1.128 – 192.168.1.255 (192.168.1.128 – адрес сети, 192.168.1.255 – широковещательный адрес). В каждой подсети по 126 хостов.

При делении сети на нечётное число подсетей количество хостов в каждой подсети может быть различным. Например, можно разбить сеть 192.168.1.0/24 на три подсети. В этом случае 256 адресов исходной сети модно поделить так: 1-я подсеть - 128, 2-я подсеть - 64, 3-я подсеть - 64.

Маска первой подсети: $128 = 2^7$ (7 нулевых бита), 32 – 7 = 25 единичных бита, т.е. /25 или 255.255.255.128;

Маска второй и третьей подсетей: $64 = 2^6$ (6 нулевых бита), 32 – 6 = 26 единичных бита, т.е. /26 или 255.255.255.192.

Т.о., 1-я подсеть: 192.168.1.0/25 (128 адресов, 126 хостов), 192.168.1.0 – адрес сети, 192.168.1.127 – широковещательный адрес;

2-я подсеть: 192.168.1.128/26 (64 адреса, 62 хоста), 192.168.1.128 – адрес сети, 192.168.1.191 – широковещательный адрес;

3-я подсеть: 192.168.1.192/26 (64 адреса, 62 хоста), 192.168.1.192– адрес сети, 192.168.1.255 – широковещательный адрес.

Лабораторная работа №1

Построение простых моделей компьютерных сетей в NetEmul

Цель работы: ознакомиться с основами работы с программным эмулятором NetEmul. Научиться строить простые модели ЛВС.

Основные термины и определения:

Концентратор (hub) – сетевое устройство, предназначенное для объединения устройств сети в сегменты. Основной принцип его работы заключается в трансляции пакетов, поступающих на один из его портов на все другие порты. Работает на физическом уровне модели OSI.

Коммутатор (switch) – сетевое устройство, используемое в сетях передачи пакетов, предназначенное для объединения нескольких сегментов. Передает данные от одного порта к другому на основе содержащейся в пакете информации. Работает на канальном уровне модели OSI.

Сетевой порт (application port) - параметр протоколов TCP и UDP, определяющий назначение пакетов данных в формате IP, передаваемых на хост по сети. Это идентифицируемый номером системный ресурс, выделяемый приложению, выполняемому на некотором сетевом хосте, для связи с приложениями, выполняемыми на других сетевых хостах (в том числе с другими приложениями на этом же хосте).

MAC-адрес (от англ. **Media Access Control** — управление доступом к среде, также **Hardware Address**) - это уникальный физический идентификатор сетевого устройства. Установленный производителем аппаратный адрес устройства, присоединённого к сетевой среде, необходимый для системы управления доступом к ней.

IP-адрес (Internet Protocol Address) – уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к сети, построенной по протоколу **IP**. Существует две версии протокола IP: **IPv4** и **IPv6**.

TCP (**Transmission Control Protocol**) – один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях **TCP/IP**. Выполняет функции протокола транспортного уровня модели OSI и стека **TCP/IP**.

UDP (User Datagram Protocol) - это простой, ориентированный на дейтаграммы протокол без организации соединения, предоставляющий быстрое, но необязательно надежное транспортное обслуживание. Выполняет функции протокола транспортного уровня модели OSI и стека **TCP/IP**.

1. Порядок выполнения лабораторной работы

1. Запустить программу NetEmul. Создать новый документ. Для этого в появившемся окне программы в главном меню выбрать Файл→ Новый. Панель устройств станет активной и можно приступать к созданию модели сети.

2. С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

а) Номер группы;

b) ФИО студентов, выполняющих работу;
c) Исходные данные к заданию (адрес сети/маска) из таблицы 1.1 с указанием количества хостов в данной сети (определение маски подсети и количества адресов отразить в отчёте).

Таблица 1.1- Исходные данные к заданию
(выбирается по последней цифре пароля)

№	Адрес сети/маска	№	Адрес сети/маска
1	10.1.5.0/27	9	10.2.2.160/27
2	172.18.8.0/25	10	172.21.11.128/28
3	10.2.7.64/28	11	10.0.1.0/26
4	192.168.1.16/25	12	192.168.0.0/26
5	10.0.9.0/27	13	10.1.3.128/27
6	172.23.22.0/24	14	172.29.30.0/27
7	10.1.4.16/26	15	10.0.7.192/28
8	192.168.31.4/25	16	192.168.0.32/26

1.1. Непосредственное соединение двух компьютеров

1. На рабочее поле эмулятора добавить два компьютера с помощью кнопки «Добавить компьютер» на панели устройств.
2. Соединить добавленные компьютеры. Для этого
   a) нажать кнопку «Создать соединение» на панели устройств;
   b) навести указатель на один из компьютеров;
   c) зажав левую кнопку мыши, провести линию до второго компьютера, после чего отпустить левую кнопку мыши;
   d) в появившемся диалоговом окне настроек интерфейсов подтвердить соединение между интерфейсами eth0, нажав «Соединить» (рис. 1.1);

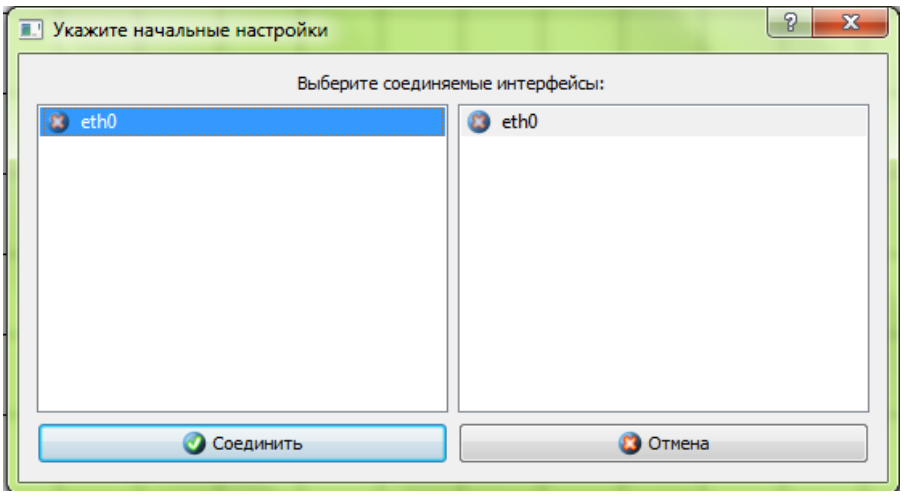

Рисунок 1.1 – Окно соединяемых интерфейсов

e) компьютеры соединены, на каждом конце соединения показан номер используемого интерфейса (в данном случае - 0), а индикатор соединения на иконке компьютера сменил цвет с красного на жёлтый.

Индикатор соединения может иметь три положения:

- красный - устройство не подключено;
- жёлтый - устройство подключено, но не настроено;
- зеленый - устройство подключено, настроено и готово к работе.

3. Настроить компьютеры, задав каждому IP-адрес и маску подсети в соответствии с вариантом. Для этого

a) выбрать «Перемещение объектов» на панели устройств и выделить первый компьютер щелчком левой клавиши мыши;

b) щелчком правой клавиши мыши вызвать контекстное меню и выбрать пункт интерфейсы (рис. 1.2);

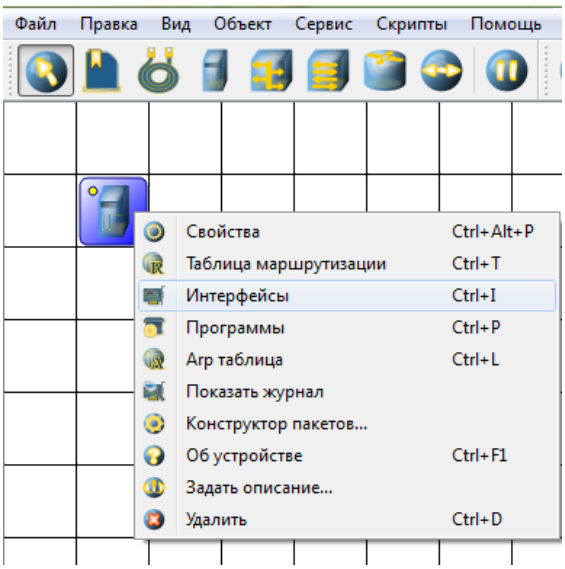

Рисунок 1.2 – Настройка устройства

c) в появившемся окне указать в соответствующих полях IP-адрес и маску подсети, нажать «Применить» и «ОК» (рис. 1.3);

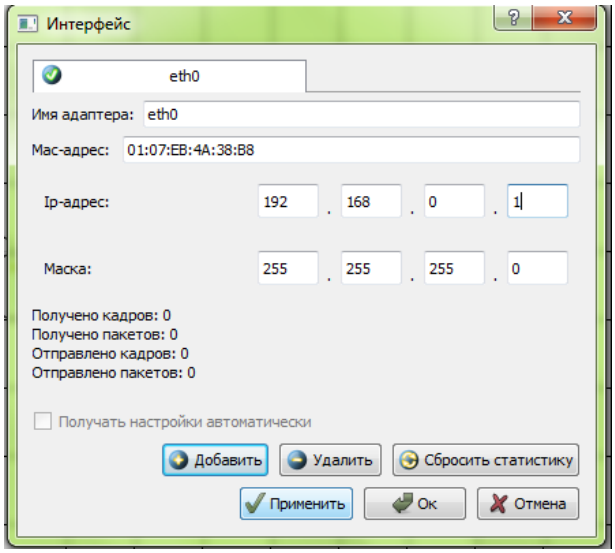

Рисунок 1.3 – Настройка интерфейса устройства

d) при правильных настройках индикатор соединения на иконке компьютера сменит цвет с жёлтого на зелёный;
e) добавить возле каждого компьютера надпись с его IP-адресом и маской подсети как показано на рис. 1.4.

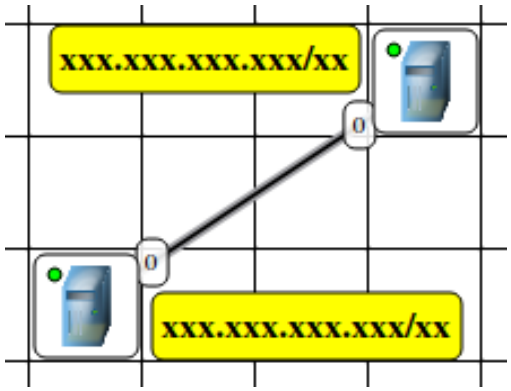

Рисунок 1.4 – Схема модели соединения двух компьютеров

4. Проверить работоспособность построенной модели сети, передав пакеты от одного компьютера до другого. Для этого

a) выбрать «Отправить данные» на панели устройств;
b) под курсором (на рабочем поле программы) должен появиться красный круг;
c) навести курсор с красным кругом на передающий компьютер и нажать левую клавишу мыши;
d) в появившемся окне «Отправка» указать протокол TCP, размер данных 5 КВ (рис. 1.5), нажать «Далее»;

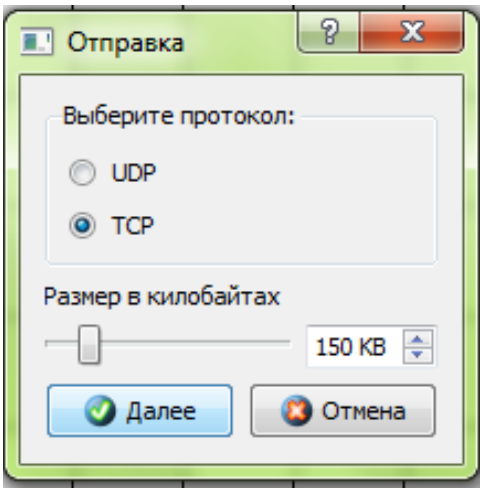

Рисунок 1.5 – Параметры отправки данных

e) навести курсор с зелёным кругом на принимающий компьютер, и нажать левую клавишу мыши;
f) в появившемся окне подтвердить интерфейс на принимающем компьютере eth0, нажав «Отправка» (рис. 1.6);

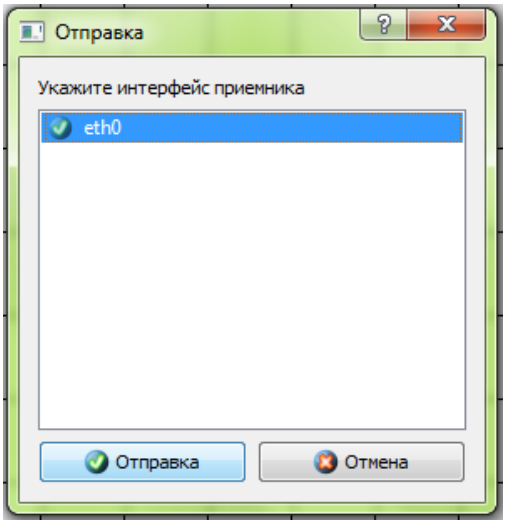

Рисунок 1.6 – Указание принимающего интерфейса

g) проследить за перемещением пакетов;
h) продемонстрировать преподавателю работоспособность построенной модели;
i) просмотреть статистику переданных и полученных компьютерами пакетов в окне «Интерфейсы», проанализировать данные журналов устройств (выбрать «Перемещение объектов», выделить устройство, на панели инструментов нажать на «показать журнал устройства»).

5. В отчёт занести схему сети, указать настройки устройств, настройки соединения, статистику по пакетам. Сделать вывод.

6. Сохранить документ под именем Сеть_1.1. Для этого на сетевом диске в папке МОМСС найти папку своей группы и создать в ней папку с именем: первые буквы фамилий студентов бригады, группа (например, для Иванова и Петрова из группы А-1 папка имеет имя ИП А-1).

1.2. Построение локальной сети на концентраторах

1. Выбрать исходные данные для выполнения работы согласно варианту.

2. Добавить на рабочее поле эмулятора 6 компьютеров и 3 концентратора согласно схеме рис. 1.7.

Соединить устройства.

Настроить компьютеры и добавить возле каждого компьютера надпись с его IP-адресом и маской подсети.

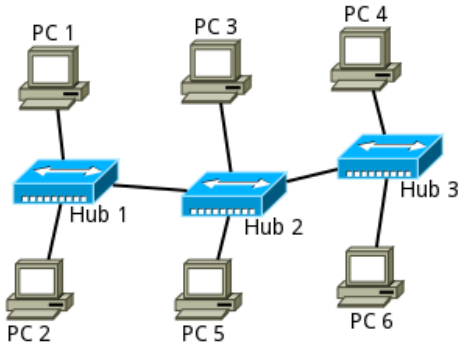

Рисунок 1.7 – Схема модели сети на основе концентраторов

3. Проверить работоспособность построенной модели сети, передав пакеты (TCP, 5 KB) от одного компьютера к другому. Проследить за перемещением пакетов и сделать выводы об особенностях работы локальной сети на основе концентраторов.

4. Продемонстрировать преподавателю работоспособность построенной модели.

5. Сохранить документ под именем Сеть_1.2.

1.3. Построение локальной сети на коммутаторах

1. Выбрать исходные данные для выполнения работы согласно варианту.

2. На рабочем поле эмулятора построить модель сети в соответствии со схемой рис. 1.8.

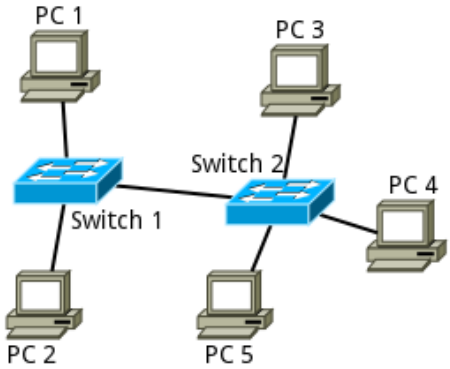

Рисунок 1.8 - Схема модели сети на основе коммутаторов

3. Настроить компьютеры и добавить возле каждого компьютера надпись с его IP-адресом и маской сети.

4. Проверить работоспособность построенной модели сети, передав пакеты (TCP, 5 KB) от одного компьютера к другому. Проследить за перемещением пакетов и сделать выводы об особенностях работы локальной сети на основе коммутаторов.

5.Продемонстрировать преподавателю работоспособность построенной модели.

6. Сохранить документ под именем Сеть_1.3.

2. Контрольные вопросы

1. Уровни эталонной модели OSI, их функции.

2. Перечислить виды сетевой адресации. Пояснить структуру каждого вида сетевых адресов.

3. Что такое сетевой интерфейс?

4. Как работает концентратор?

5. Как работает коммутатор?

6. Топологии локальных сетей.

7. Принцип работы протокола TCP.

Лабораторная работа №2

Объединение нескольких сетей. Маршрутизация.

Цель работы: Познакомиться с основными принципами маршрутизации. Научиться формировать статические маршруты, прописывать их в таблицы маршрутизации сетевых устройств.

Основные термины и определения:

Маршрутизатор (router) – сетевое устройство, которое на основании информации о топологии сети и определённых правил принимает решения о пересылке пакетов между различными сегментами сети. Использует адрес получателя, указанный в пакетах данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Работает на сетевом уровне модели OSI.

Таблица маршрутизации – таблица, состоящая из сетевых маршрутов и предназначенная для определения наилучшего пути передачи сетевого пакета. Описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора.

Сетевой шлюз (gateway) – это точка сети, которая служит выходом в другую сеть. Сетевой шлюз может быть аппаратным или программным решением, или и тем, и другим, но обычно это программное обеспечение, установленное на маршрутизаторе или компьютере.

В пределах сети или подсети хосты связываются друг с другом без потребности в каком-либо промежуточном устройстве. Когда хост должен связаться с другой сетью, посредническое устройство действует как шлюз к другой сети. Адрес шлюза фактически представляет собой IP-адрес интерфейса устройства (например, роутера), с помощью которого осуществляется подключение компьютера локальной сети к внешней сети.

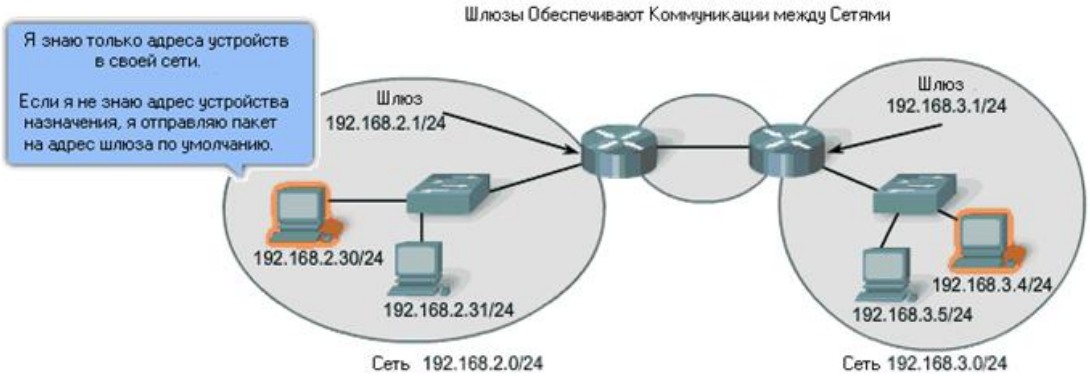

Рисунок 2.1 – Сетевой шлюз

Как показано на рисунке 2.1, адрес шлюза является адресом интерфейса маршрутизатора, который соединяется с той же самой сетью, что и сам хост. Чтобы связаться с устройством в другой сети, хост использует адрес этого шлюза, или шлюза по умолчанию, для передачи пакета за пределы локальной сети.

Маршрутизатор также нуждается в маршруте, который определяет, куда далее передать пакет. Его называют адресом следующего хопа. Если этот

маршрут будет доступен маршрутизатору, то маршрутизатор передаст пакет к следующему хопу - маршрутизатору, который предлагает путь к целевой сети.

ARP (Address Resolution Protocol) – протокол сетевого уровня, предназначенный для определения MAC-адреса по известному IP-адресу. Для определения MAC-адреса получателя по IP-адресу хост формирует широковещательный Ethernet-кадр, содержащий ARP-запрос (ARP-Request). Запрос содержит MAC и IP отправителя и IP получателя. Хост, обнаруживший свой IP в поле "сетевой адрес получателя", дописывает свой MAC-адрес и отправляет ARP-ответ (ARP-Reply). Получив искомый MAC-адрес, хост заносит его в ARP-кэш.

TCP (**Transmission Control Protocol**) – один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях **TCP/IP**. Выполняет функции протокола транспортного уровня модели OSI и стека **TCP/IP**.

UDP (User Datagram Protocol) - это простой, ориентированный на дейтаграммы протокол без организации соединения, предоставляющий быстрое, но необязательно надежное транспортное обслуживание. Выполняет функции протокола транспортного уровня модели OSI и стека **TCP/IP**.

1. Порядок выполнения лабораторной работы

1. Запустить программу NetEmul. Создать новый документ. Для этого в появившемся окне программы в главном меню выбрать Файл → Новый. Панель устройств станет активной и можно приступать к созданию модели сети.

2. С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

d) Номер группы;

e) ФИО студентов, выполняющих работу.

1.1. Объединение подсетей в единую сеть

Задание 1. Локальная сеть состоит из двух подсетей. Адрес сети выбирается в соответствии с вариантом (таблица 2.1).

Таблица 2.1 - Варианты адресации сетей
(выбирается по последней цифре пароля)

№	Адрес сети/маска	№	Адрес сети/маска
1	10.73.0.0/23	**9**	172.24.34.0/23
2	192.168.74.0/23	**10**	10.82.0.0/23
3	172.25.34.0/23	**11**	192.168.8.0/23
4	10.76.0.0/23	**12**	172.24.48.0/23
5	10.77.0.0/23	**13**	10.10.85.0/23
6	192.168.78.0/23	**14**	192.168.6.0/23
7	10.79.1.0/23	**15**	10.93.0.0/23
8	10.10.80.0/23	**16**	192.168.95.0/23

Требуется:

1. Определить адреса подсетей, маску и количество хостов каждой подсети;
2. Построить модель сети, настроить устройства;
3. Организовать передачу данных между хостами различных подсетей;
4. В отчёт занести схему сети, указать настройки устройств, настройки соединения, статистику по пакетам. Сделать вывод.
5. Сохранить документ под именем Сеть_2.1 в папке своей бригады, находящейся на сетевом диске в папке группы каталога МОМСС.

Указания по выполнению

a) В рабочем окне эмулятора построить модель сети в соответствии со схемой рис. 2.2. Хосты PC1-4 относятся к первой подсети, а хосты PC5, 6 – ко второй подсети.

b) Настроить интерфейсы хостов.

c) Попытаться организовать передачу пакетов (например, TCP, 5 KB) между компьютерами одной подсети, затем между компьютерами различных подсетей (например, между PC1 и PC6). Сделать выводы.

d) Настроить маршрутизацию компьютера PC 1, передающего данные хосту PC 6. Для этого вызвать двойным щелчком левой клавиши мыши меню Свойства, указать адрес шлюза, включить маршрутизацию.

e) Организовать передачу TCP-пакетов (10 KB), затем организовать передачу UDP-пакетов (10 KB). Проследить за перемещением пакетов. Сделать выводы. В отчёт занести содержимое журналов устройств. Продемонстрировать результат преподавателю.

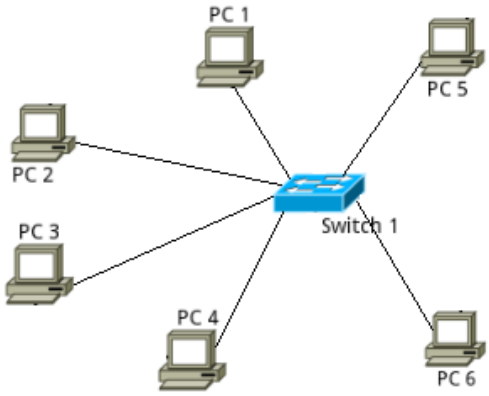

Рисунок 2.2 – Схема локальной сети

Задание 2. Построить модель сети, состоящей из трёх подсетей (IP-адрес сети: 192.168.0.0/22). В сеть входят два коммутатора и 6 компьютеров. Продемонстрировать работоспособность сети, организовав передачу данных между любой парой хостов различных подсетей заданной сети. В отчёт занести схему сети, настройки устройств, настройки соединения, статистику по пакетам.

Сохранить документ под именем Сеть_2.2.

1.2. Объединение сетей маршрутизатором

Задание 1.Построить модель сети, изображённой на рис. 2.3.

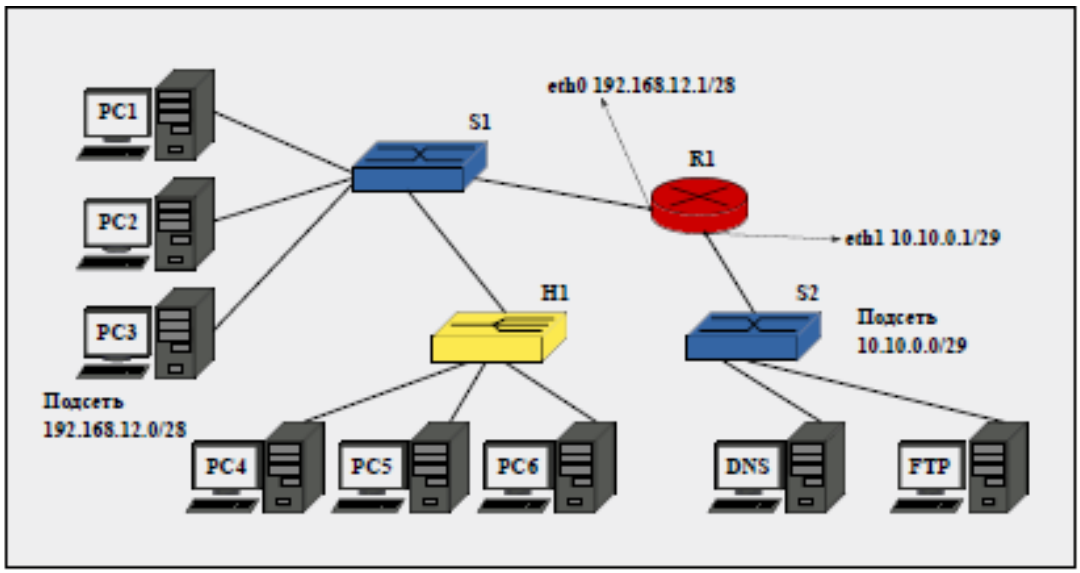

Рисунок 2.3 – Схема сети задания 1 п. 1.2

На рис. 2.3:
R1 – маршрутизатор;
S1, S2 – коммутаторы;
H1 – концентратор.

Маршрутизатор R1 объединяет две сети 192.168.12.0/28 и 10.10.0.0/29. Интерфейс маршрутизатора eth0 имеет IP-адрес 192.168.12.1, а eth1 – 10.10.0.1. Компьютеры PC1-6 находятся в сети 192.168.12.0/28, а DNS и FTP-сервер – в сети 10.10.0.0/29.

При настройке сети на каждом компьютере необходимо прописать IP-адрес шлюза, включить маршрутизацию на маршрутизаторе.

Организовать передачу данных по сети между хостами, принадлежащими различным сетям, по протоколу TCP (2 КВ). Отобразить журналы маршрутизатора, передающего и принимающего компьютеров. Сделать вывод.

Сохранить документ под именем Сеть_2.3.

Задание 2. Построить модель сети, изображённой на рис. 2.4.

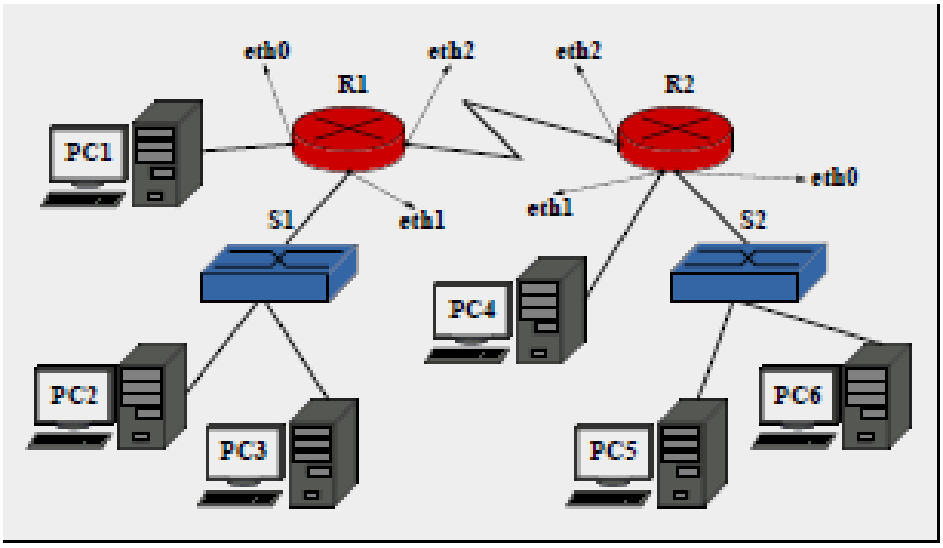

Рисунок 2.4 – Схема сети задания 2 п. 1.2

Хосту PC1 и интерфейсу eth0 маршрутизатора R1 назначить IP-адреса из диапазона 91.122.40.4/30.

Для назначения IP-адресов узлам PC2 и PC3, а также соответствующему порту маршрутизатора R1 (eth1), следует использовать адреса из диапазона Сеть 1 табл. 2.2.

Таблица 2.2 - Варианты адресации сетей (выбирается по последней цифре пароля)

№	Сеть 1	Сеть 2	№	Сеть 1	Сеть 2
1	10.73.0.0/16	172.23.73.0/24	**9**	172.24.34.0/24	10.81.0.0/16
2	192.168.74.0/24	172.18.74.0/24	**10**	10.82.0.0/16	172.24.82.0/24
3	172.25.34.0/24	10.75.0.0/24	**11**	192.168.8.0/24	172.28.83.0/24
4	10.76.0.0/16	172.16.76.0/24	**12**	172.24.48.0/24	10.10.84.0/24
5	10.77.0.0/16	192.168.0.0/16	**13**	10.10.85.0/24	192.168.85.0/24
6	192.168.78.0/24	172.18.78.0/24	**14**	192.168.6.0/24	172.26.86.0/24
7	10.79.1.0/24	172.17.19.0/24	**15**	10.93.0.0/16	172.23.93.0/24
8	10.10.80.0/24	192.168.80.0/24	**16**	192.168.95.0/24	10.95.0.0/16

Хосту PC4 и соответствующему порту второго маршрутизатора R2 (eth1) необходимо назначить IP-адреса из диапазона 91.122.40.8/30.

Аналогично, для назначения IP-адресов узлам PC5 и PC6, а также соответствующему порту второго маршрутизатора R2 (eth0), следует использовать адреса из диапазона Сеть 2 табл. 2.2.

Интерфейсу eth2 первого маршрутизатора (R1), а также интерфейсу eth2 второго маршрутизатора (R2) необходимо назначить IP-адреса из диапазона 91.122.40.0/30.

Установить правила статической маршрутизации для всех непосредственно подключенных и удаленных сетей на маршрутизаторах R1 и R2, а также указать адрес шлюза на каждом компьютере.

Узлам PC2 и PC3 должны быть доступны узлы PC5 и PC6. А узлу PC1 должен быть доступен узел PC4.

Проверить работоспособность сети, передав пакеты (TCP, 2 КВ) между удалёнными друг от друга сетями. Отметить узел отправителя, узел получателя, а также узлы, участвующие в рассылке. Отобразить журналы (отправителя, получателя, маршрутизаторов). Сделать выводы об особенностях работы локальной сети на основе маршрутизаторов.

Продемонстрировать преподавателю работоспособность построенной модели.

Сохранить документ под именем Сеть_2.4.

2. Контрольные вопросы

В отчёте лабораторной работы должны содержаться ответы на контрольные вопросы:

1. Как работает маршрутизатор?

2. Статическая и динамическая маршрутизация. Достоинства и недостатки. Основные протоколы динамической маршрутизации. Механизм работы.

3. Что такое шлюз? Какую функцию он выполняет?

4. Функция трансляции сетевых адресов в маршрутизаторе.

5. Принципы организации передачи по протоколу UDP.

Лабораторная работа №3

Протокол ARP. Получение сетевых настроек по DHCP.

Цель работы: Ознакомиться с механизмом работы протокола ARP.

Основные термины и определения:

ARP (Address Resolution Protocol) – протокол сетевого уровня, предназначенный для определения MAC-адреса по известному IP-адресу. В семействе протоколов IPv6 протокола ARP не существует, его функции возложены на ICMPv6.

ICMP (**Internet Control Message Protocol**) – это механизм сообщения об ошибках. Обеспечивает маршрутизаторам, обнаруживающим ошибки, способ сообщения об ошибке первоначальному источнику. Выполняет следующие основные функции: обмен тестовыми сообщениями для выяснения наличия и активности узлов сети; анализ достижимости узлов и сброс пакетов, направленных к недостижимым узлам; изменение маршрутов (Redirect); уничтожение пакетов с истекшим временем жизни (Time-To-Live); синхронизация времени в узлах сети; управление трафиком (регулирование частоты отправки пакетов).

Ethernet - технология передачи данных локальных компьютерных сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI.

DHCP (Dynamic Host Configuration Protocol) — протокол динамической настройки узла**) -** технология, предназначенная для автоматического присвоения IP-адресов сетевым устройствам.

Краткие теоретические сведения:

ARP протокол получил широкое распространение благодаря повсеместности IP-сетей, построенных поверх Ethernet. Описание протокола ARP опубликовано в RFC 826.

Существуют следующие типы сообщений ARP: ARP-запрос (ARP-request) и ARP-ответ (ARP-reply).

Принцип работы протокола: узел A, которому нужно выполнить отображение IP-адреса на MAC-адрес узла B, формирует ARP-запрос, вкладывает его в кадр канального уровня, указывая в нём известный IP-адрес (узел B), и рассылает запрос широковещательно (в поле MAC-адрес назначения заголовка Ethernet указывается широковещательный MAC-адрес FF:FF:FF:FF:FF:FF). Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел B формирует ARP-ответ, в котором указывает свой IP-адрес и свой MAC-адрес, и отправляет его непосредственно узлу A.

При получении ARP-ответа узел A записывает в кэш ARP-запись соответствия IP-адреса и MAC-адреса узла B. Время хранения записи ограничено. По истечении времени хранения узел A отправляет повторный запрос, но уже адресно. Если ответ не получен, то снова посылается широковещательный запрос.

На рис. 3.1 показана структура кадра ARP с учётом заголовка Ethernet.

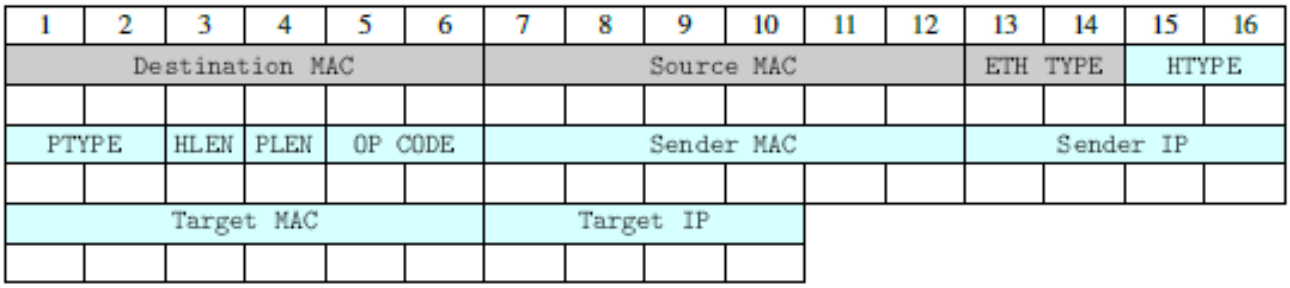

Рисунок 3.1 – Кадр протокола ARP

Значения полей заголовка кадра ARP приведены в таблице 3.1 ниже.

Таблица 3.1 – Значения полей заголовка кадра ARP

Поле	Значение
HTYPE	Номер протокола передачи канального уровня (0x0001 для протокола Ethernet)
PTYPE	Код протокола сетевого уровня (0x0800 для протокола IPv4)
HLEN	Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт
PLEN	Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта
OP CODE	Код операции: 0x01 в случае ARP-запроса и 0x02 в случае ARP-ответа
Sender MAC	Физический адрес отправителя
Sender IP	Сетевой адрес отправителя
Target MAC	Физический адрес получателя. При запросе поле заполняется нулями
Target IP	Сетевой адрес получателя

Самопроизвольный ARP (**gratuitous ARP**) — такое поведение ARP, когда ARP-ответ присылается в том случае, если в этом (с точки зрения получателя) нет особой необходимости, без запроса. Он применяется для определения конфликтов IP-адресов в сети: как только станция получает IP-адрес (статический или динамический), рассылается самопроизвольный ARP-ответ.

Самопроизвольный ARP может быть полезен в следующих случаях:
- обновление ARP-таблиц;
- информирование коммутаторов;
- извещение о включении сетевого интерфейса.

Сетевая атака ARP-спуфинг. ARP-spoofing основан на использовании самопроизвольного ARP.

Чтобы перехватить сетевые пакеты, которые атакуемый хост (A) отправляет на хост B, атакующий хост (C) формирует ARP-ответ, в котором ставит в соответствие IP-адресу хоста B свой MAC-адрес. Далее этот пакет отправляется на хост A. В том случае, если хост A поддерживает самопроизвольный ARP, он модифицирует собственную ARP-таблицу и помещает туда запись, где вместо настоящего MAC-адреса хоста B стоит MAC-адрес атакующего хоста C. Теперь пакеты, отправляемые хостом A на хост B, будут передаваться хосту C (рис. 3.2).

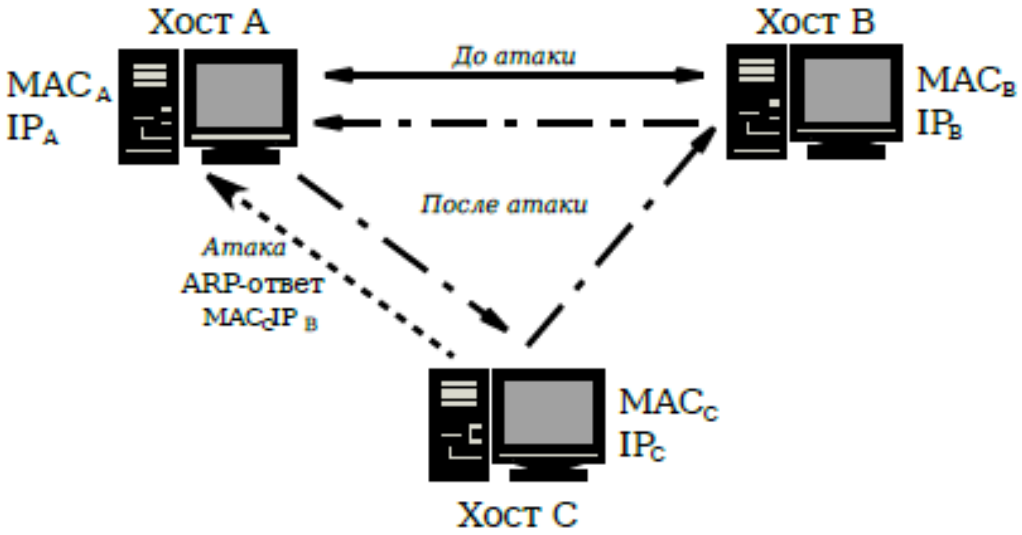

Рисунок 3.2 – Схема ARP-спуфинга

1. Порядок выполнения лабораторной работы

1. Запустить программу NetEmul. Создать новый документ. Для этого в появившемся окне программы в главном меню выбрать Файл → Новый. Панель устройств станет активной и можно приступать к созданию модели сети.

2. С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

f) Номер группы;

g) ФИО студентов, выполняющих работу.

1.1. Изучение работы протокола ARP

Задание 1:

1. Выбрать исходные данные для выполнения работы согласно своему варианту (таблица 3.2). Полученную согласно варианту сеть с маской /27 разбить на две подсети с маской /28 каждая.

Таблица 3.2- Варианты адресации сетей (выбирается по последней цифре пароля)

№	Адрес сети/маска	№	Адрес сети/маска
1	10.0.1.0/27	**9**	10.1.1.64/27
2	10.0.2.32/27	**10**	10.1.2.96/27
3	10.0.3.64/27	**11**	10.1.3.128/27
4	10.0.4.96/27	**12**	10.1.4.160/27
5	10.0.5.128/27	**13**	10.1.5.192/27
6	10.0.6.160/27	**14**	10.1.6.224/27
7	10.0.7.192/27	**15**	10.1.7.0/27
8	10.0.8.224/27	**16**	10.1.8.32/27

2. Построить сеть в соответствии с рис. 3.3.

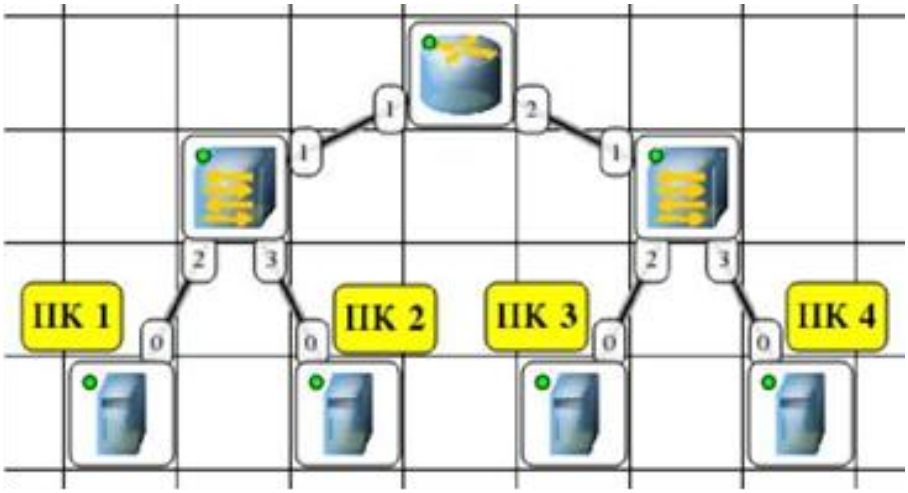

Рисунок 3.3 – Модель сети для изучения протокола ARP

3. Настроить интерфейсы компьютеров и маршрутизаторов, задав каждому IP-адрес и маску подсети (слева — первая подсеть в заданной сети, справа — вторая подсеть). Добавить возле каждого компьютера и интерфейса роутера надписи с их IP-адресом и маской подсети.

4. Проверить работоспособность построенной модели, передав пакеты (UDP, 2 КВ) от компьютера в левой подсети до компьютера в правой подсети.

5.Запустить для компьютеров 1 и 2 журналы пакетов. Очистить ARP-таблицу компьютера 1.

6. Выделить компьютер 1 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-запроса для определения MAC-адреса компьютера 2. Изображение окна настройки пакета сохранить в отчёте.

7. Запустить ARP-запрос, проследить за ним и за сгенерированным для него ARP-ответом по схеме сети и журналам компьютеров 1 и 2.

8.Открыть ARP-таблицу компьютера 1 и убедиться, что запись добавилась в таблицу.

9. Сохранить скриншот экрана (с открытыми журналами) для отчёта.

Задание 2 (Реализация атаки ARP-spoofing):

1. Запустить для компьютеров 1 и 2 журналы пакетов. При необходимости очистить их.

2. Очистить ARP-таблицу компьютера 1.

3. Выделить компьютер 2 и сформировать пакет ARP-ответа, в котором будут указаны

- MAC отправителя — MAC компьютера 2;
- IP отправителя — IP интерфейса роутера в левой подсети;
- MAC получателя — MAC компьютера 1;
- IP получателя — IP компьютера 1.

4. Запустить ARP-ответ, проследить за ним. Может возникнуть окно о дублировании IP-адресов в сети — это происходит в том случае, если из-за действий коммутатора пакет-атаку получает и роутер. Окно быстро закрыть.

5. Сразу же запустить передачу пакетов (UDP, 5 КВ) от компьютера 1 на компьютер 3. Убедиться, что пакеты вначале приходят на компьютер 2 и лишь

потом (если на компьютере 2 включена маршрутизация) отправляются на компьютер 3 (через маршрутизатор).

6. Сохранить скриншот экрана (с открытыми журналами) для отчета. После выполнения работы продемонстрировать преподавателю работоспособность построенной модели. Проект сохранить под именем NET_3.1 в папке своей бригады.

7. Сделать выводы.

1.2. Настройка автоматического получения сетевых настроек по протоколу DHCP

1.Выбрать исходные данные для выполнения работы согласно своему варианту (таблица 3.3). Полученную согласно варианту сеть с маской /26 разбить на 8 подсетей с маской /29 каждая.

Таблица 3.3 Варианты адресации сетей (выбирается по последней цифре пароля)

№	Адрес сети/маска	№	Адрес сети/маска
1	10.0.1.0/26	**9**	10.1.1.128/26
2	10.0.2.64/26	**10**	10.1.2.192/26
3	10.0.3.128/26	**11**	10.1.3.0/26
4	10.0.4.192/26	**12**	10.1.4.64/26
5	10.0.5.0/26	**13**	10.1.5.128/26
6	10.0.6.64/26	**14**	10.1.6.192/26
7	10.0.7.128/26	**15**	10.1.7.0/26
8	10.0.8.192/26	**16**	10.1.8.32/26

2. Построить сеть в соответствии с рис. 3.4.

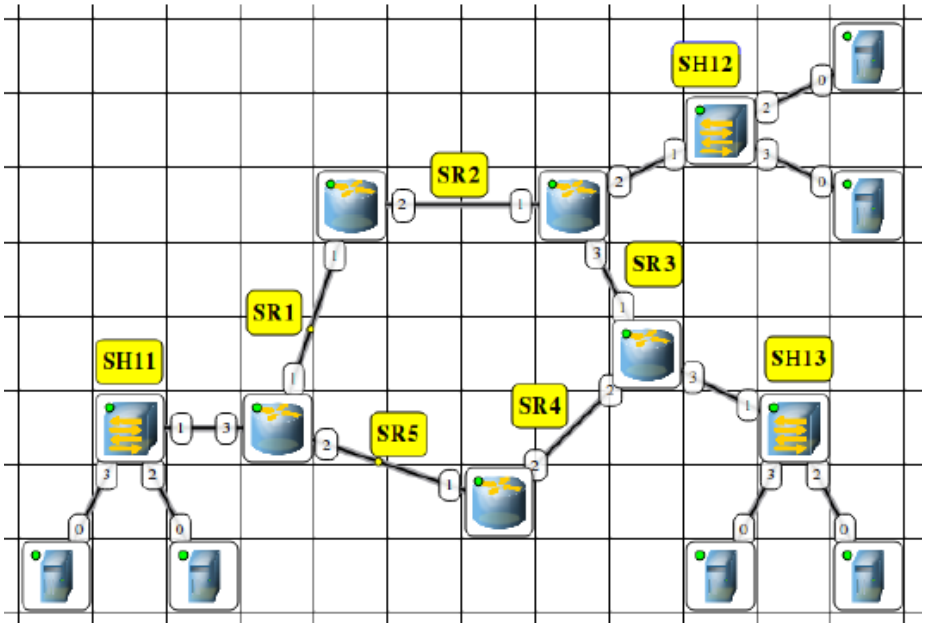

Рисунок 3.4 – Модель сети для изучения работы DHCP

3. Распределить полученные ранее адреса сетей между сетями SR1- SR5 и SH11-SH13. Добавить возле каждой сети надпись с её IP-адресом.

4. Настроить интерфейсы маршрутизаторов, задав каждому IP-адрес и маску подсети в соответствии с выбранным распределением.

5. На маршрутизаторах, которые отвечают за сети SH11-SH13 добавить и запустить программу DHCP-сервер. Не забудьте поставить флаг для активации программы.

6. В настройках каждого DHCP-сервера указать интерфейс, «смотрящий» в сторону сети SH (для SH12, SH13), тип адресов — динамические, диапазон адресов, выделяемых для динамической адресации, маску подсети и IP-адрес шлюза. Для сети SH11 настроить статическую выдачу IP-адресов.

7. На каждом компьютере добавить и запустить программу DHCP-клиент. Не забудьте поставить флаг для активации программы.

8. В настройках каждого DHCP-клиента укажите интерфейс, который должен автоматически получать сетевые настройки.

9. Открыть диалог настройки интерфейсов каждого компьютера и убедиться, что стоит флаг «Получать настройки автоматически».

10. Дождаться, пока все компьютеры не получат сетевые настройки. Определить, какие IP-адреса получили компьютеры.

11. Проверить работоспособность построенной модели сети, передав пакеты (TCP, 5 КВ) между компьютерами в разных подсетях.

12. После выполнения работы продемонстрировать преподавателю работоспособность построенной модели. Проект сохранить под именем NET_3.2. В отчёте отобразить все окна настроек. Сделать выводы.

Список использованных источников

1. Сетевые технологии. Определение IP-адреса. - URL: http://сетиэвм.рф/index.php/servis/opredelenie-ip-adresa.
2. RFC 1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. – URL: http://www.rfc-base.org/rfc-1519.html.
3. Keenetic Limited. Пример расчета количества хостов и подсетей на основе IP-адреса и маски. - URL: https://help.keenetic.net/hc/ru/articles/213965829.
4. Сетевые технологии и всё, что с ними связано. – URL: http://datanets.ru/setevye-shlyuzy.html.
5. RFC-826 An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. – URL: http://www.rfc-base.org/rfc-826.html.
6. Владимиров С.С. Компьютерные сети передачи данных: лабораторный практикум. – СПб: СПб ГУТ, 2016. – 24 с.
7. Небаев И.А. Компьютерные сети передачи данных: учебное пособие к лабораторным работам. – СПб: СПб ГУТ, 2013. – 43 с.