МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Институт цифровых технологий

Кафедра «Общая информатика»

С.Х. Биджиева
В.П. Рядченко

ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ, СИСТЕМЫ И ТЕЛЕКОММУНИКАЦИИ

Лабораторный практикум
для обучающихся 1 курса по направлению подготовки
09.03.03. Прикладная информатика

Черкесск 2023

УДК 004.7
ББК 32.971.35
Б 59

Рассмотрено на заседании кафедры «Общая информатика»
Протокол № 1 от «02» 09.2022г.
Рекомендовано к изданию редакционно-издательским советом СКГА
Протокол № 24 от «26» 09.2022г.

Рецензенты: Эльканова Л.М. - к. ф-м. н., доцент кафедры «Общая информатика»

Б59 **Биджиева, С.Х.** Вычислительные сети, системы и телекоммуникации: лабораторный практикум для обучающихся 1 курса по направлению подготовки 09.03.03. Прикладная информатика / С.Х Биджиева, В.П. Рядченко. – Черкесск: БИЦ СКГА, 2023.-72с.

В лабораторном практикуме представлен материал для освоения обучающимися дисциплины «Вычислительные сети, системы и телекоммуникации». Практикум состоит из двух частей: в теоретической части представлена теоретическая информация; практическая часть включает задания, направленные на закрепление и расширение знаний студентов в области вычислительных сетей, систем и телекоммуникаций

УДК 004.7
ББК 32.971.35

ВВЕДЕНИЕ

Данный лабораторный практикум предназначен для обучающихся по направлению подготовки 09.03.03. Прикладная информатика. Лабораторный практикум составлен на основе рабочей программы по дисциплине «Вычислительные сети, системы и телекоммуникации», в соответствии с требованиями Государственного образовательного стандарта к минимуму содержания и уровню подготовки выпускника по дисциплине.

Цель освоения дисциплины «Вычислительные системы, сети и телекоммуникации»: сформировать способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Задачи дисциплины:

– сформировать знания в области современных информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры

– сформировать навыки использования методов поиска и анализа информации для подготовки документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности

– сформировать способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1-2

Преобразование десятичных чисел в двоичные и двоичных в десятичные. Классификация способов сетевой адресации

Цель работы: изучить понятие протокола, IP-адреса, приобретение навыков вычисления подсетей.

Методические указания

IP-адрес – это уникальный числовой адрес, однозначно идентифицирующий узел, группу узлов или сеть. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел (так называемых «октетов»), разделенных точками, каждое из которых может принимать значения в диапазоне от 0 до 255, например, 128.10.2.30 - традиционная десятичная форма представления адреса, 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

IP-адрес 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.

На следующем рисунке показан пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

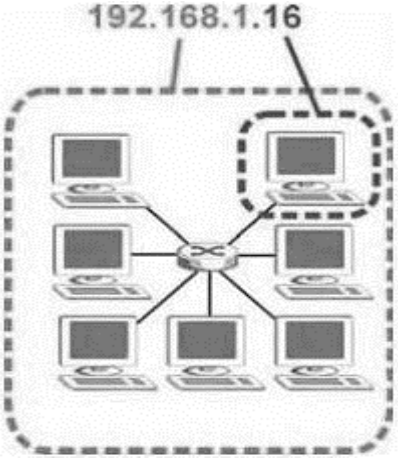


Рисунок 1.1- Номер сети и идентификатор хоста

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 подсети используется для определения того, какие биты являются частью номера сети, а какие – частью идентификатора хоста (для этого применяется логическая операция конъюнкции – "И"). Маска подсети включает в себя 32 бита. Если бит в маске подсети равен "1", то соответствующий бит IP-адреса является частью номера сети. Если бит в маске подсети равен "0", то соответствующий бит IP-адреса является частью идентификатора хоста.

Таблица 1.1. –Пример выделения номера сети и идентификатора хоста в IP-адресе

	1-ый октет: (192)	**2-ой октет: (168)**	**3-ий октет: (1)**	**4-ый октет: (2)**
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	**11111111**	**11111111**	**11111111**	00000000
Номер сети	**11000000**	**10101000**	**00000001**	
Идентификатор хоста				00000010

Маску подсети 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. Маски подсети записываются в формате десятичных чисел с точками, как и IP-адреса. В следующих примерах показаны двоичная и десятичная запись 8-битной, 16-битной, 24-битной и 29-битной масок подсети.

Таблица 1.2–Маски подсети

	Двоичная 1-ый октет:	**Двоичная 2-ой октет:**	**Двоичная 3-ий октет:**	**Двоичная 4-ый октет:**	**Десятичная**
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Количество разрядов в номере сети определяет максимальное количество хостов, которые могут находиться в такой сети. Чем больше бит в номере сети, тем меньше бит остается на идентификатор хоста в адресе. IP-адрес с идентификатором хоста из всех нулей представляет собой IP-адрес сети (192.168.1.0 с 24-битной маской подсети, например). IP-адрес с идентификатором хоста из всех единиц представляет собой широковещательный адрес данной сети (192.168.1.255 с 24-битной маской подсети, например). Так как такие два IP-адреса не могут использоваться в качестве идентификаторов отдельных хостов, максимально возможное количество хостов в сети вычисляется как в таблице 1.3.

Таблица 1.3-Максимально возможное число хостов

Маска подсети		**Размер идентификатора хоста**		**Максимальное количество хостов**
8 бит	255.0.0.0	24 бит	$2^{24} – 2$	16777214
16 бит	255.255.0.0	16 бит	$2^{16} – 2$	65534
24 бит	255.255.255.0	8 бит	$2^{8} – 2$	254
29 бит	255.255.255.248	3 бит	$2^{3} – 2$	6

Классы сетей

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

– Если адрес начинается с 0, то сеть относят к классу А, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей). В сетях класса А количество узлов должно быть больше 2^{16}, но не превышать 2^{24}.

– Если первые два бита адреса равны 10, то сеть относится к классу В и является сетью средних размеров с числом узлов 2^{8} - 2^{16}. В сетях класса В под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.

– Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 2^{8}. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.

– Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

– Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

– В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

– адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

– форма группового IP-адреса - multicast - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения в отличие от широковещательных называются мультивещательными. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Таблица 1.4

Класс адреса	**Диапазон 1-го октета**	**Маска подсети по умолчанию (в десятичном и двоичном формате)**	**Максимальное количество хостов**
A	**1-127**	**255.0.0.0 11111111.00000000.00000000.00000000 …/8**	**2^{24} – 2 =16777214**
B	**128-191**	**255.255.0.0 11111111.11111111.00000000.0000000 …/16**	**2^{16} – 2=65534**
C	**192-223**	**255.255.255.0 11111111.11111111.1111111.00000000 …/24**	**2^{8} – 2=254**
D	**224-239**	**Для многоадресной рассылки**	
E	**240-255**	**Зарезервировано**	

Формирование подсетей

С помощью подсетей одну сеть можно разделить на несколько. В приведенном ниже примере администратор сети создает две подсети, чтобы изолировать группу серверов от остальных устройств в целях безопасности. В этом примере сеть компании имеет адрес 192.168.1.0. Первые три октета адреса (192.168.1) представляют собой номер сети, а оставшийся октет – идентификатор хоста, что позволяет использовать в сети максимум $2^8 – 2 =$ 254 хостов.

Сеть компании до ее деления на подсети показана на следующем рисунке.

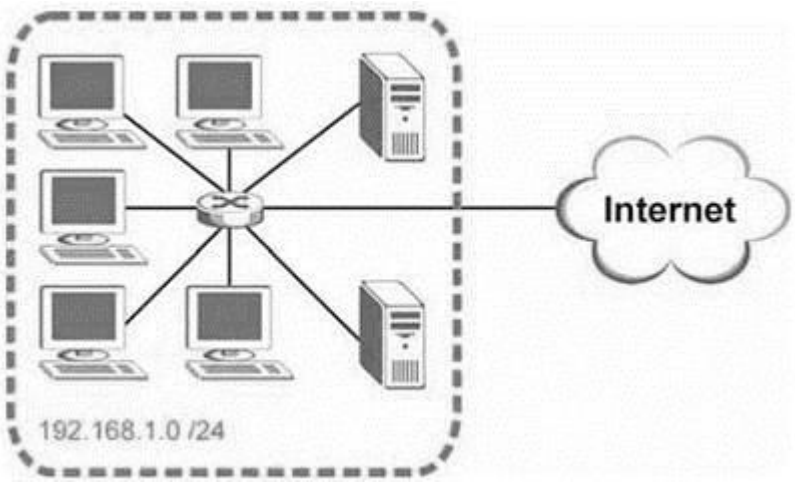


Рисунок 1.2- Пример формирования подсетей: до разделения на подсети

Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, можно "позаимствовать" один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25).

"Одолженный" бит идентификатора хоста может быть либо нулем, либо единицей, что дает нам две подсети: 192.168.1.0 /25 и 192.168.1.128 /25. Сеть компании после ее деления на подсети показана на следующем рисунке. Теперь она включает в себя две подсети, **A** и **B.**

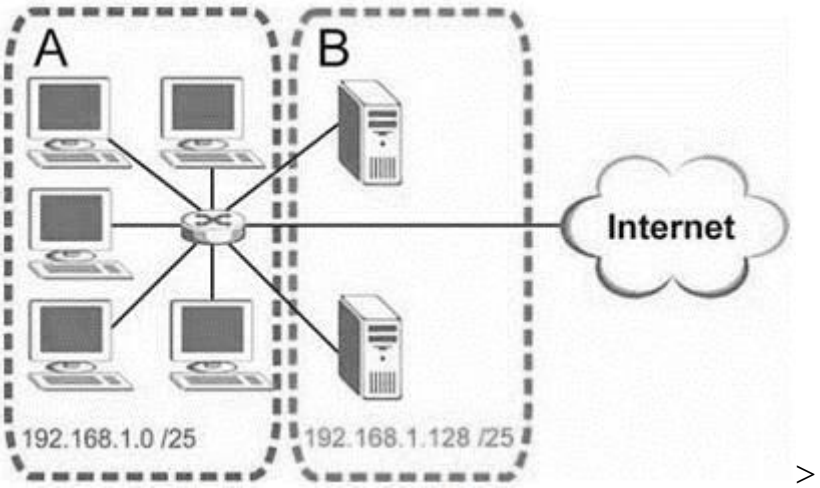


Рисунок 1. 3 - Пример формирования подсетей: после деления на подсети

В 25-битной подсети на идентификатор хоста выделяется 7 бит, поэтому в каждой подсети может быть максимум $2^7 - 2 = 126$ хостов (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети).

Адрес 192.168.1.0 с маской 255.255.255.128 является адресом подсети **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Таким образом, наименьший IP-адрес, который может быть закреплен за действительным хостом в подсети **A** – это 192.168.1.1, а наибольший – 192.168.1.126.

Аналогичным образом диапазон идентификаторов хоста для подсети **B** составляет от 192.168.1.129 до 192.168.1.254.

Ход работы:

При работе с *IP*-адресами возникает необходимость перевода двоичных чисел в десятичные и наоборот. Это можно сделать на *Windows*-калькуляторе. Выполните в *Windows* команду **Пуск-Программы-Стандартные-Калькулятор**, потом **Вид-Программист** (рис.1.4, 1.5).

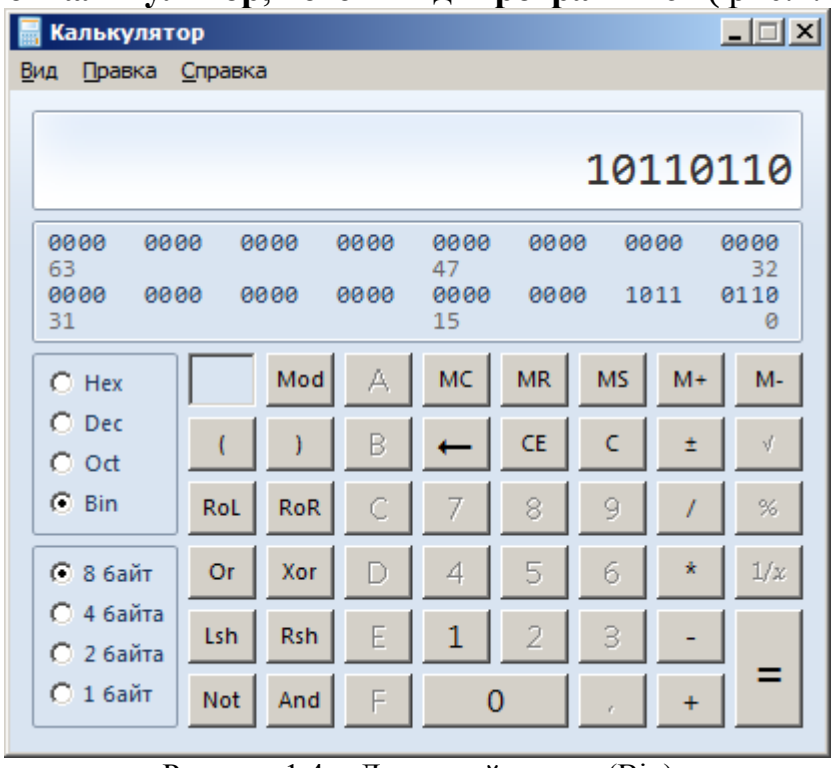


Рисунок 1.4 - Двоичный режим (Bin)

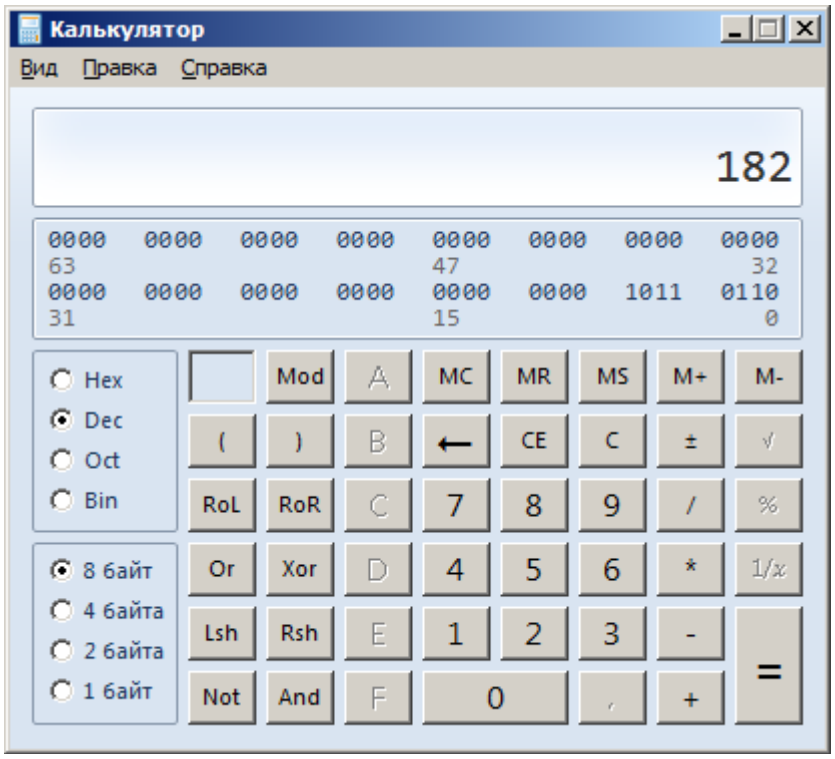


Рисунок 1.5 - Десятичный режим (Dec)

Задание 1. Дополните таблицу 1.5 используя *Windows*-калькулятор.

Таблица 1.5

	Десятичный IP-адрес	**Класс адреса**	**Количество бит в идентификаторе сети**	**Максимальное количество узлов (2П-2)**
10010001.00100000.00111011.00011000	**145.32.59.24**	**Класс B**	**16**	**2^{16}**
11001000.00101010.10000001.00010000	200.42.129.16			
10011001.00100000.00111011.00011000				
11001000.00101010.11000001.00010000				
10110001.00100000.00111011.00011000				
11101000.00101010.10000001.00010000				

Задание 2. На основе примера, разобранного для сетей класса А, заполнить таблицу 1.6 (по варианту – таблица 1.7).

Для выполнения задания 2 необходимо выполнить следующие действия:

а) Перевести каждое число IP-адреса в двоичную форму. Для перевода можно воспользоваться программой «Калькулятор», установив «Вид/Программист».

б) По первым битам IP-адреса определить класс сети.

в) В соответствии с классом определить маску сети по умолчанию.

г) Выписать только те биты IP-адреса, которые соответствуют единичным битам в маске сети. Это будет номер сети.

д) Выписать те биты IP-адреса, которые соответствуют нулевым битам в маске сети. Это будет номер хоста.

е) В двоичном представлении IP-адреса биты, соответствующие номеру хоста, заменить единицами. Представить получившийся адрес в точечной нотации. Это будет широковещательный адрес.

Пример выполнения задания 1.

Пусть IP-адрес 64.10.20.30

Переводим числа в двоичный формат:

$64_{10}=01000000_2$

$10_{10}=00001010_2$

$20_{10}=00010100_2$

$30_{10}=00011110_2$

Записываем двоичную форму представления IP-адреса:

01000000.00001010.00010100.00011110

Первые биты адреса – 01, значит, это сеть класса А.

Маска сети по умолчанию: 255.0.0.0

Записываем в двоичной форме маску сети и IP-адрес:

Маска: 11111111. 00000000.00000000.00000000

IP-адрес: 01000000. 00001010.00010100.00011110

Эти биты соответствуют номеру сети

А эти биты соответствуют номеру хоста

Значит, номер сети - 01000000_2 или 64_{10}

номер хоста - $00001010.00010100.00011110_2$ или $10.20.30_{10}$

Заменяем в IP-адресе номер хоста единицами, получим широковещательный адрес $01000000.111111.111111.111111_2$ или 64.255.255.255

Следовательно:

IP-адрес	64.10.20.30
Класс сети	A
Маска сети	255.0.0.0
Номер сети	64.0.0.0
Номер хоста	0.10.20.30
Широковещательный адрес	64.255.255.255

Число сетей 2^{24}-2

Таблица 1.6

Номер по порядку	Характеристика сети	Класс сети		
		A	B	C
1	2			
	IP-адрес			
	Класс сети			
	Маска сети			
	Номер сети			
	Номер хоста			
	Широковещательный адрес			
	Число сетей 2^7-2			

Варианты индивидуальных заданий 1.

Таблица 1.7

Номер варианта	IP-адрес к заданию 3
	192.168.72.33
	190.172.55.40
	123.232.14.72
	196.232.66.54
	193.123.55.67
	191.172.55.42
	178.66.57.18
	10.0.0.20
	67.192.44.89
	128.34.67.11
	193.34.126.44
	156.32.11.93
	167.168.169.170
	145.44.11.77
	132.45.171.99
	198.164.55.55
	192.77.121.144
	12.13.14.15
	44.57.62.39
	152.15.66.5
	132.45.171.99
	198.164.155. 5
	192.77.11.44
	12.130.140.150

	44.57.162.31
	152.154.66.65
	152.15.66.17
	132.45.171.88

Задание 3.

3.1 Определение количества доступных сетевых адресов

Для сети класса А на основе указанного числа бит сети заполните таблицу 1,8, чтобы определить маску подсети к количество возможных адресов хостов для маски.

Таблица 1.8

Классовый адрес	Десятичная маска подсети	Двоичная маска подсети	Количество хостов для подсети ($2^n - 2$)
/20			
/21			
/22			
/23			
/24			
/25			
/26			
/27			
/28			
/29			
/30			

Задание 4. Определение подсетей на основе другого сетевого адреса

Предположим, что вам выделена сеть 192.168.1.0/24.

1. Сколько бит потребуется позаимствовать для задания 6 подсетей?

2. Укажите классовый адрес и маску подсети в двоичном и десятичном формате, которые позволят создать 6 подсетей.

3. Используйте метод, включающий восемь действий, чтобы задать 6 подсетей (Таблица 1.9).

Таблица 1.9

Действие	**Описание**
1.	Укажите разделяемый октет в двоичном формате.
2.	Укажите маску или длину классового префикса в двоичном формате.
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.
4.	Скопируйте значимые биты четыре раза.
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.
6.	В последней строке укажите широковещательный адрес, поставив 1 в битаххоста.
7.	В средних строках укажите идентификатор первого и последнего хостовподсети.
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсетина единицу. Повторите шаги с 4 по 8 для всех подсетей.

Заполните таблицу 1.10, чтобы задать каждую из подсетей.

Таблица 1.10

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательныйадрес
0			
1			
2			
3			
4			
5			
6			
7			

Вопросы для проверки

1. Дайте определение протокола и IP-адреса

2. Назовите классы IP-адресов.

3. Что такое хост?

4. Как можно определить к какому классу относится IP-адрес?

5. Как определить номер сети и номер узла IP-адреса?

Содержание отчета:

1. Титульный лист.

2. Цель работы.

3. Заполненные таблицы.

Контрольные вопросы:

1. Методика преобразования чисел: из десятичной системы счисления в двоичную, из двоичной системы счисления в десятичную.

2. Преобразование IP адресов из двоичного формата в десятичный.

3. Методика назначения подсетей на основе другого сетевого адреса исетевого адреса с классовым адресом.

ЛАБОРАТОРНАЯ РАБОТА № 3
Сетевые протоколы

Цель работы: Знакомство с программными средствами для тестирования параметров соединения в компьютерных сетях и проверки настройки протокола TCP/IP. Изучение основ работы с утилитами TCP/IP.

Сетевой протокол - набор правил, позволяющий осуществлять *обмен данными* между составляющими *сеть* устройствами, например, между двумя сетевыми картами (рис.3.1).

Рисунок 3.1--Иллюстрация к понятию Сетевой протокол

TCP/IP

Стек протоколов *TCP*/*IP* — это набор протоколов, его название происходит от двух наиболее важных протоколов, являющиеся основой связи в сети *Интернет*. Протокол *TCP* разбивает передаваемую информацию на порции (пакеты) и нумерует их. С помощью протокола *IP* все пакеты передаются получателю. Далее с помощью протокола *TCP* проверяется, все ли пакеты получены. При получении всех порций *TCP* располагает их в нужном порядке и собирает в единое целое. В сети *Интернет* используются две версии этого протокола:

- Маршрутизируемый сетевой протокол IPv4. В протоколе этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 32 бита (т.е. 4 октета или 4 байта).
- IPv6 позволяет адресовать значительно большее количество узлов, чем IPv4. Протокол Интернета версии 6 использует 128-разрядные адреса, и может определить значительно больше адресов.

IP-адреса стандарта IPv6 имеют длину 128 бит и поэтому в четыре раза длиннее, чем IP-адреса четвертой версии. IP-адреса версии v6 записываются в следующем виде: X:X:X:X:X:X:X:X, где X является шестнадцатеричным числом, состоящим из 4-х знаков(16 бит), а каждое число имеет размер 4 бит.

Каждое число располагается в диапазоне от 0 до F. Вот пример IP-адреса шестой версии: 1080:0:0:0:7:800:300C:427A. В подобной записи незначащие нули можно опускать, поэтому фрагмент адреса: 0800: записывается, как 800:.

ARP

Для взаимодействия сетевых устройств друг с другом необходимо, чтобы у передающего устройства был *IP*- и *MAC*-адреса получателя. Набор протоколов *TCP*/*IP* имеет в своем составе специальный протокол, называемый *ARP* (Address *Resolution Protocol* — протокол преобразования адресов), который позволяет автоматически получить *MAC-адрес* по известным *IP*-адресам

DHCP-протокол

Распределением *IP*-адресов для подключения к сети *Интернет* занимаются провайдеры, а в локальных сетях – сисадмины. Назначение *IP*-адресов узлам сети при большом размере сети представляет для администратора очень утомительную процедуру. Поэтому для автоматизации процесса разработан протокол *Dynamic Host Configuration Protocol* (*DHCP*), который освобождает администратора от этих проблем, автоматизируя процесс назначения *IP*-адресов всем узлам сети.

HTTP протокол

HTTP протокол служит для передачи гипертекста, т.е. для пересылки Web-страниц с одного компьютера на другой. Основой *HTTP* является технология "клиент-*сервер*", то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают *запрос*, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

FTP протокол

FTP протокол передачи файлов со специального файлового сервера на *компьютер* пользователя. Установив *связь* с удаленным компьютером, *пользователь* может скопировать *файл* с удаленного компьютера на свой или скопировать *файл* со своего компьютера на удаленный.

POP протокол

POP стандартный протокол получения почтового соединения. Серверы *POP* обрабатывают входящую почту, а протокол *POP* предназначен для обработки запросов на получение почты от клиентских почтовых программ.

SMTP протокол

SMTP-протокол, который задает набор правил для отправки почты. *Сервер SMTP* возвращает либо подтверждение о приеме, либо *сообщение об ошибке*, либо запрашивает дополнительную информацию.

Команды и утилиты ОС Windows10 (cmd).

- **Netstat.** Команда netstat отображает статистику активных подключений TCP, портов, прослушиваемых компьютером, статистики Ethernet, таблицы маршрутизации IP, статистики Ipv4 (для протоколов IP, ICMP, TCP и UDP) и Ipv6 (для протоколов Ipv6, ICMPv6, TCP через Ipv6 и UDP через Ipv6). Запущенная без параметров, команда netstat отображает подключения TCP. (ESTABLISHED- установленный)

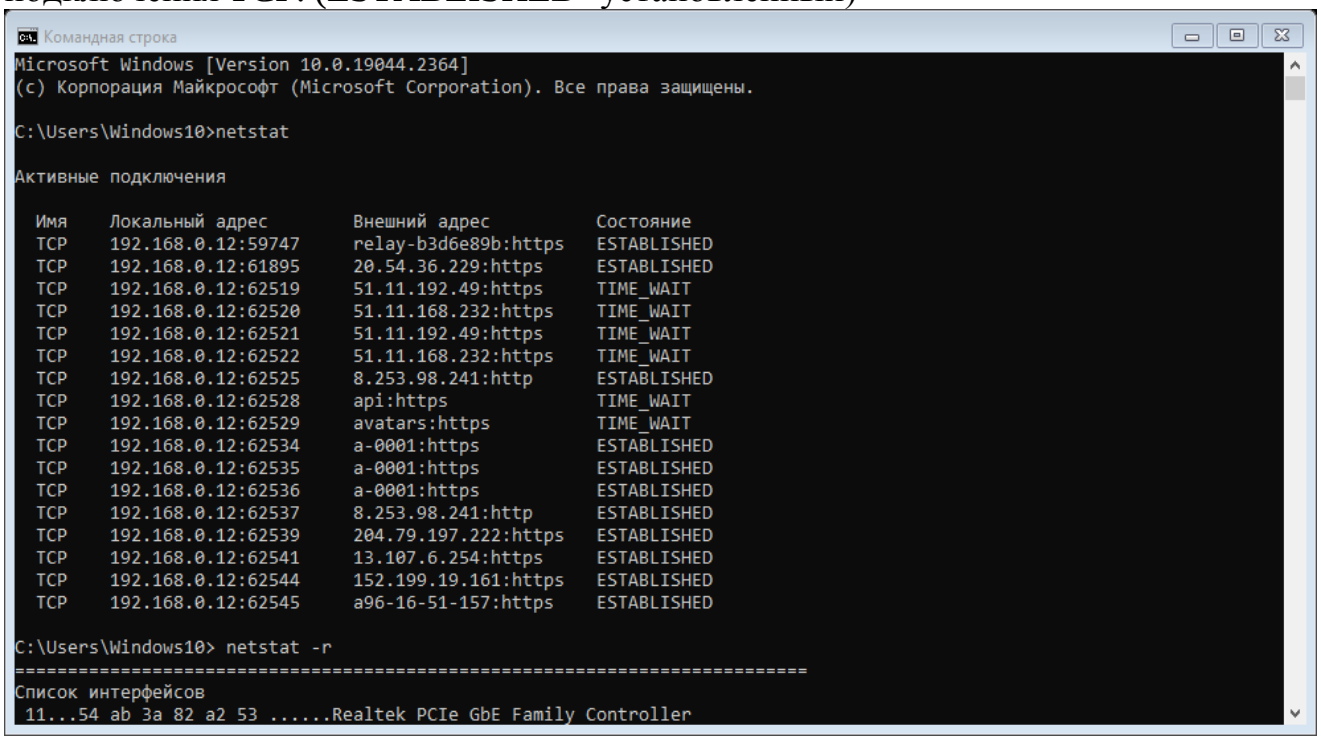


Рисунок 3.2

Формат команды: **netstat [-a] [-e] [-n] [-o] [-p протокол] [-r] [-s] [интервал]**, где:

–a –вывод всех активных подключений TCPи прослушиваемых компьютером портов TCP и UDP.

–e – вывод статистики Ethernet, например, количества отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом

–s.

–n – вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен.

–o – вывод активных подключений TCP и включение кода процесса (PID) для каждого подключения. Код процесса позволяет найти приложение на вкладке Процессы диспетчера задач Windows. Этот параметр может комбинироваться с ключами –a, -n и –p.

–p протокол – вывод подключений для протокола, указанного параметром протокол. В этом случае параметр протокол может принимать значения tcp, udp, tcpv6 или udpv6. Если данный параметр используется с ключом –s для вывода статистики по протоколу, параметр протокол может

иметь значение tcp,udp, icmp, ip, tcpv6, udpv6, icmpv6 или ipv6.

–s – вывод статистики по протоколу. По умолчанию выводится статистикадля протоколов TCP, UDP, ICMP и IP. Если установлен протокол Ipv6 для Windows XP, отображается статистика для протоколов TCP через Ipv6, UDP через Ipv6, ICMPv6 и Ipv6. Параметр –p может использоваться для указания набора протоколов.

–r – вывод содержимого таблицы маршрутизации IP. Эта команда эквивалентна команде route print.

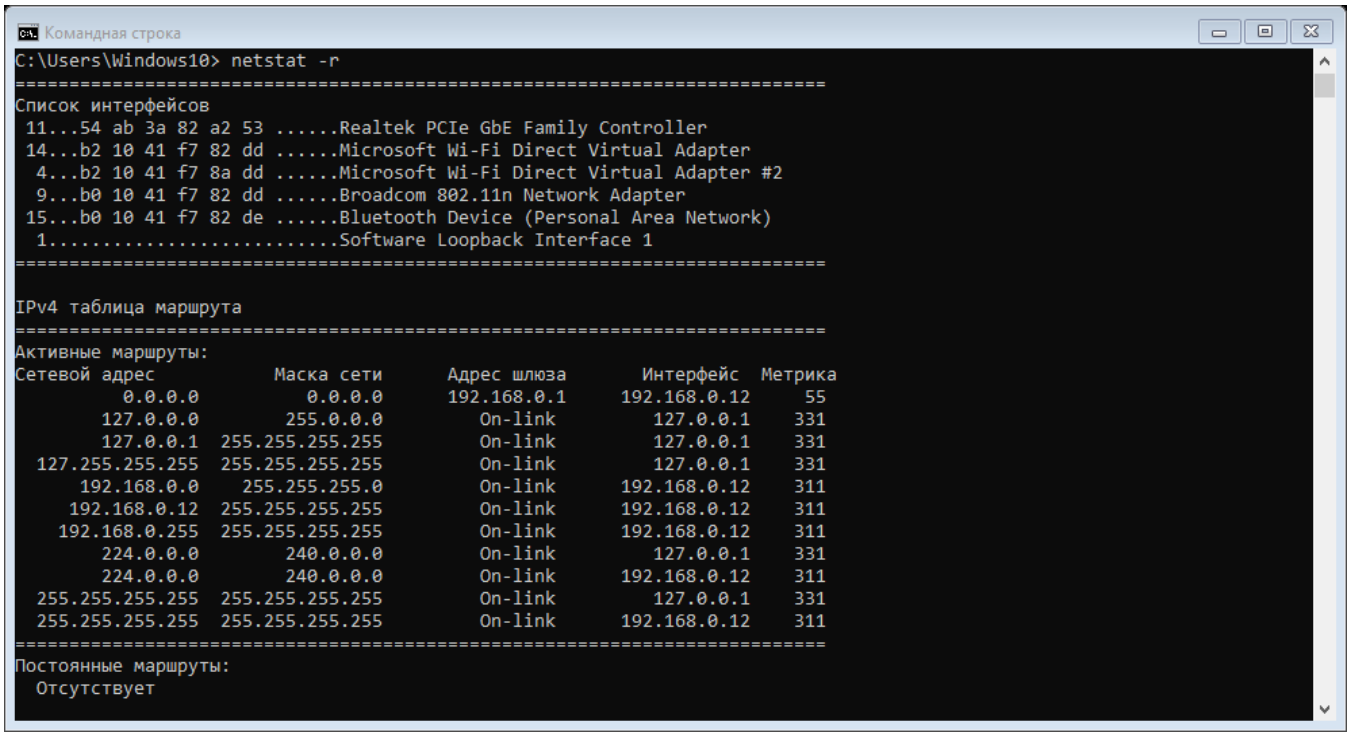


Рисунок 3.3

интервал – обновление выбранных данных с интервалом, определенным параметром интервал (в секундах). Нажатие клавиш CTRL+C останавливает обновление. Если этот параметр пропущен, netstat выводит выбранные данныетолько один раз.

/? – отображение справки в командной строке.

Ping — утилита командной строки для проверки соединений в сетях на основе TCP/IP. Команда PING с помощью отправки сообщений с эхо-запросом по протоколу ICMP проверяет соединение на уровне протокола IP с другим компьютером, поддерживающим TCP/IP. После каждой передачи выводится соответствующее сообщение с эхо-ответом.

Формат команды: **ping [-t] [-a] [-n счетчик] [-l размер] [-f] [-i TTL] [-v тип] [-r счетчик] [-s счетчик] [{-j список_узлов | -k список_узлов}] [-w интервал] [имя_конечного_компьютера]**

-t – Задает для команды ping отправку сообщений с эхо-запросом к точке назначения до тех пор, пока команда не будет прервана. Для прерывания команды и вывода статистики нажмите комбинацию CTRL-BREAK. Для прерывания команды ping и выхода из нее нажмите клавиши CTRL-C.

-a – Задает разрешение обратного имени по IP-адресу назначения. Вслучае успешного выполнения выводится имя соответствующего узла.

-n счетчик – Задает число отправляемых сообщений с эхо-запросом. Поумолчанию — 4.

-l размер – Задает длину (в байтах) поля данных в отправленных сообщениях с эхо-запросом. По умолчанию — 32 байта. Максимальный размер — 65527.

-f – Задает отправку сообщений с эхо-запросом с флагом «Don't Fragment»в IP-заголовке, установленном на 1. Сообщения с эхо-запросом не фрагментируются маршрутизаторами на пути к месту назначения. Этот параметр полезен для устранения проблем, возникающих с максимальным блоком данных для канала (Maximum Transmission Unit).

-i TTL – Задает значение поля TTL в IP-заголовке для отправляемых сообщений с эхо-запросом. По умолчанию берется значение TTL, заданное по умолчанию для узла. Для узлов Windows XP это значение обычно равно 128. Максимальное значение TTL — 255.

-v тип – Задает значение поля типа службы (TOS) в IP-заголовке для отправляемых сообщений с эхо-запросом. По умолчанию это значение равно 0. тип — это десятичное значение от 0 до 255.

-r счетчик – Задает параметр записи маршрута (Record Route) в IP-заголовке для записи пути, по которому проходит сообщение с эхо-запросом и соответствующее ему сообщение с эхо-ответом. Каждый переход в пути использует параметр записи маршрута. По возможности значение счетчика задается равным или большим, чем количество переходов между источником и местом назначения. Параметр счетчик имеет значение от 1 до 9.

-s счетчик – Указывает вариант штампа времени Интернета (Internet Timestamp) в заголовке IP для записи времени прибытия сообщения с эхо-запросом и соответствующего ему сообщения с эхо-ответом для каждого перехода. Параметр счетчик имеет значение от 1 до 4.

-j список_узлов – Указывает для сообщений с эхо-запросом использованиепараметра свободной маршрутизации в IP-заголовке с набором промежуточных точек назначения, указанным в списке_узлов. При свободной маршрутизации последовательные промежуточные точки назначения могут быть разделены одним или несколькими маршрутизаторами. Максимальное число адресов или имен в списке узлов — 9. Список узлов — это набор IP-адресов (в точечно-десятичной нотации), разделенных пробелами.

-k список_узлов – Указывает для сообщений с эхо-запросом использование параметра строгой маршрутизации в IP-заголовке с набором промежуточных точек назначения, указанным в списке_узлов. При строгой маршрутизации следующая промежуточная точка назначения должна быть доступной напрямую (она должна быть соседней в интерфейсе маршрутизатора). Максимальное число адресов или имен в списке узлов равно 9. Список узлов — это набор IP-адресов (в точечно-десятичной нотации), разделенных пробелами.

-w интервал – Определяет в миллисекундах время ожидания получения

сообщения с эхо-ответом, которое соответствует сообщению с эхо-запросом. Если сообщение с эхо-ответом не получено в пределах заданного интервала, то выдается сообщение об ошибке «Request timed out». Интервал по умолчанию равен 4000 (4 секунды).

имя_конечного_компьютера – Задает точку назначения, идентифицированную IP-адресом или именем узла.

Tracert. Команда TRACERT определяет путь до точки назначения с помощью посылки в точку назначения эхо-сообщений протокола Control Message Protocol (ICMP) с постоянным увеличением значений срока жизни (Time to Live, TTL). Выведенный путь — это список ближайших интерфейсов маршрутизаторов, находящихся на пути между узлом источника и точкой назначения. Ближний интерфейс представляют собой интерфейс маршрутизатора, который является ближайшим к узлу отправителя на пути. Запущенная без параметров, команда tracert выводит справку.

Формат команды: **tracert [-d] [-h максимальное_число_переходов] [-j список_узлов] [-w интервал [имя_конечного_компьютера].**

-d – Предотвращает попытки команды tracert разрешения IP-адресов промежуточных маршрутизаторов в имена. Увеличивает скорость вывода результатов команды tracert.

-h максимальное_число_переходов – Задает максимальное количество переходов на пути при поиске конечного объекта. Значение по умолчанию равно 30.

-j список_узов – Указывает для сообщений с эхо-запросом использованиепараметра свободной маршрутизации в заголовке IP с набором промежуточных мест назначения, указанных в списке_узлов. При свободной маршрутизации успешные промежуточные места назначения могут быть разделены одним или несколькими маршрутизаторами. Максимальное число адресов или имен в списке - 9. Список_адресов представляет набор IP-адресов (в точечно-десятичной нотации), разделенных пробелами.

-w интервал – Определяет в миллисекундах время ожидания для получения эхо-ответов протокола ICMP или ICMP-сообщений об истечении времени, соответствующих данному сообщению эхо-запроса. Если сообщение не получено в течение заданного времени, выводится звездочка (*). Таймаут по умолчанию 4000 (4 секунды).

- имя_конечного_компьютера – задает точку назначения, указанную IP-адресом или именем узла.

-? – Отображает справку в командной строке по утилите tracert.

Ход работы

Задание 1. Получить сетевые настройки компьютеров

Для того, чтобы узнать *IP-адрес* необходимо открыть командную строку Windows. Это можно сделать несколькими способами, например: Win + R (откроется окошко «Запуск программы»); в поле ввода вписать: cmd

(откроется консоль); ввести команду: ipconfig или запустить в ОС *Windows* на выполнение команду **Пуск – Программы – Стандартные – Командная Строка** и наберете в ней **ipconfig**(рис.3.4).

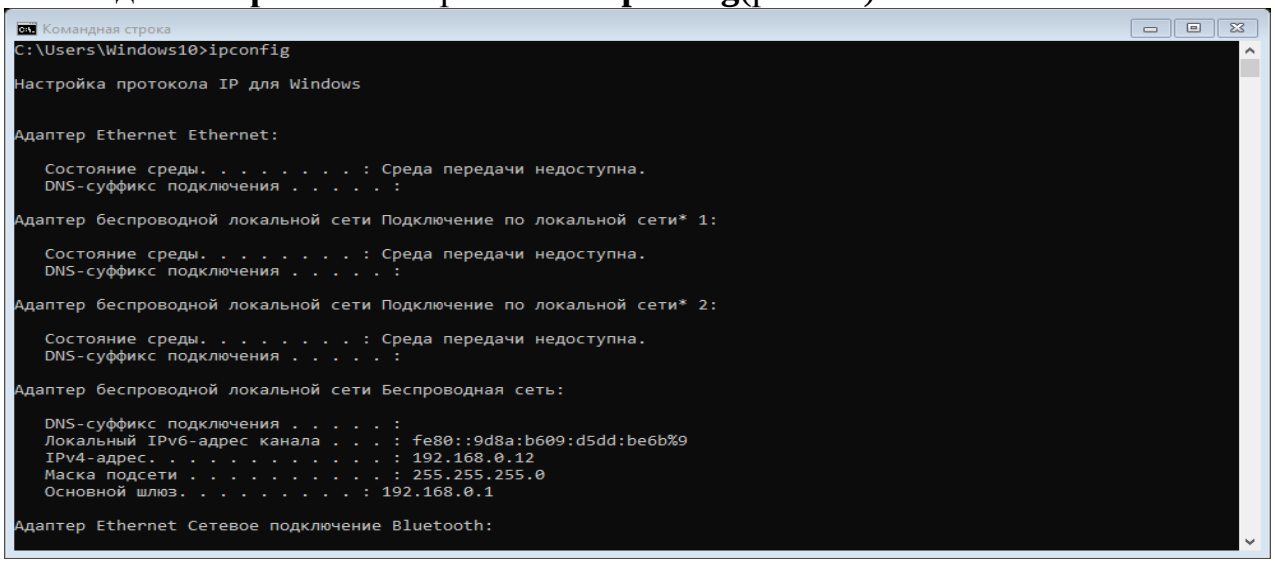


Рисунок 3.4 -IP адрес вашего ПК в десятичной системе счисления

Здесь мы видим IP в двух версиях: IPv4 и IPv6

Ipconfig - Отображает все текущие значения конфигурации сети TCP/IP и обновляет параметры протокола DHCP и системы доменных имен (DNS). При использовании без параметров **ipconfig** отображает IP-адреса версии 4 (IPv4) и IPv6, маску подсети и шлюз по умолчанию для всех адаптеров.

Чтобы отобразить основную конфигурацию TCP/IP для всех адаптеров, необходимо ввести: **ipconfig**

Чтобы отобразить полную конфигурацию TCP/IP для всех адаптеров, необходимо ввести: **ipconfig /all**

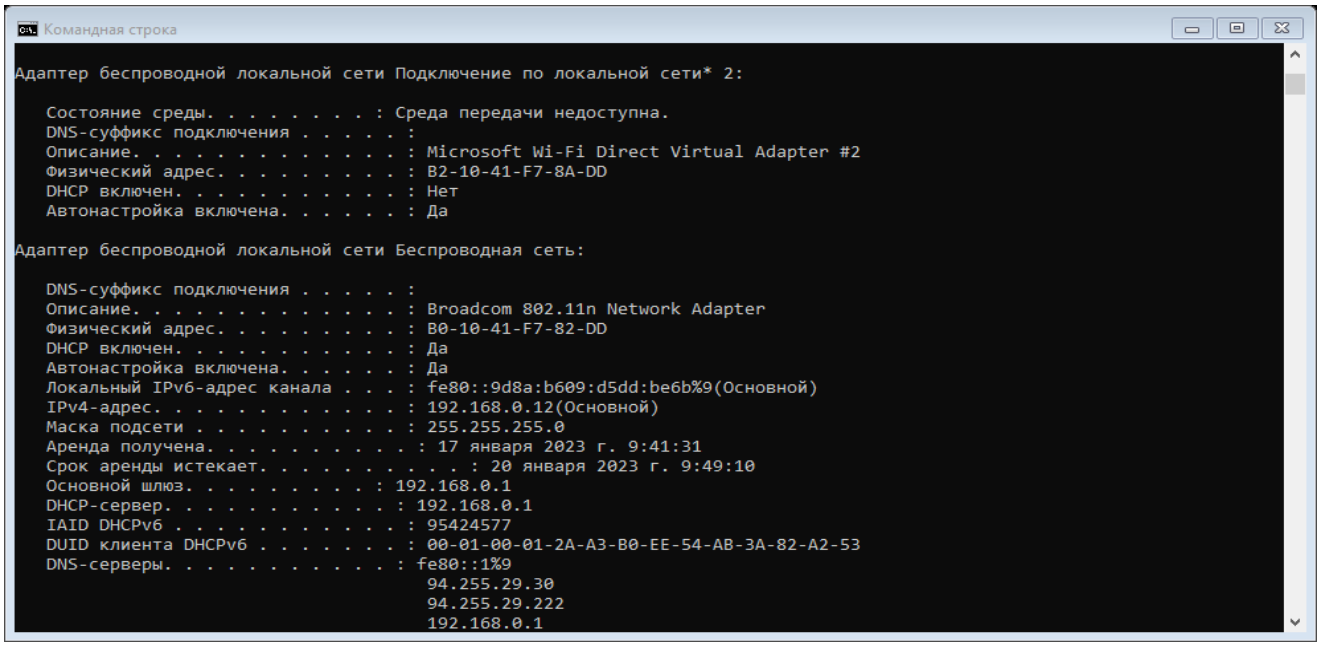


Рисунок 3.5 – Отображение полной конфигурации TCP/IP для всех адаптеров

Чтобы обновить IP-адрес, назначенный DHCP только для адаптера локальной сети, необходимо ввести: **ipconfig /renew**

Чтобы очистить кэш сопоставителя DNS при устранении неполадок с разрешением DNS-имен, необходимо ввести: **ipconfig /flushdns**

Чтобы отобразить идентификатор класса DHCP для всех адаптеров с именами, начинающимися с Local, необходимо ввести: **ipconfig /showclassid Local***

Чтобы задать идентификатор класса DHCP для ПРОВЕРЯЕМого адаптера локальной сети, необходимо ввести: **ipconfig /setclassid Local Area Connection TEST**

Задание 2. Определить MAC-адрес ПК

Помимо IP адреса, есть еще и такое понятие, как MAC- адрес.

MAC-адрес (или аппаратный адрес) - это цифровой код длиной 6 байт, устанавливаемый производителем сетевого адаптера и однозначно идентифицирующий данный адаптер. Согласно стандартам на сеть Ethernet, не может быть двух сетевых адаптеров с одинаковым MAC-адресом. Пример записи MAC-адреса: 00:E0:18:C3:11:89.

Для того, чтобы узнать MAC-адрес сетевой карты в ОС Windows XP нужно выполнить следующие действия: Пуск-Выполнить-cmd и нажимаем ОК;

В командной строке набираем ipconfig /all и нажимаем Enter (рис.3.6).

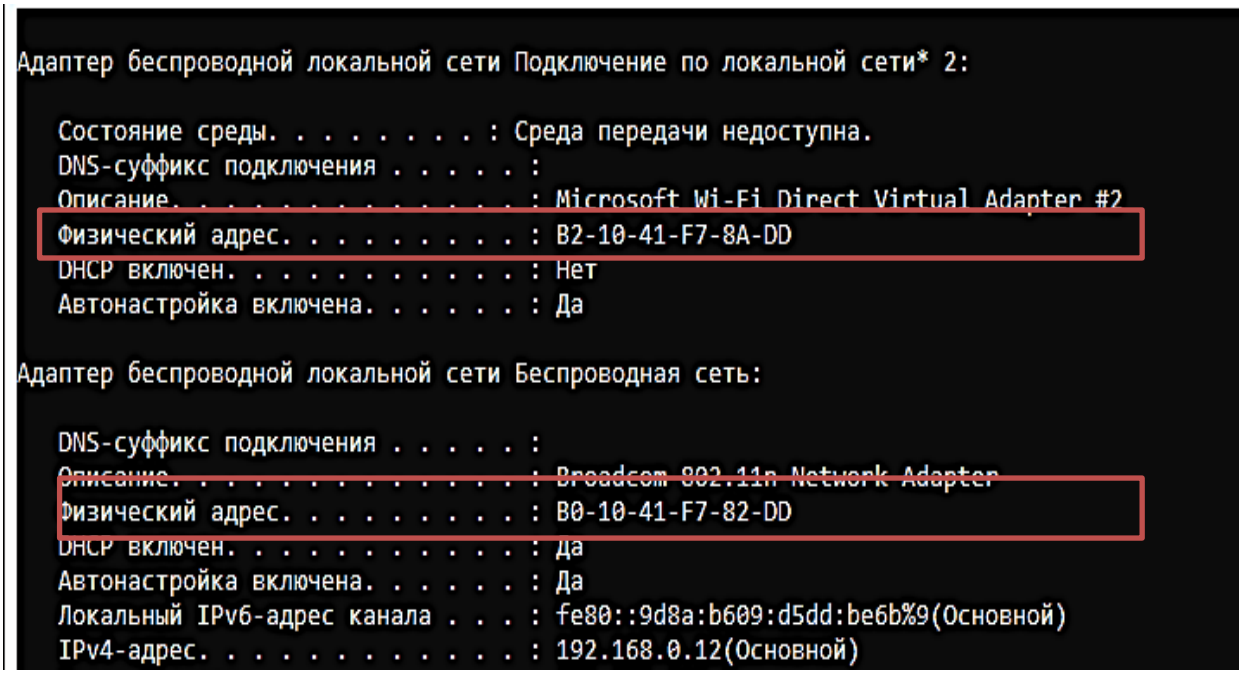


Рисунок 3.6 – Аппаратный адрес ПК

Находим пункт "физический адрес" — это и есть MAC-адрес. Если на компьютере установлено несколько сетевых карт, то пунктов "физический адрес" может быть несколько. В Widows XP можно MAC адрес определять специальными утилитами (рис. **3.6**).

Задание 3. DNS-сервер

DNS-сервер служит для преобразования доменных имен в IP-адреса, либо наоборот - IP-адресов в доменные имена.

Пример

Доменное имя: www.site.ru

IP-адрес сервера: 194.226.215.67

Например, если выполните в командной строке команду ping на какой-либо веб-сервер, то вы увидите, что его доменное имя транслируется в его IP адрес (рис. 2.7). Эту трансляцию и осуществляет DNS-сервер.

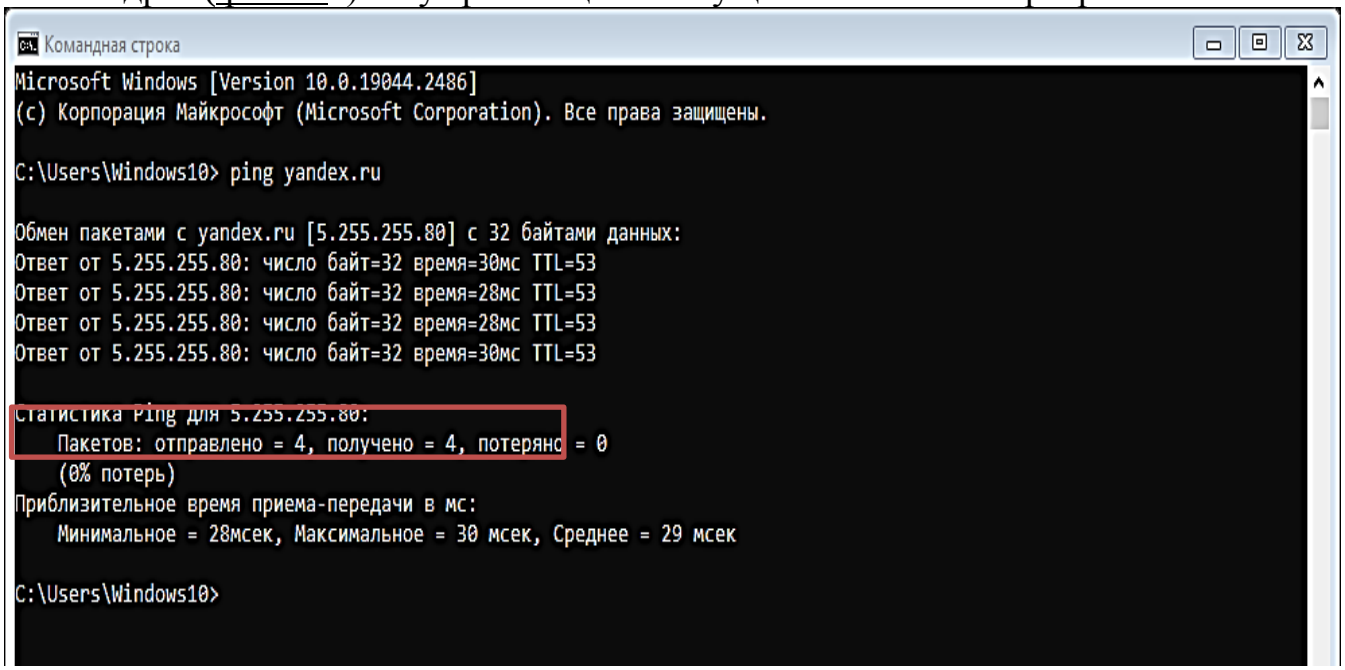


Рисунок 3.7 – Доменное имя (yandex.ru) преобразуется в IP адрес

Найти IP адрес для следующих доменных имен:

1. www.cybersecurity.ru
2. www.costacilento.it
3. www.google.ru
4. www.opera.com
5. www.microsoft.com
6. www.icq.com

Задание 4. Определить географическое положение сервера (IP Locate) (по варианту).

Для этого выполнить команду **Пуск – Программы – Стандартные – Командная Строка**, команда tracert и адрес (например www.mail.ru) (рис.3.8).

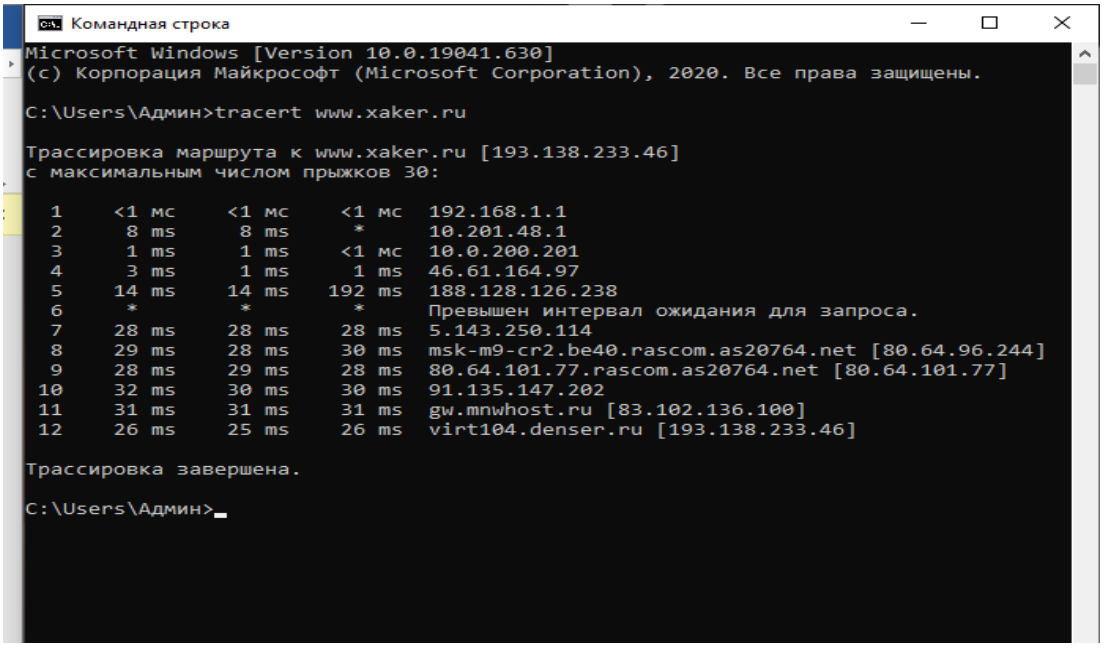


Рисунок 3.8

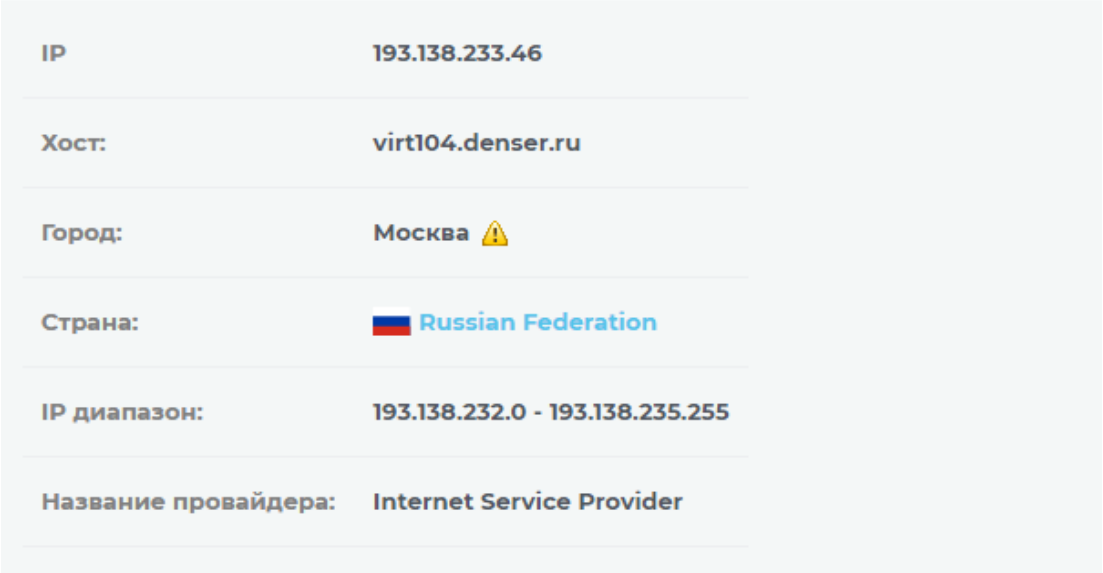


Рисунок 3.9

Варианты (для задания 6)

Вариант 1

a) www.mail.ru
b) www.dig.012.net.il
c) www.1c.ru
d) www.yandex.ru, www.habr.ru, www.webmoney.ru

Вариант 2

a) www.cybersecurity.ru
b) www.costacilento.it
c) www.google.ru
d**)** www.opera.com, www.microsoft.com, www.icq.com

Вариант 3
1)
a) www.xakep.ru
b) www.skylink.it
c) www.ru.board.com
d) www.ozone.ru

Вариант 4
a) sipnet.ru
b) www.red2000.com.mx
c) http://sipnet.ru/
d) www.avp.ru

Вариант 5
a) www.sibnet.ru
b) www.zelfservice.nl.uu.net
c) www.linux.org
d) 4konverta.com

Вариант 6
a) www.microsoft.ru
b) www.mckenna.net.nz
c) **www.cyberplat.ru**
d)geeknews.ru, infuture.ru, internet.ru

Вариант 7
a) live.cnews.ru
b) www.lg.nexlinx.net.pk
c) www.paycash.ru
d) www.csc.fi

Вариант 8
a) markettalk.ru
b) www.telesurf.com.py
c) www.eu.org
d) geospot.ru, livents.ru, tripster.ru

Вариант 9
a) askme.ru
b) www.home.pl
c) www.helios.de
d) wifi4free.ru

Вариант 10
a) ozone.ru
b) www.switch.ch
c) novoteka.ru, news2.ru, webplanet.ru
d) www.youtube.com

Задание 5. Определение маски сети

Рассчитать диапазон IP-адресов по IP-адресу и Маске подсети для вашего компьютера

Маской подсети (маской сети) называется битовая *маска*, определяющая, какая часть *IP*-адреса узла сети относится к адресу сети, а какая — к адресу узла. Например, узел с *IP*-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0/24 с длиной префикса 24 бита с числом узлов 254 (рис.3.10).

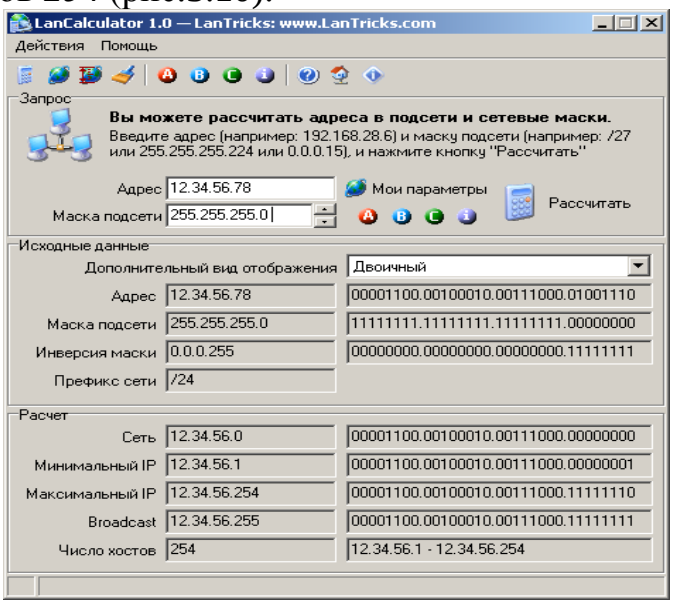


Рисунок 3.10 - Пояснение к термину Маски подсети
(расчеты выполнены в программе LAN Calculator)

IP калькуляторов довольно много. Можно использовать онлайн калькуляторы (рис.3.11).

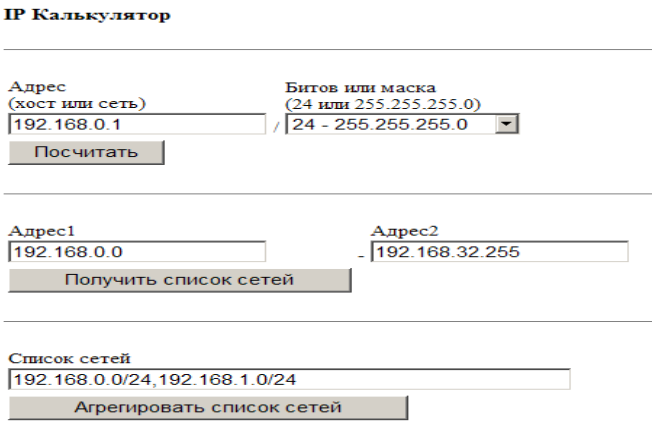


Рисунок 3.11– Онлайн IP калькулятор IP калькулятор на http://ip-calculator.ru/

Путем ввода в калькулятор вашего IP и маски вы можете рассчитать диапазоны IP-адресов от начального (минимального) до конечного (максимального). Диапазон IP адресов записывают в виде префикса. Иначе говоря, если вам встречается запись IP-адресов вида 10.96.0.0/11, то здесь 11 это префикс. Он означает количество единичных разрядов в маске подсети. Для приведённого примера маска подсети будет иметь 11 единиц, потом

нули, т.е. двоичный вид 11111111 11100000 00000000 00000000 или то же самое в десятичном виде: 255.224.0.0. 11 разрядов IP-адреса отводятся под номер сети, а остальные из 32 бит, т.е. 32 - 11 = 21 разряд полного адреса — под локальный адрес в этой сети. Итого, 10.96.0.0/11 означает диапазон адресов от 10.96.0.1 до 10.127.255.254. Для автоматизации подобных расчетов воспользуйтесь программой LanCalculator для Windows XP. Просто введите IP и Маску и нажмите на кнопку Рассчитать. Тот же результат вы получите проще и быстрее (рис. 3.12)

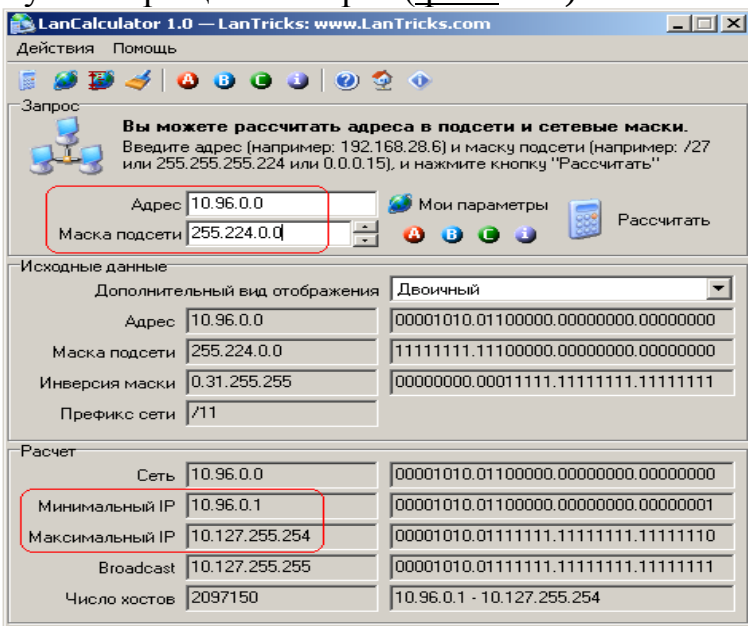


Рисунок 3.12 – Расчет диапазона IP адресов по IP адресу и Маске подсети

Вопросы для проверки

1. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
2. Что такое петля обратной связи?
3. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?
4. Как работает утилита tracert?
5. Каково назначение протокола ARP?
6. Какие утилиты можно использовать для определения IP адреса?
7. Какие утилиты можно использовать для определения физического адреса?
8. Что такое сетевой протокол?
9. Зачем введена модель OSI/ISO?
10. В чем принципиальное отличие протоколов TCP и UDP?

Содержание отчета:

1. Титульный лист. Цель работы. Результаты выполнения всех команд. Выводы.

Контрольные вопросы:1.Как определить MAC-адрес ПК ?

2. Для чего служит DNS-сервер

ЛАБОРАТОРНАЯ РАБОТА 4
Опрессовка прямого провода по стандарту Т568В

Цель: сформировать навыки обжимки витой пары, предназначенной для соединения *PC –HUB* с контролем правильности обжима, а также производить опрессовку сетевых розеток категории 5 под *разъем* RJ45.

Сетевые кабели

Для построения сети обычно используют один из трех проводников: *витая пара*, коаксиальный *кабель*, оптоволоконный *кабель*.

Витая пара

В настоящее время это наиболее распространённый сетевой проводник, состоящий из 8 медных проводников, перевитых друг с другом для уменьшения электромагнитных помех. *Длина* сегмента из такого провода – до 100 метров (рис.4.1).

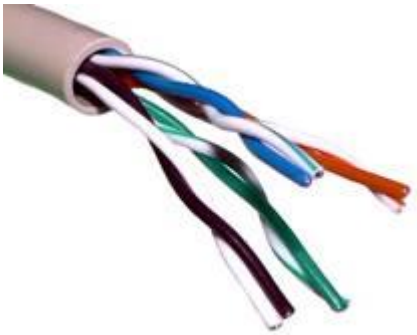


Рисунок 4.1 - Витая пара

С сетевой картой *кабель* соединяется разъемом 8P8C (рис.4.2)..

Рисунок 4.2 - Разъем 8P8C

Сетевое оборудование

Сетевая карта

Сетевые карты отвечают за передачу информации между ПК в сети. Каждая карта имеет свой индивидуальный *Mac-адрес*.

MAC-адрес сетевой карты – это уникальный *идентификатор*, предоставленный ей изготовителем. В сетях *Ethernet* он позволяет идентифицировать каждый *узел сети* и доставлять данные только этому узлу.

Основные характеристики:

- установленная микросхема контроллера (микрочип);
- разрядность – имеются 32- и 64-битные сетевые карты (определяется микрочипом);
- скорость передачи – от 10 до 1000 Мбит/с;
- разъем под тип подключаемого кабеля (коаксиальный, витая пара, волоконно-оптический кабель) – рис. 4.3.

Рисунок 4.3 - Сетевые карты на коаксиал и витую пару

Концентратор (хаб) и коммутатор (свитч)

Концентратор (*хаб*) используется, если в сети участвует больше 2 компьютеров. К нему сходятся все сетевые кабели витой пары в топологии *звезда*. Сигнал хаба получают все ПК сети, а не только та *сетевая карта*, которой адресован пакет данных. В настоящее время *концентраторы* сняты с производства и встречаются редко. Внешне свитч или *коммутатор* (*Switch*) практически не отличается от *Hub*, но *коммутатор* (*Switch*) - более интеллектуальное устройство, где есть свой *процессор*, внутренняя *шина* и буферная *память*. Если концентратор просто передает пакеты от одного порта ко всем остальным, то *Switch* анализирует *Mac* адреса, откуда и куда отправлен пакет информации и соединяет только эти компьютеры, в то время как остальные каналы остаются свободными. Это позволяет намного увеличить *производительность* сети, так как уменьшает количество паразитного трафика и обеспечивает большую фактическую *скорость передачи* данных, особенно в сетях с большим количеством пользователей – рис. 4.4.

Рисунок 4.4 - Свитч D-Link DES-1008D 8-port 10/100Mbps

Итак, концентратор обозначается значком  и его основная *функция* – это повторение сигналов, поступающих на один из его портов, на всех остальных портах (*Ethernet*).

Сетевой *коммутатор*, или свитч, обозначается значком  и в отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, *коммутатор* передает данные только непосредственно получателю. Это повышает *производительность* и *безопасность* сети, избавляя остальные *сегменты* сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор хранит в памяти таблицу, в которой указывается соответствие *MAC*-адреса узла порту коммутатора. При включении коммутатора эта *таблица* пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо *порт* данные передаются на все остальные порты коммутатора. При этом *коммутатор* анализирует кадры и, определив *MAC-адрес* хоста-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит *кадр*, предназначенный для хоста, *MAC-адрес* которого уже есть в таблице, то этот *кадр* будет передан только через *порт*, указанный в таблице. Если *MAC-адрес* хоста-получателя еще не известен, то *кадр* будет продублирован на все интерфейсы. Со временем *коммутатор* строит полную таблицу для всех своих портов, и в результате трафик локализуется.

Маршрутизатор (роутер)

Маршрутизатор - сетевое устройство, которое на основании информации о топологии сети и определённых правил принимает решения о пересылке пакетов между различными сегментами сети. Обозначается значком  - рис. 4.5.

Рисунок 4.5 - Беспроводной маршрутизатор D-Link 300Мбит/с (DIR-615/E4B)

Принцип работы маршрутизатора таков: он использует *адрес* получателя, указанный в пакетах данных, и определяет *по* таблице маршрутизации *путь*, *по* которому следует передать данные. *Маршрутизатор* может выбрать один из нескольких маршрутов доставки пакета адресату.

Маршрут – последовательность прохождения пакетом информации узлов сети.

В отличии от коммутатора, *маршрутизатор* видит все связи подсетей друг с другом, поэтому он может выбрать наилучший *маршрут* и при наличии нескольких альтернативных маршрутов. Решение о выборе маршрута принимается каждым маршрутизатором, через который проходит сообщение. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Ход работы:

Задание 1. Изучение сетевой карты, вынутой из ПК

Сетевая карта– плата, устройство, устанавливается в материнскую плату (рис. 4.6). Другое название сетевой карты – *сетевой адаптер*. *Сетевая карта* служит для соединения компьютера с другими компьютерами *по* локальной сети или для подключения к сети *Интернет*. Современные материнские платы имеют встроенную сетевую карту.

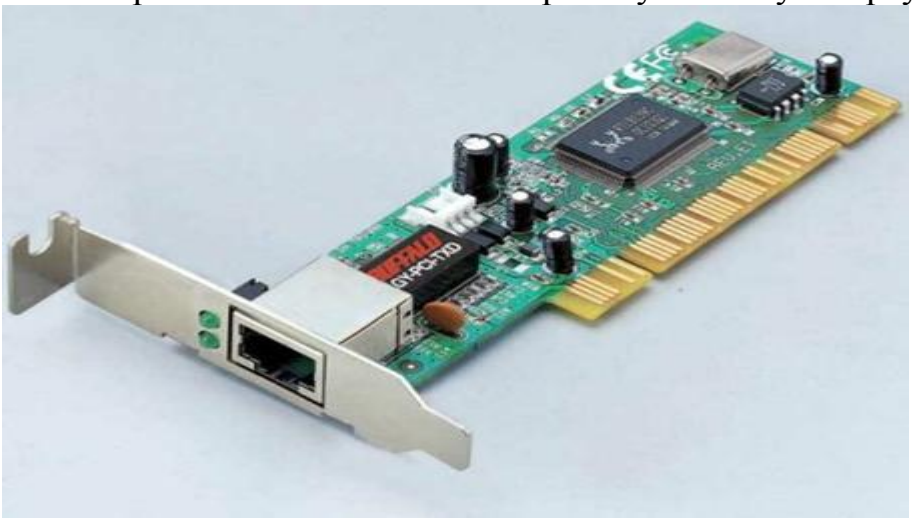


Рисунок 4.6 – Сетевая карта на чипе Realtek

Выбор производителя сетевой карты важен *по* следующим параметрам:

- надежность работы
- поддержка драйверами
- скорость

Когда речь идет о построении надежной и быстрой сети с богатыми возможностями мониторинга и управления, лидерами являются компании Intel и 3Com. Параметры сетевых карт определяются используемыми в них чипами. В современных картах обычно есть один большой чип, выполняющий функции контроллера шины и собственно сети. Среди других микросхем карты – приемопередатчик, энергонезависимая *память*, возможно *ПЗУ* для удаленной загрузки. Производителей чипов сетевых контроллеров гораздо меньше, чем производителей сетевых карт. При этом одни практически монополизируют выпуск карт на своих чипах (3Com, Intel), а другие (Realtek, *Via*) занимаются исключительно выпуском микросхем и их продажей.

1.Осмотрите сетевую карту, вынутую из ПК. Определите тип шины (*интерфейс*), к которой она подключается. Для этого посмотрите на ту часть сетевой карты, которая имеет контакты. Если *длина* этой стороны менее 10 см, то карта подключается к шине *PCI*. Кроме типа интерфейса у сетевых карт есть несколько других, менее важных параметров:

- поддержка Boot ROM (загрузка ПК без жесткого диска по сети)
- поддержка Wake On Lan (включение ПК по сети)
- поддержка режима Full Duplex (одновременные прием и передача информации, требуют поддержки этого режима от всего остального оборудования сегмента сети)
- количество индикаторов на задней панели

2. Определите тип физической среды (кабеля), с которой работает *сетевая карта*. Посмотрите на металлическую пластину, к которой крепится карта. Круглый *коннектор* свидетельствует о том, что эта карта для коаксиального кабеля; *разъем RJ-45* – для работы с витой парой. Найдите в *Интернет* ответ на вопрос о коннекторе для оптического кабеля самостоятельно.

Задание 2. Изучение сетевой карты, вставленной в ПК

В **Windows** выполните команду **Пуск-Панель управления-Система-Оборудование-Диспетчер устройств** и раскройте *список* **Сетевые платы** (рис. 4.7).

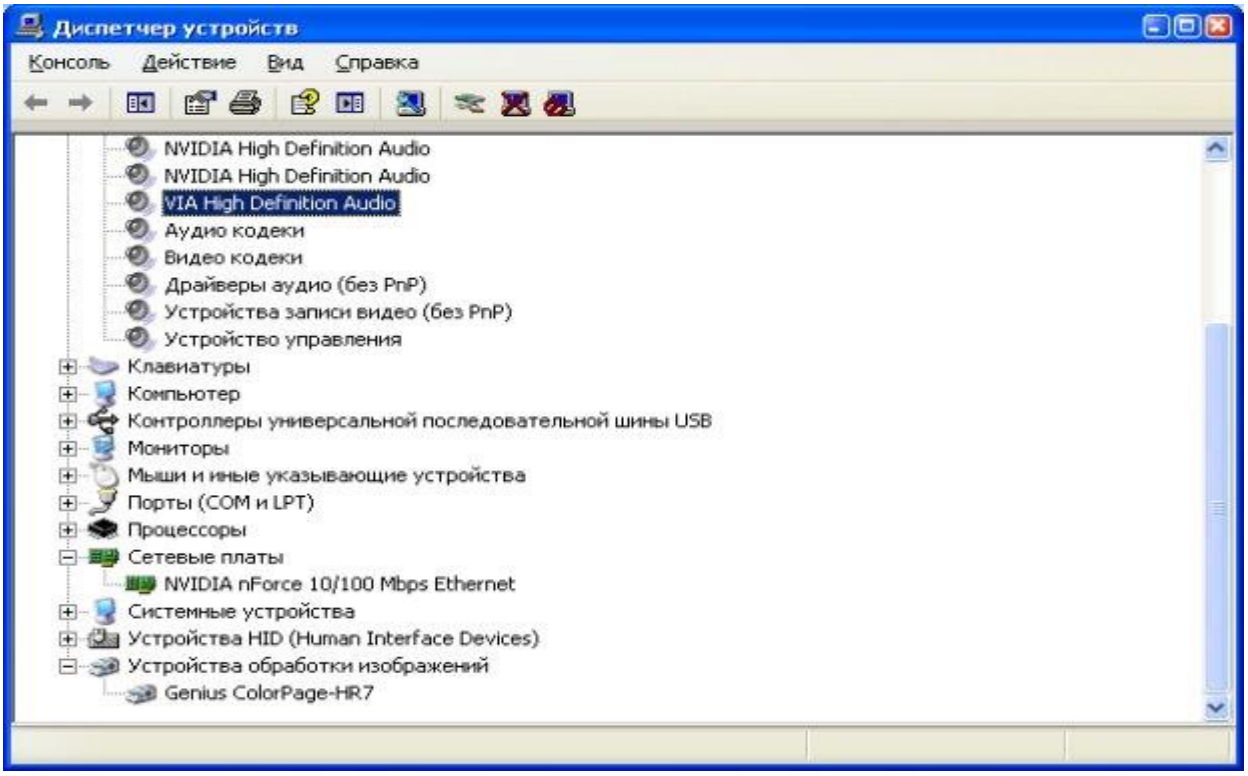
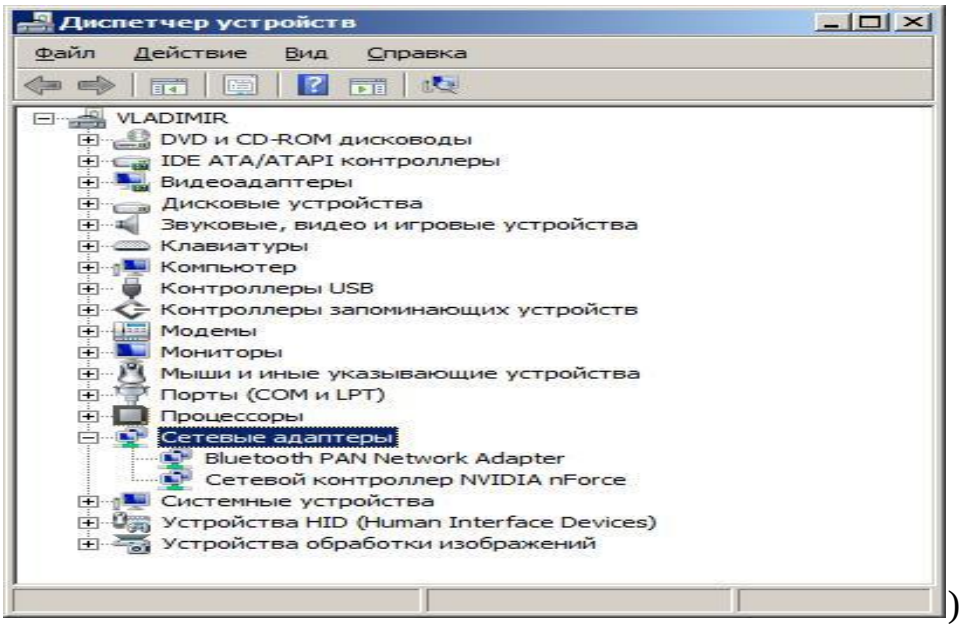


Рисунок 4.7 - В ПК установлена только одна сетевая плата

В **Windows 7** выполните команду **Пуск-Панель управления-Оборудование и звук-Диспетчер устройств** и раскройте *список* **Сетевые адаптеры**



).

Рисунок 4.8 - В ПК установлено два сетевых адаптера

Если у вас на сетевой плате нет желтых восклицательных знаков и красных крестиков, то ее драйвер установлен и работает корректно. Если напротив сетевого адаптера отображен восклицательный знак на фоне желтого круга, то драйвер конфликтует с другим устройством. Если напротив сетевой карты появился красный крестик, то драйвера вообще нет и его следует искать и устанавливать.

Задание 3. Опрессовка прямого провода по стандарту Т568В

При монтаже локальных сетей сегодня наиболее распространена неэкранированная *витая пара* 5й категории (CAT-5E) – рис. 4.9.

Рисунок 4.9 - Кабель витая пара

Обжим такого кабеля для соединения ПК (*PC*)-ХАБ (*HUB*) по стандарту Т568В изображен на рис. 4.10.

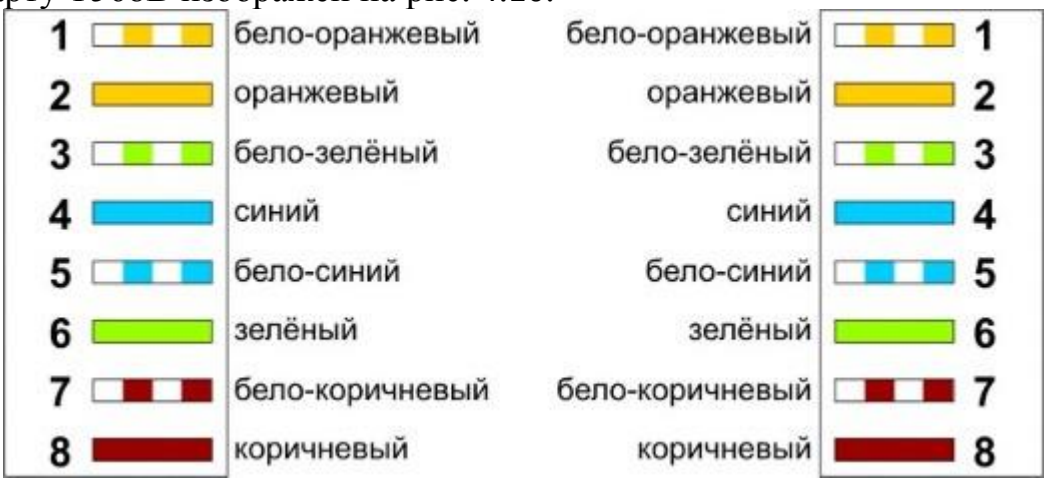
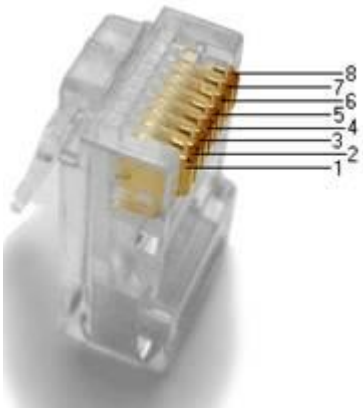


Рисунок 4.10 - Прямой обжим для соединения ПК-ХАБ
(Одинаковый цвет проводников с обеих сторон кабеля)

Обжим (опрессовка) по варианту Т568А - стандарт, имеющий хождение в США и Канаде, а в России, в основном, применяется стандарт Т568В.

Для обжима (опрессовки) витой пары вам потребуются пара коннекторов RJ-45и специальные клещи (кримпер) - рис 4.11-4.13.



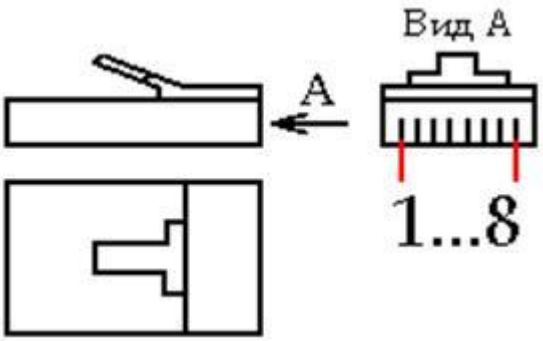


Рисунок 4.11 - Нумерация контактов разъема RJ-45

Рисунок 4.12. Кримпер

Рисунок 4.13. Коннектор вставлен в кримпер

Последовательность действий при обжиме:

- Аккуратно обрежьте конец кабеля резаком, встроенным в обжимной инструмент.
- Снимите с кабеля изоляцию ножом, встроенным в обжимной инструмент.
- Разведите и расплетите проводки, выровняйте их в один ряд. Обкусите проводки так, чтобы их осталось чуть больше сантиметра.
- Вставьте проводники в коннектор RJ-45. Убедитесь, все ли провода полностью вошли в разъем и уперлись в его переднюю стенку.
- Вставьте коннектор в устройство для обжима коннектора.
- Надавите на клещи так, чтобы контакты коннектора зажали проводники внутри него.

На рис. 4.14 показан неправильный обжим витой пары. На примере слева оставлены слишком длинные жилы, из-за чего расстояние от коннектора до оплетки остается незащищенным. Также кабель теряет прочность. На втором примере жилы срезаны слишком коротко, оплетка входит в коннектор и длина концов проводников не позволяет создать их полноценный контакт с коннектором.

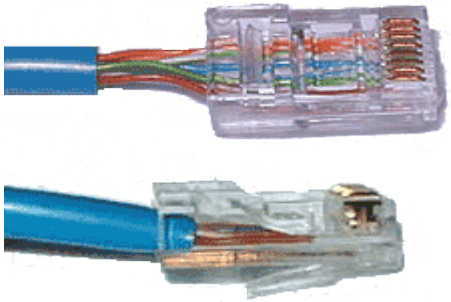


Рисунок 4.14 - Ошибки обжима кабеля

Контроль результата

Для проверки правильности обжима соедините кабелем сетевую карту и *HUB* (*коммутатор*, свич) и убедитесь в правильной работе такого кабеля. Другой вариант – использовать специальный тестер со светодиодной индикацией (рис. 4.15).

Рисунок 4.15 - Внешний вид тестера для проверки витых пар RJ-45 модели FA-7012B

В продаже представлено множество тестеров для проверки витых пар *RJ-45* разного уровня сложности и ценового диапазона. Однако, принцип работы их аналогичен. Так, например, кабельный тестер FA-7012B состоит из 2 функциональных блоков – передатчика и приемника, которые подключаются к концам кабельной линии через разъемы *RJ-45* или RJ-12. Он позволяет обнаружить оборванные пары, закороченные пары, перепутанные провода в одной паре, перепутанные пары и перепутанные провода между разными парами. Также прибор позволяет проверить *целостность* экрана кабеля. Блок-передатчик последовательно опрашивает состояние каждого провода в кабеле, а блок-приёмник возвращает ответ по неиспользуемой в конкретный момент паре. Последовательное загорание светодиодов сигнализирует о правильном соединении. Устройство питается от 1 батареи типа "Крона" 9 В.

Вопросы для проверки

1. Что такое сетевые адаптеры на компьютере?
2. Виды сетевых адаптеров
3. Как включить сетевой адаптер на Windows 7?
4. Виды сетевого оборудования
5. Что такое Коннектор ?
6. Опишите последовательность действий при обжиме сетевого кабеля для соединения ПК (*PC*)-ХАБ (*HUB*) по стандарту T568B

Содержание отчета:

a. Титульный лист.
b. Цель работы.
c. Результаты выполнения всех команд.
d. Выводы. (Отчет составляем на основе вопросов для проверки)

Контрольные вопросы:

1. Если напротив сетевой карты стоит красный крестик, что это значит?

ЛАБОРАТОРНАЯ РАБОТА 5
Ознакомление с интерфейсом программы NetEmul. Соединение ЭВМ в сеть

Цель работы: Ознакомиться с основами работы с программным эмулятором ЛВС NetEmul, освоить основы логического моделирования компьютерной сети.

Интерфейс программы

Для начала установим программу, запустим и русифицируем ее командой **Сервис-Настройки** (рис. 5.1).

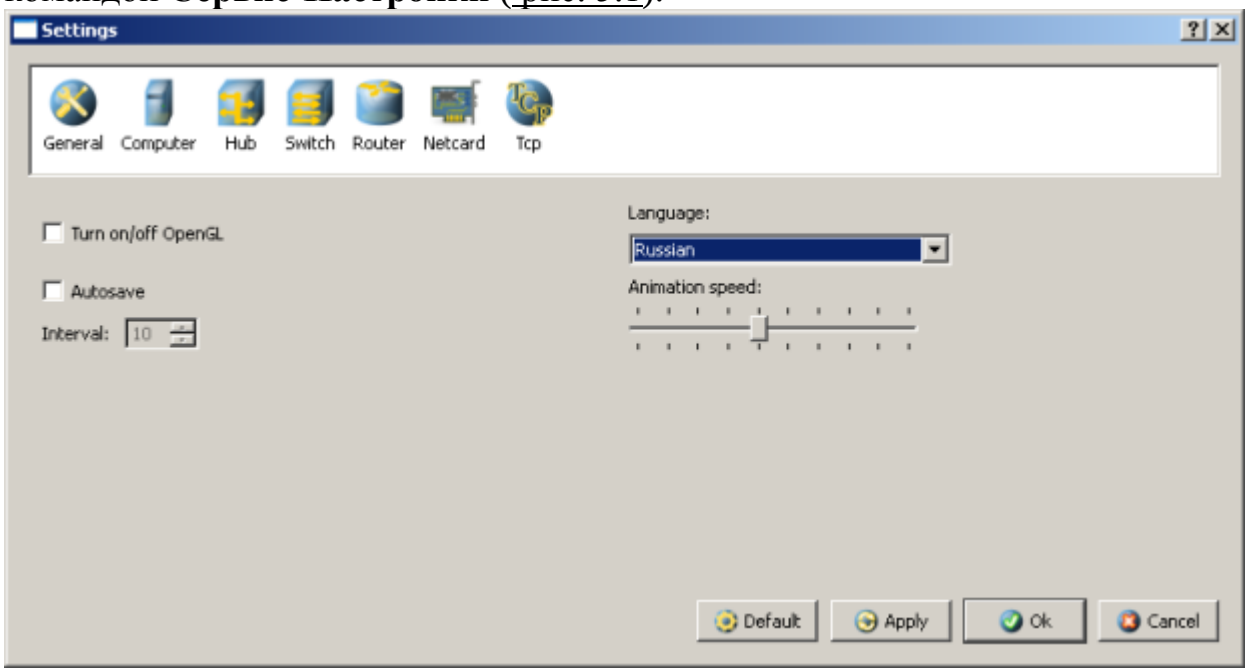
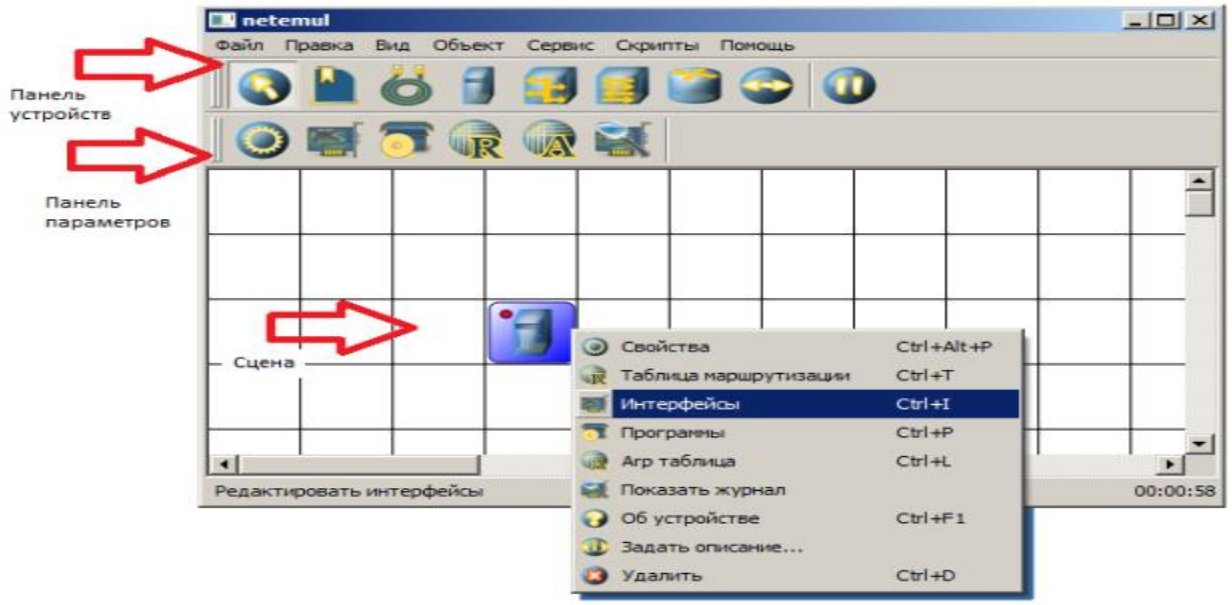


Рисунок 5.1 - Интерфейс программы

В главном окне программы все элементы размещаются на рабочей области (на **Сцене**). На всей свободной области сцены, размеченной сеткой можно ставить устройства, при этом они не должны пересекаться. На **Панели устройств** размещены все необходимые для построения сети инструменты, а также кнопка отправки сообщений и **Запустить /Остановить.** На **Панели параметров** расположены свойства объектов. Для выделенного объекта появляются только те свойства, которые характерны для него (рис. 5.2).



l

Рисунок 5.2.1 - Интерфейс программы Netemul

Рис.2

Панель устройств (рис5.2.1) предназначена для добавления и перемещения ряда сетевых устройств. Описание пунктов панели (слева-направо):

1.Перемещение объектов – позволяет перемещать устройства по сцене;

2.Текстовая надпись – позволяет добавить текстовую заметку на сцену;

3.Кабель (создать соединение) – позволяет соединять устройства в сети;

4.Добавить компьютер – установка персонального компьютера на сцену;

5.Добавить концентратор – установка сетевого концентратора (hub) на сцену;

6.Добавить коммутатор – установка сетевого коммутатора (switch) на сцену;

7.Добавить маршрутизатор – установка сетевого маршрутизатора (router) на сцену;

8.Отправить данные – используется для проверки работоспособности сети.

9.Остановить симуляцию – останавливает запущенную передачу данных в сети.

Рисунок 5.2.2 - Интерфейс программы Netemul

Панель параметров (рис.5.2.2) предназначена для настройки отдельно взятого устройства в сети. Важно отметить, что у каждого из сетевых устройств используются собственные настройки, поэтому не все пункты будут активны для каждого из устройств в сети. Описание пунктов панели

(слева-направо):

1. Показать свойства – вызывает диалоговое окно со свойствами сетевого устройства. Например, для компьютера это шлюз; для концентратора и коммутатора – количество портов и MAC-адреса в сети; для маршрутизатора – количество портов и включение или выключение маршрутизации.

2. Редактирование интерфейсов – пункт меню, с помощью которого задаются IP-адреса и маски подсети. Используется для настройки компьютера и маршрутизатора.

3. Установленные программы – с помощью данного пункта можно присвоить компьютеру и маршрутизатору свойство сервера или клиента;

4. Таблица маршрутизации – с помощью данного пункта можно задать правила маршрутизации;

5. ARP-таблица – позволяет задать соответствие между IP-адресами и MAC-адресами устройства;

6. Журнал устройства – с помощью данного пункта можно просмотреть подробный журнал событий устройства в сети, где отображаются проходящие через него пакеты при передаче данных.

Ход работы:

Для запуска эмулятора NetEmul необходимо либо воспользоваться соответствующим пунктом главного меню операционной системы, либо выполнить в терминале команду netemul.

Задание 1. Соединение двух ЭВМ напрямую

Добавить на рабочее поле эмулятора два компьютера (рис. 5.3), использовав кнопку «Добавить компьютер» на панели инструментов.

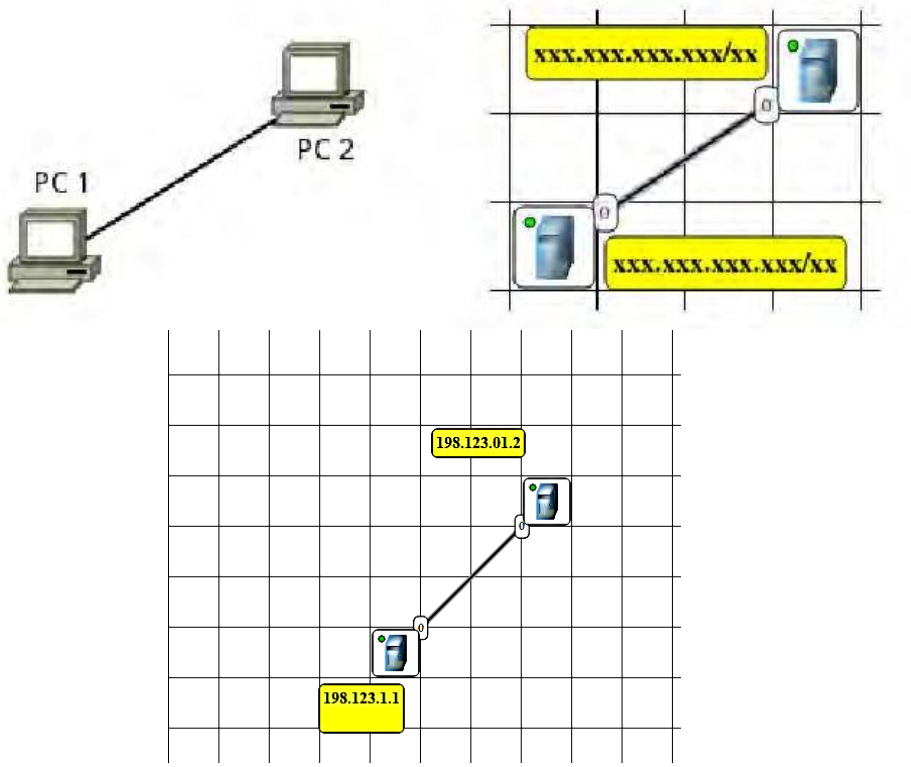


Рисунок 5.3– Соединение двух ЭВМ напрямую

Соединить добавленные компьютеры как показано на рис. 5.3.

Для этого:

а) нажать кнопку «Создать соединение» на панели инструментов;

б) навести указатель на один из компьютеров;

в) зажав ЛКМ, перевести курсор на второй компьютер – за курсором от первого компьютера должна тянуться прямая линия;

г) отпустить ЛКМ – после этого должно появиться окно начальных настроек с выбором соединяемых интерфейсов;

д) подтвердить соединение между интерфейсами eth0 и eth0, нажав «Соединить»;

е) если все сделано правильно, то компьютеры теперь соединены, на каждом конце соединения показан номер используемого интерфейса (в данном случае - 0), а индикатор соединения на иконке компьютера сменил цвет с красного на желтый (соединение есть, но интерфейсы не настроены).

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

а) выбрать инструмент «Перемещение объектов» на панели инструментов;

б) выделить первый компьютер щелчком ЛКМ;

в) вызвать контекстное меню щелчком ПКМ и выбрать пункт

«Интерфейсы»;

г) в появившемся окне указать в соответствующих полях IP-адрес и маску подсети;

д) подтвердить ввод последовательным нажатием кнопок «Применить» и «ОК»;

е) если все сделано правильно, то индикатор соединения на иконке компьютера должен сменить цвет с желтого на зеленый (соединение есть, и интерфейсы настроены);

ж) добавить возле каждого компьютера надпись с его IP-адресом и маской подсети как показано на рис. 5.3.

Проверить работоспособность построенной модели ЛВС, передав пакетыот одного компьютера до другого. Для этого необходимо:

а) выбрать инструмент «Отправить данные» на панели инструментов;

б) под курсором (на рабочем поле программы) должен появиться красныйкруг;

в) навести курсор с красным кругом на передающий компьютер и нажатьЛКМ;

г) в появившемся окне «Отправка» указать: протокол TCP, размер данных5 KB;

д) нажать «Далее» — окно пропадет, а кружок под курсором сменит цветна зеленый;

е) навести курсор с зеленым кругом на принимающий компьютер нажатьЛКМ;

ж) в появившемся окне подтвердить интерфейс на принимающем компьютере eth0, нажав «Отправка»;

з) проследить за перемещением пакетов.

Задание 2

Построить одноранговую локальную сеть (рис.5.4).

1. Добавьте на рабочую область два компьютера и один концентратор.
2. Присвойте каждому компьютеру IP-адрес.
3. Соедините устройства.
4. Проверьте работоспособность сети.
5. Сохраните выполненную работу.

Ход выполнения

1. Для добавления устройств на рабочую область:

На панели устройств выберите объект «Компьютер», и щелкните левой кнопкой мыши на свободные клетки поля, чтобы добавить устройства;

Таким же образом добавьте на рабочую область устройство «Концентратор».

2. Для присвоения компьютерам IP-адресов:

·Выделите компьютер, щелкнув на него левой кнопкой мыши;

·На панели параметров выберите пункт «Редактировать интерфейсы»;

·В появившемся окне в строке «IP-Адрес» введите IP-адрес 198.123.0.1 и нажмите кнопку «ОК»;

Таким же образом присвойте IP-адрес 198.123.0.2 второму компьютеру.

3. Для соединения устройств:

На панели инструментов выберите объект «Кабель»;

Наведите курсор мыши на устройство «Концентратор», и зажав левую кнопку мыши проведите линию до первого компьютера, после чего отпустите левую кнопку мыши;

В появившемся диалоговом окне настроек интерфейсов выберите в левой колонке пункт «LAN1», а во второй «eth0», и нажмите кнопку «Соединить»;

Таким же образом соедините концентратор со вторым компьютером, выбрав в диалоговом окне настроек интерфейсов в левой колонке пункт «LAN2».

4. Для проверки работоспособности сети:

На панели устройств выберите объект «Отправить данные»;

Наведите курсор мыши на первый компьютер и нажмите левую кнопку;

В появившемся диалоговом окне «Отправка» выберите TCP протокол для передачи данных и установите необходимый объем для передачи, после чего нажмите кнопку «Далее»;

Наведите курсор мыши на второй компьютер и нажмите левую кнопку мыши;

В появившемся диалоговом окне «Отправка» выберите интерфейс приемника «eth0» и нажмите кнопку «Отправка»;

В случае верной настройки сети, по линиям, которые соединяют устройства, начнется передача данных, которые представлены в программе в виде точек.

5. Сохраните изменения в файле проекта командой Файл, Сохранить.

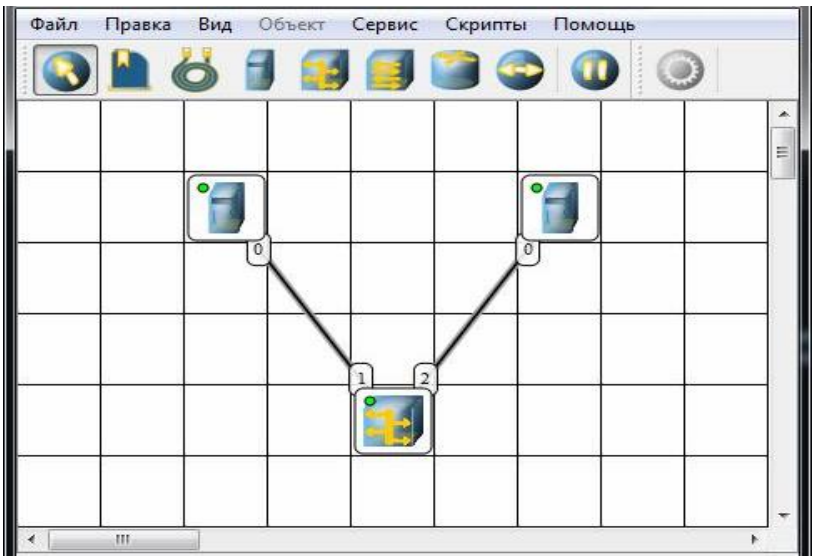
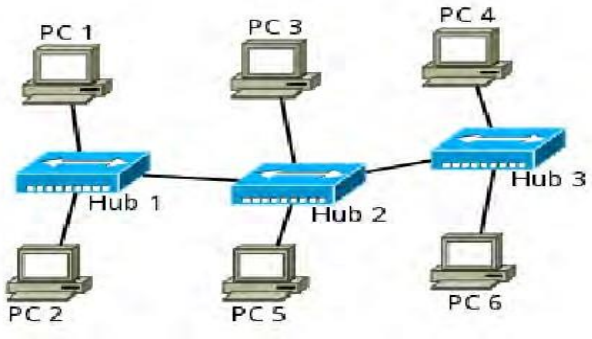
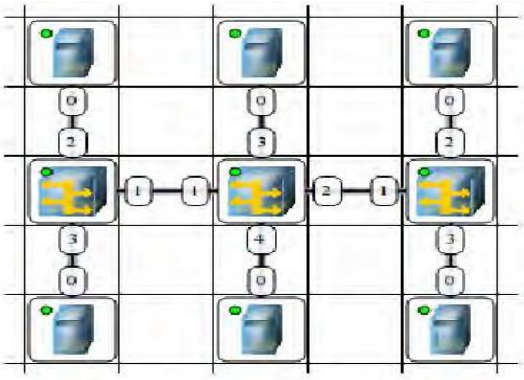


Рисунок 5.4 -Построение ЛВС на концентраторах

Задание 3. Добавить на рабочее поле эмулятора шесть компьютеров и три концентратора как показано на рис. 5.5. Соединить устройства как показано на рис. 1.2. Добавить возле каждого компьютера надпись с его IP-адресом и маской подсети. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе концентраторов.





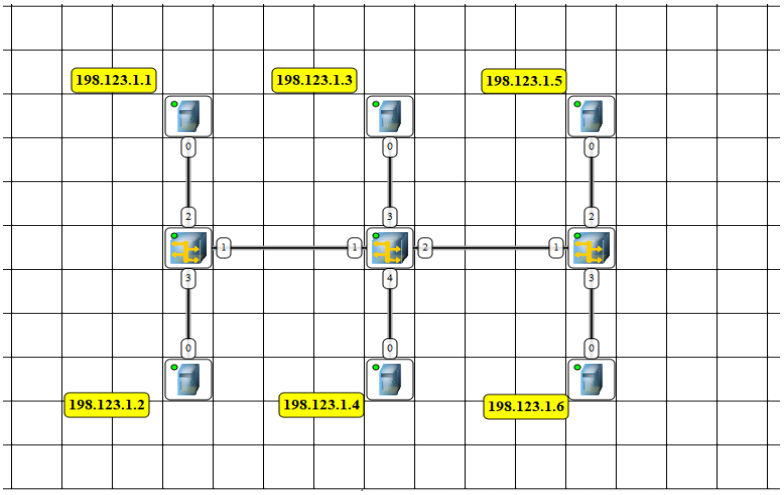


Рисунок 5.5 – Построение ЛВС на концентраторах

Задание 4. Построение ЛВС на коммутаторах

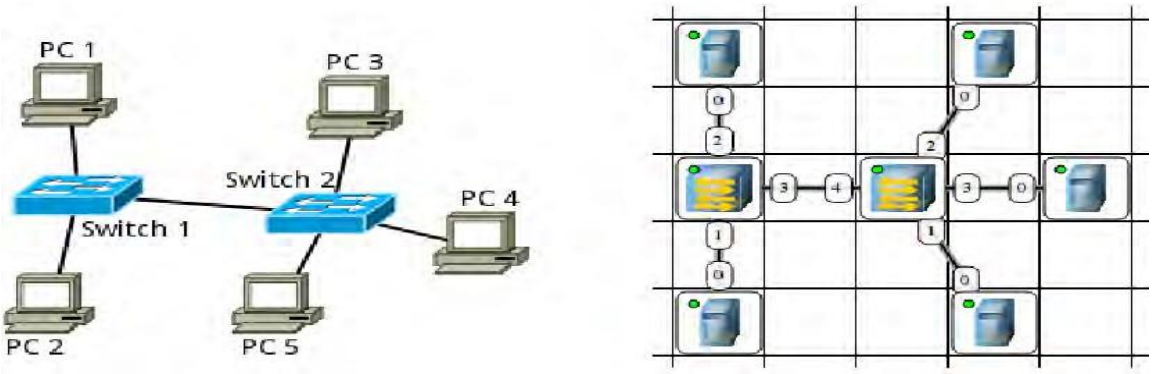


Рисунок 5.6 – Построение ЛВС на коммутаторах

Добавить на рабочее поле эмулятора пять компьютеров и два коммутаторакак показано на рис. 5.6.

Соединить устройства как показано на рис. 5.7.

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

Таблица 5.1–Варианты заданий

№	IP-адрес
1.	**10.124.56.220**
2.	**113.72.101.11**
3.	**173.143.32.194**
4.	**200.69.139.217**
5.	**88.212.236.76**
6.	**93.187.72.48**
7.	**72.163.4.161**
8.	**15.217.232.245**
9.	**69.20.59.80**
10.	**43.243.130.61**

Добавить возле каждого компьютера надпись с его IP-адресом и маской подсети. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 500 KB) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе коммутаторов.

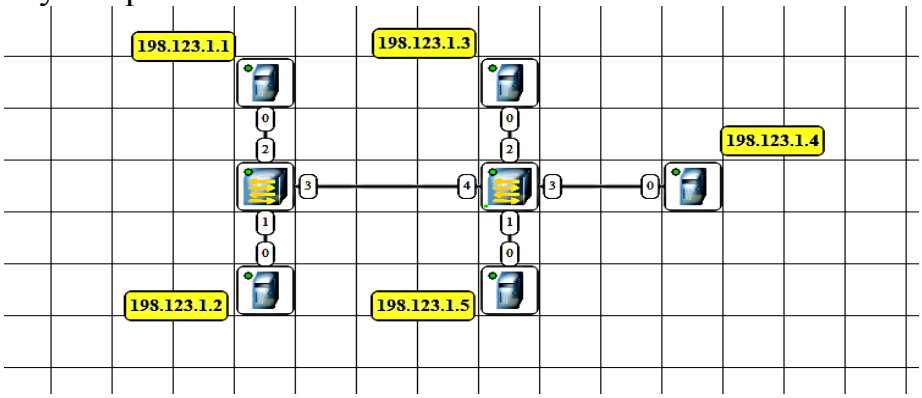


Рисунок 5.7. – Построение ЛВС на коммутаторах

Содержание отчета:

1. Титульный лист.
2. Цель работы.
3. Результаты выполнения всех команд.
4. Выводы.

Контрольные вопросы:

1. Какие сетевые устройства применяются для создания компьютернойсети?
2. Какие настройки необходимы для прямого соединения двух компьютеров по сети?
3. Напишите операции при обмене пакетами между компьютерами.
4. Перечислите особенности передачи информации при организации сетина базе концентраторов.
5. Перечислите особенности передачи информации при организации сетина базе коммутаторов.

ЛАБОРАТОРНАЯ РАБОТА 6

Маршрутизация в NetEmul

Цель работы: Научиться формировать статические маршруты и прописывать их в таблицы маршрутизации сетевых устройств

Ход работы:

Задание 1

С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую номер группы. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 6.1.

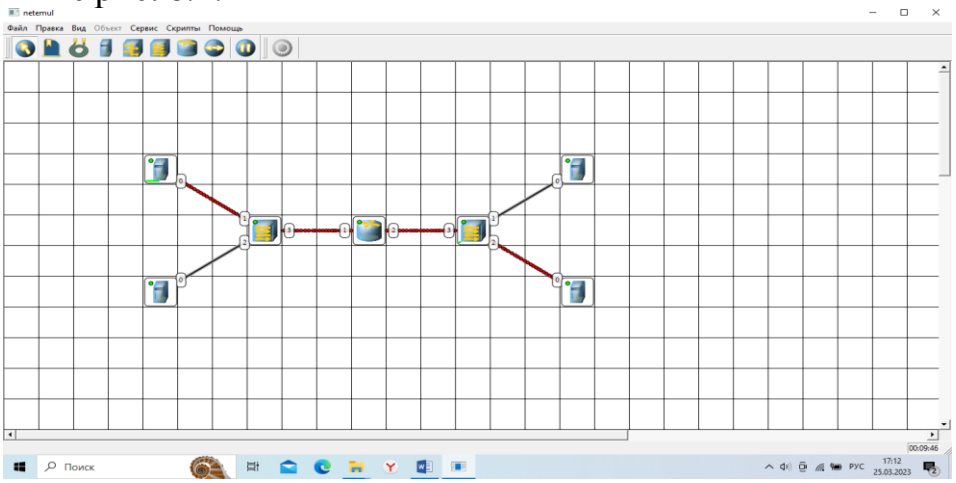


Рисунок 6.1 – Модель ЛВС

Настроить интерфейсы компьютеров (рис.6.2)
КОМПЬЮТЕР 1: 110.110.1.2
КОМПЬЮТЕР 2:110.110.1.3
КОМПЬЮТЕР 3:120.120.1.2
КОМПЬЮТЕР 4:120.120.1.3

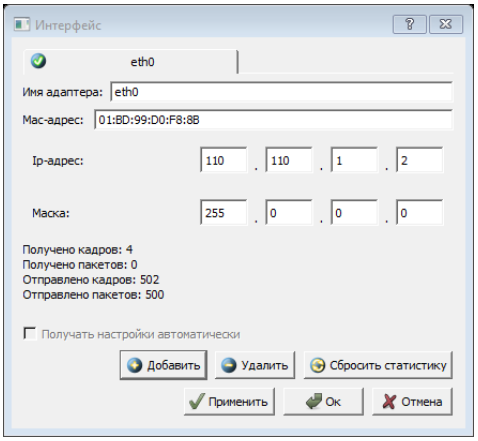


Рисунок 6.2 – Интерфейсы компьютеров

Далее нажимаем ПКМ, свойства (рис.6.3) настраиваем шлюз для всех компьютеров, поставить галочку включить маршрутизацию.
КОМПЬЮТЕР 1: 110.110.1.1
КОМПЬЮТЕР 2:110.110.1.1
КОМПЬЮТЕР 3:120.120.1.1
КОМПЬЮТЕР 4:120.120.1.1

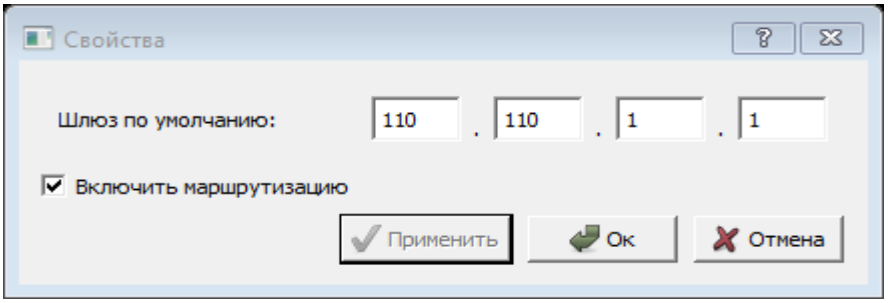


Рисунок 6.3

Далее, в свойствах каждого маршрутизатора необходимо указать количество интерфейсов, равное 4 и поставить галочку включить (рис. 6.4).

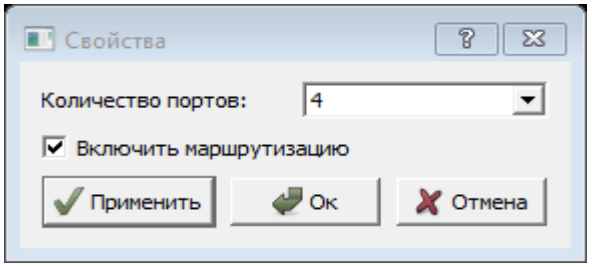


Рисунок 6.4

Настроить интерфейсы маршрутизатора, задав IP-адрес и маску подсети для ЛВС1(110.110. 1.1) и ЛВС2 (120.120. 1.1) (рис. 6.5- 6.6).

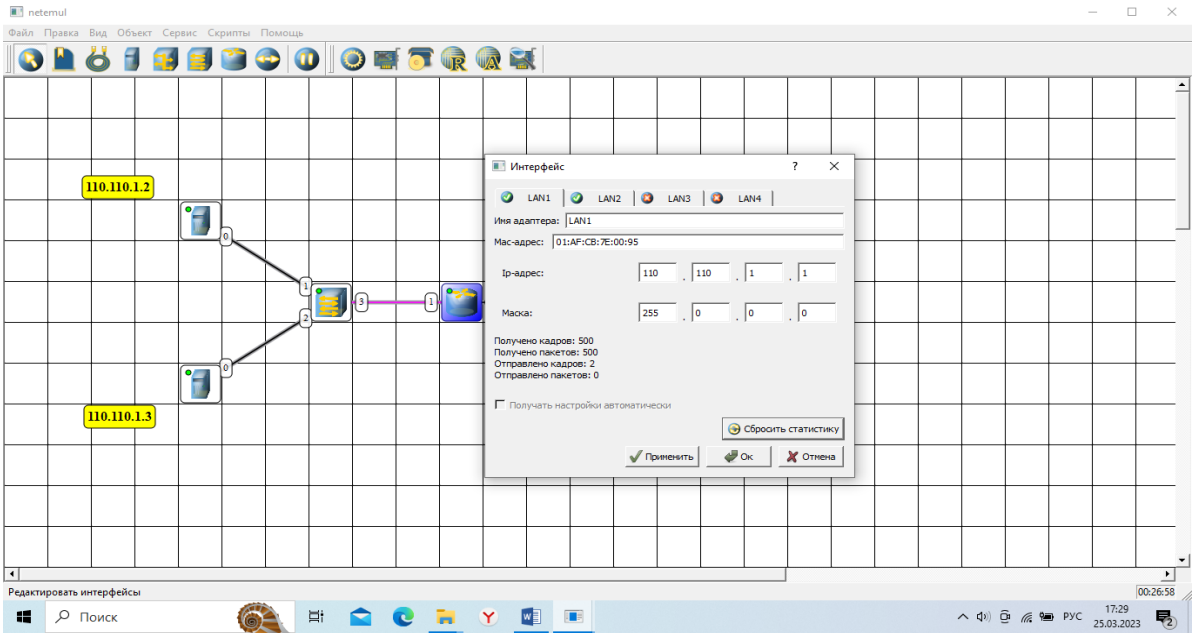


Рисунок 6.5

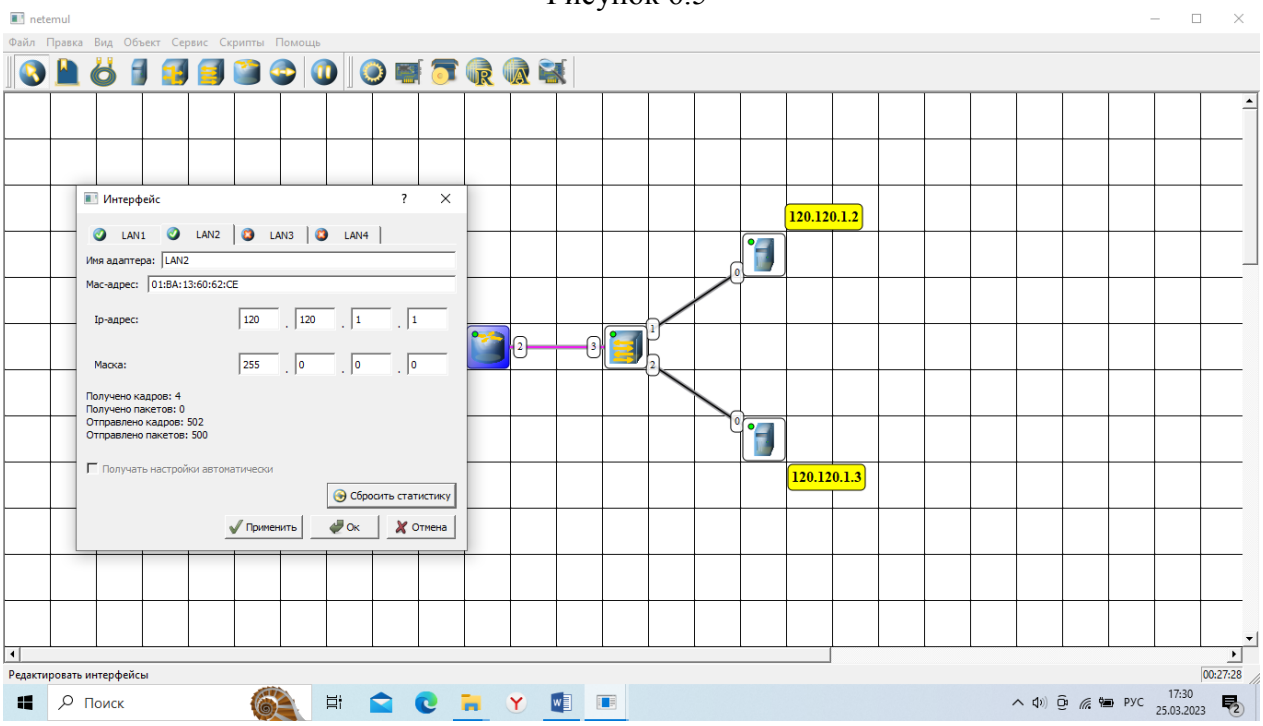


Рисунок 6.6

Проверить работоспособность построенной модели сети, передав пакеты (TCP, 500 KB) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе коммутаторов

ЛВС 3 (130.130.1.1) подключить самостоятельно и проверить работоспособность построенной модели сети (**рис. 6.7**).

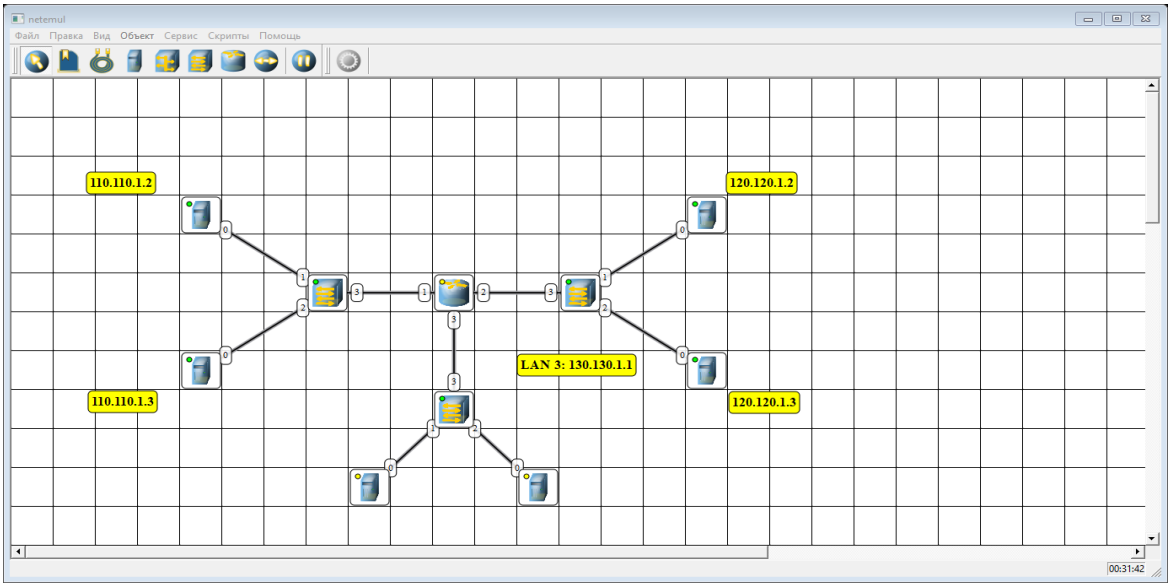


Рисунок 6.7

Задание 2.
Построить сеть с двумя маршрутизаторами

Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 6.8.

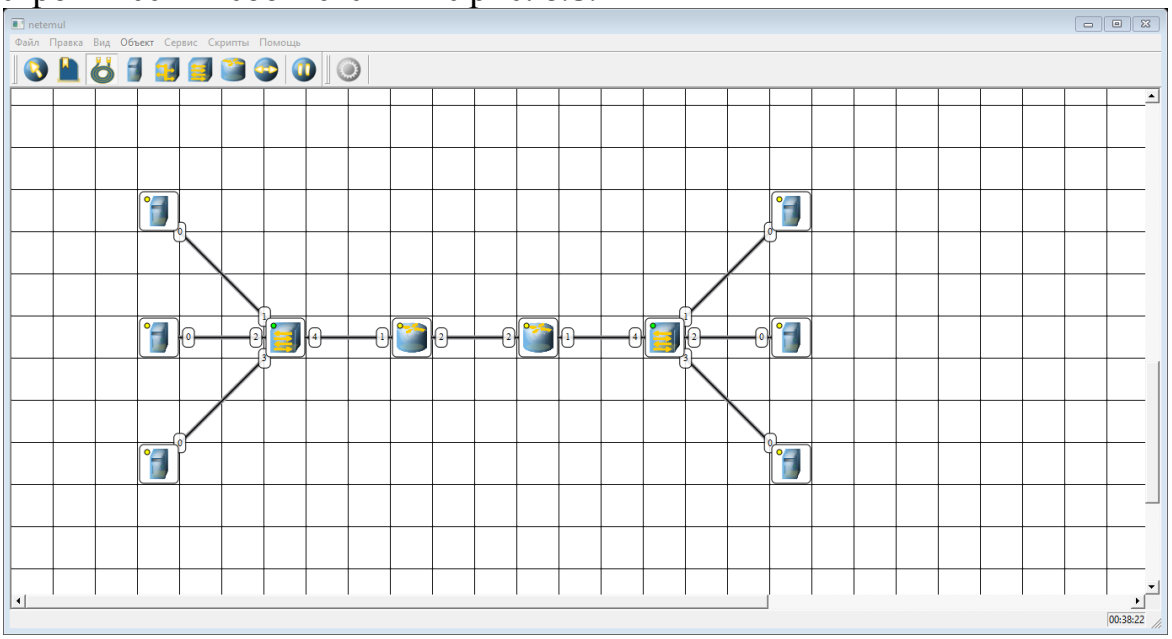


Рисунок 6.8

Настроить IP-адреса всех компьютеров ЛВС 1 и ЛВС 2 (рис.6.9).
ЛВС 1
192.168.1.2
192.168.1.3
192.168.1.4
ЛВС 2
192.168.2.2
192.168.2.3
192.168.2.4

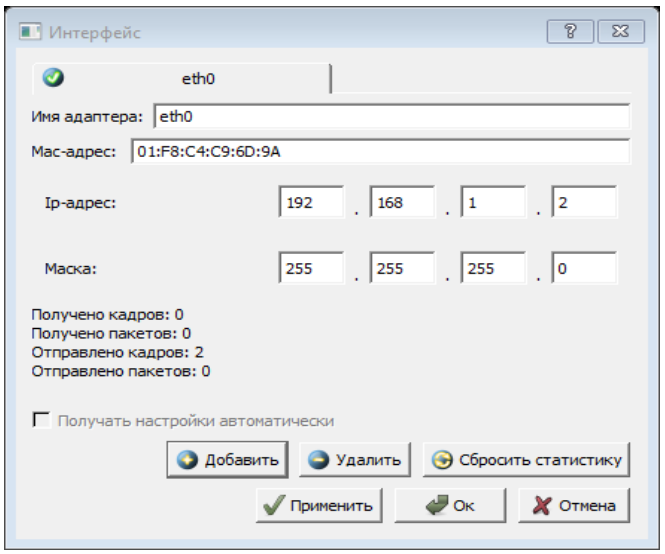


Рисунок 6.9

Настраиваем маршрутизатор (рис.6.10). Нажимаем ПКМ на 1 маршрутизатор выбираем интерфейс. Выбираем LAN 1. Задаем адрес из этой сети 192.168.1.1 (рис.6.10).

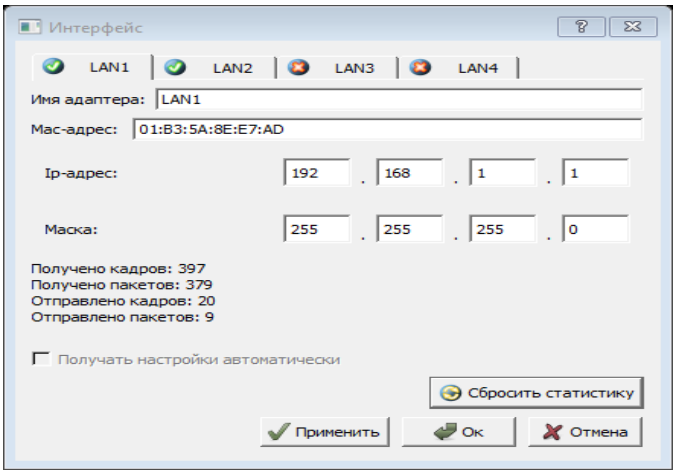


Рисунок 6.10

LAN 2 – это сеть между маршрутизаторами 200.100.50.1(рис.6.11).

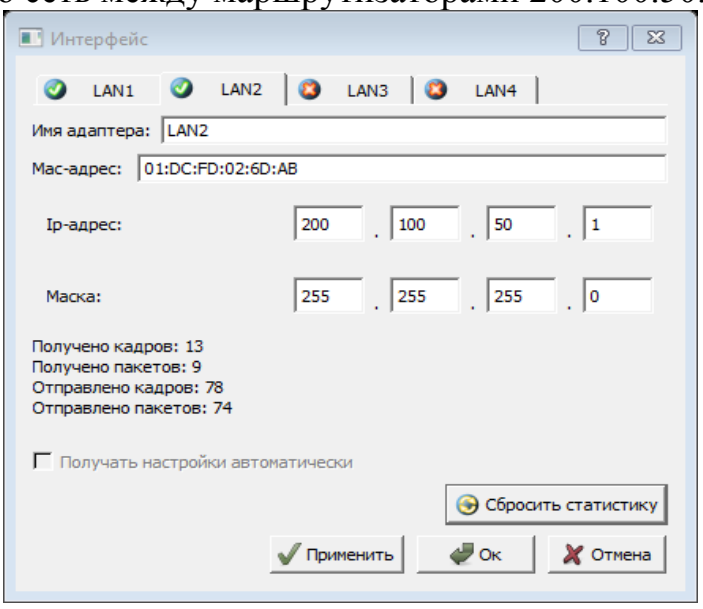


Рисунок 6.11

Настроить второй маршрутизатор адрес LAN 1:192.168.2.1 (рис.6.12).

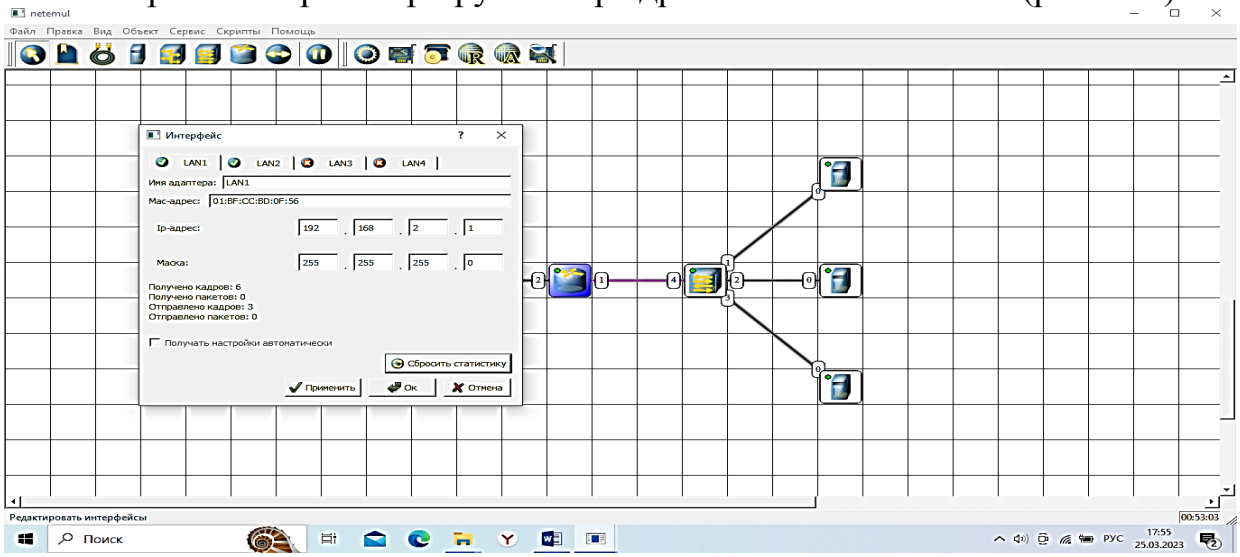


Рисунок 6.12 – Настройка LAN 1

Настроить второй маршрутизатор адрес LAN 2:200.100.50.2 (рис.6.13).

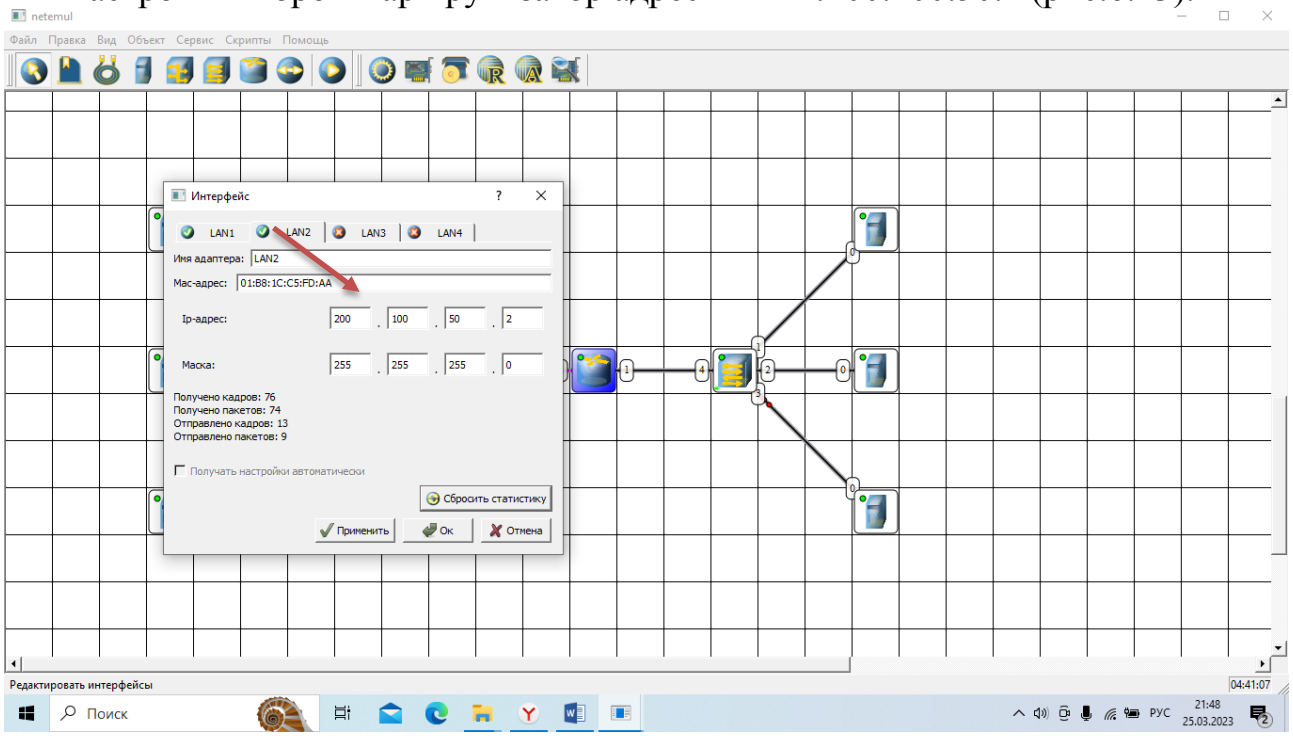


Рисунок 6.13 – Настройка LAN 2

Настроить шлюз по умолчанию у компьютеров, который совпадает с адресом маршрутизатора. Для LAN 1 – 192.168.1.1

Для LAN 2 – 192.168.2.1

Настроить свойства маршрутизаторов (рис.6.14).

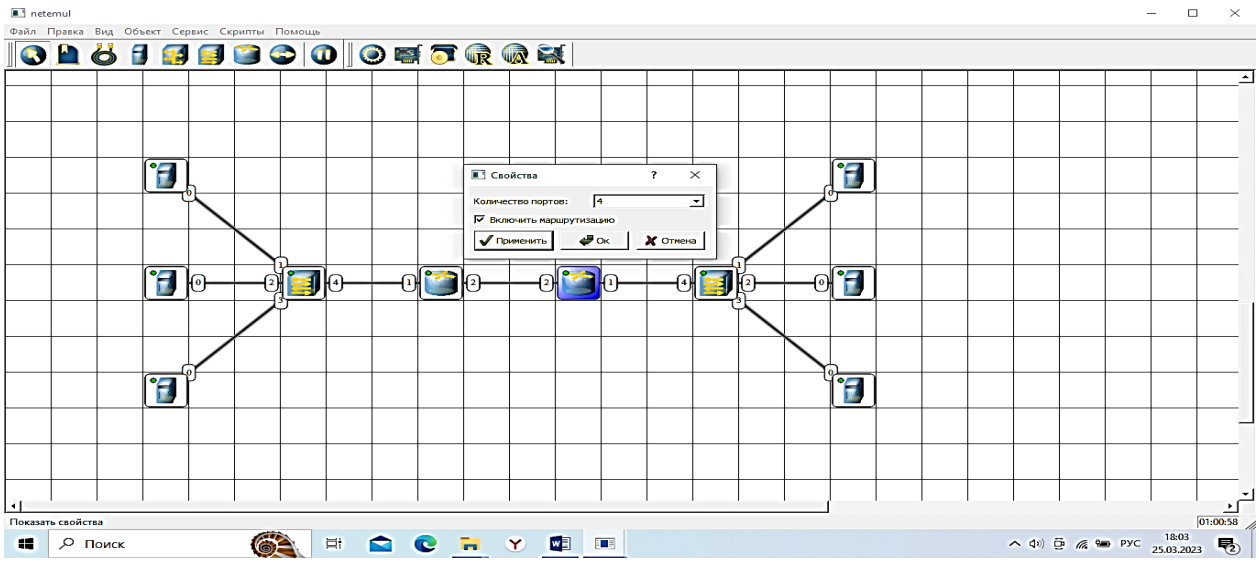


Рисунок 6.14 – Настройка свойств маршрутизаторов

Построить таблицу маршрутизации (рис.6.15, 6.1). Нажимаем ПКМ на 1 маршрутизатор выбираем таблицу маршрутизации.

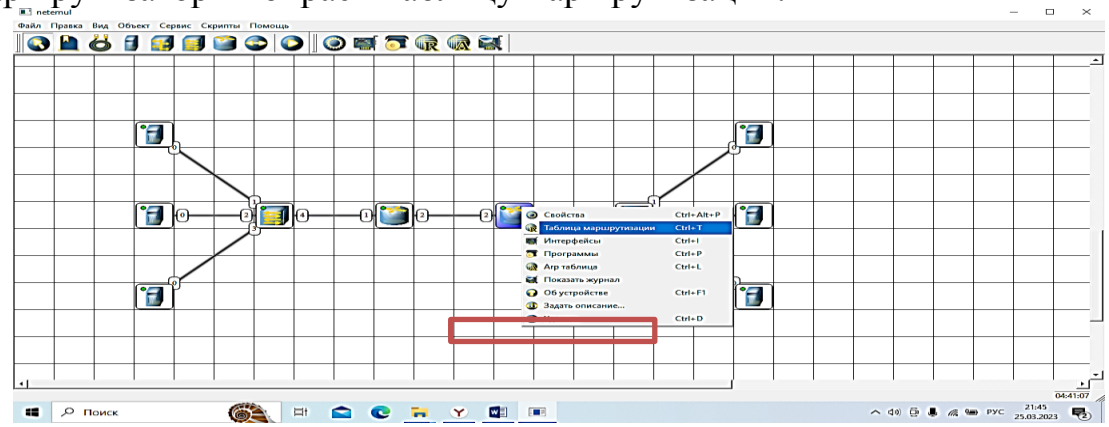


Рисунок 6.15 – Настройка таблицы маршрутизации

В таблице маршрутизации первого маршрутизатора выбрать интерфейс LAN 2 и задать:

Адрес назначения192 168 2 0

Маску 255 255 255 0

Шлюз 200.100. 50. 2 (LAN 2 второго маршрутизатора)

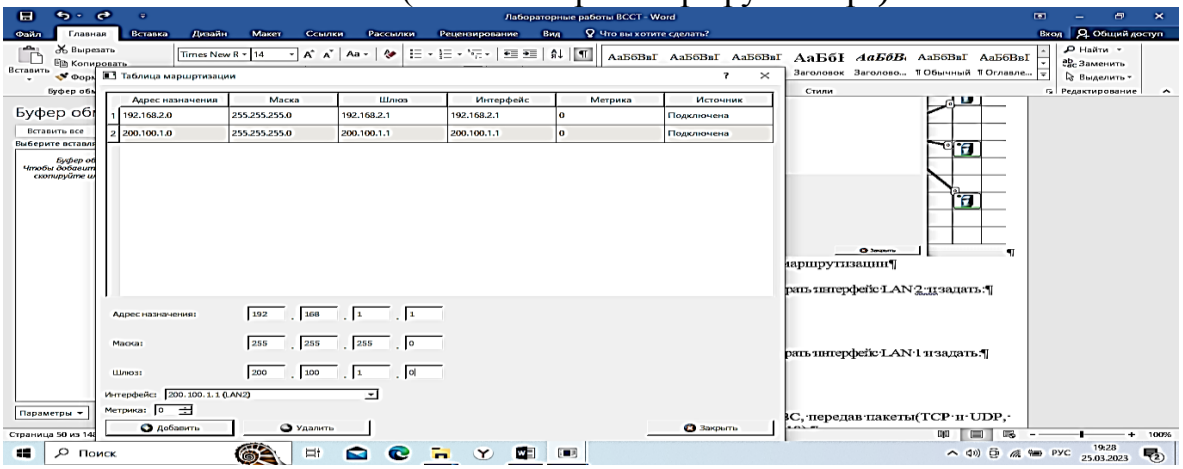


Рисунок 6.16 – Настройка таблицы маршрутизации

В таблице маршрутизации второго маршрутизатора выбрать интерфейс LAN 2 и задать:

Адрес назначения192 168 1 0

Маску 255 255 255 0

Шлюз 200.100. 50.1 (LAN 2 первого маршрутизатора)

Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP и UDP, 5 KB) между удаленными друг от друга сетями(рис.6.17).

Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе маршрутизаторов.

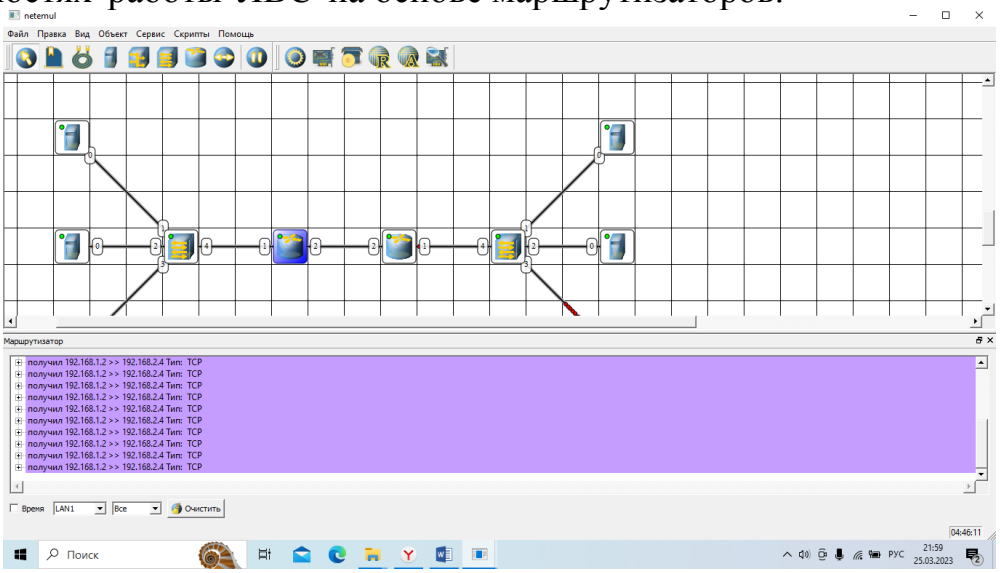


Рисунок 6.17

Содержание отчета:

1. Титульный лист.
2. Цель работы.
3. По каждому пункту лабораторной должна быть приведена схема моделис указанием IP-адресов устройств и номеров интерфейсов.
4. По каждому пункту лабораторной должны быть приведены выводы по работе.

Контрольные вопросы:

1. Что такое IP-адрес?
2. Что такое маска подсети?
3. Как работает маршрутизатор?
4. Принципы статической маршрутизации?

ЛАБОРАТОРНАЯ РАБОТА 7
Разрешение адресов по протоколу ARP

Цель работы: Ознакомиться с механизмом работы протокола ARP. Научиться формировать и отправлять пользовательские пакеты. Ознакомиться с журналом работы сетевого устройства в эмуляторе. Научиться проводить сетевую атаку вида ARP-спуфинг.

ARP (Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса сетевого устройства по известному IP-адресу.

Наибольшее распространение ARP получил благодаря повсеместности сетей IP, построенных поверх Ethernet, поскольку в подавляющем большинстве случаев при таком сочетании используется ARP. В семействе протоколов Ipv6 протокола ARP не существует, его функции возложены на ICMPv6. Описание протокола было опубликовано в ноябре 1982 г. в RFC 826.

ARP был спроектирован для случая передачи IP-пакетов через сегмент Ethernet. При этом общий принцип, предложенный для ARP, был использован и для сетей других типов.

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

Система-отправитель при помощи запроса ARP запрашивает физический адрес системы-получателя. Ответ (физический адрес узла-получателя) приходит в виде ответа ARP. Принцип работы протокола: узел (хост A), которому нужно выполнить отображение IP-адреса на MAC-адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес (хост 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 (хост B) формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель (хост A) указывает свой локальный адрес.

Схема работы показана на рисунке 7.1.

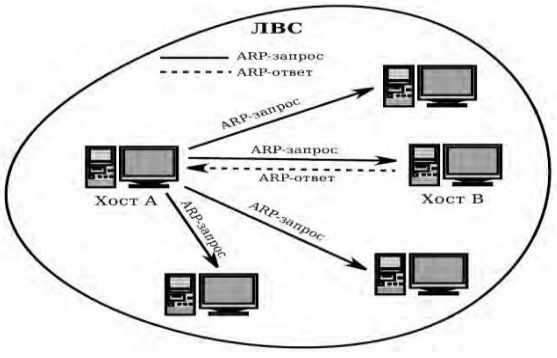


Рисунок 7.1 – Схема работы протокола ARP

При получении ARP-ответа хост A записывает в кэш ARP запись с соответствием IP-адреса хоста B и MAC-адреса хоста B, полученного из ARP-ответа. Время хранения такой записи ограничено. По истечении времени хранения хоста A посылает повторный запрос, теперь уже адресно, на известный MAC-адрес хоста B. В случае, если ответ не получен, снова посылается широковещательный запрос.

Структура кадра ARP с учетом заголовка Ethernet показана на рисунке 7.2.

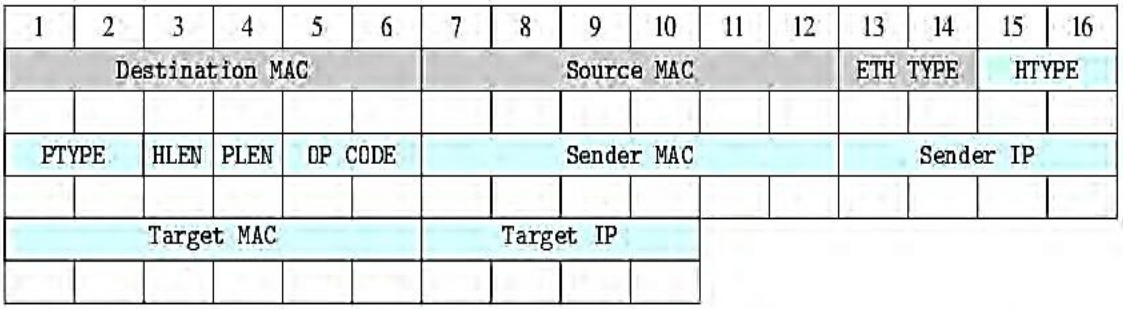


Рисунок 7.2 – Структура кадра ARP

Значения полей заголовка кадра ARP приведены в табл. 7.1.

Таблица 7.1

Поле	Значение	
HTYPE	Номер протокола передачи канального уровня (0x0001 для протокола Ethernet	
PTYPE	PE 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, когда в этом (с точки зрения получателя) нет особой необходимости. Самопроизвольный ARP-ответ — это пакет-ответ ARP, присланный без запроса. Он применяется для определения конфликтов IP- адресов в сети: как только станция получает адрес по DHCP или адрес присваивается вручную, рассылается ARP-ответ gratuitous ARP.

Самопроизвольный ARP может быть полезен в следующих случаях:

- обновление ARP-таблиц, в частности, в кластерных системах;
- информирование коммутаторов;
- извещение о включении сетевого интерфейса.

Несмотря на эффективность самопроизвольного ARP, он является особенно небезопасным, поскольку с его помощью можно уверить удаленный узел в том, что MAC-адрес какой-либо системы, находящейся с ней в одной сети, изменился, и указать, какой адрес используется теперь.

Сетевая атака ARP-спуфинг (ARP-spoofing) основана на использовании самопроизвольного ARP. Чтобы перехватить сетевые пакеты, которые атакуемый хост (A) оправляет 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.

Ход работы:

Задание 1. Построение сети.

1. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 8.3.

Настроить интерфейсы компьютеров и маршрутизаторов **(192.168.2.254),** задав каждому IP-адрес и маску подсети (**ПК1 - 198 162 2 1 (MAC-адрес** 01:6B:14:BC:4D:AC**), ПК2 -198 162 2 2 (MAC-адрес** 01:4C:63:A9:E3:02**), ПК3 -198 162 2 3 (MAC** 01:6E:44:24:4C:AA**)).** В свойствах маршрутизатора необходимо указать количество интерфейсов, равное 4.

2. Добавить возле каждого компьютера надписи с их IP-адресом и MAC-адресом.

3. Настроить на компьютерах маршруты «по умолчанию» (IP сети = 0.0.0.0; маска подсети = 0.0.0.0). Можно воспользоваться «Таблицей маршрутизации» либо вызвать свойства компьютера двойным щелчком, указать шлюз по умолчанию и включить маршрутизацию.

4. Включить маршрутизацию на маршрутизаторе.

5. Открыть ARP-таблицу компьютера: в ней нет никакой информации.

6. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от 1 компьютера до 2 компьютера.

7. Открыть ARP-таблицу компьютера: в ней есть информация о MAC-адресах этих двух компьютеров.

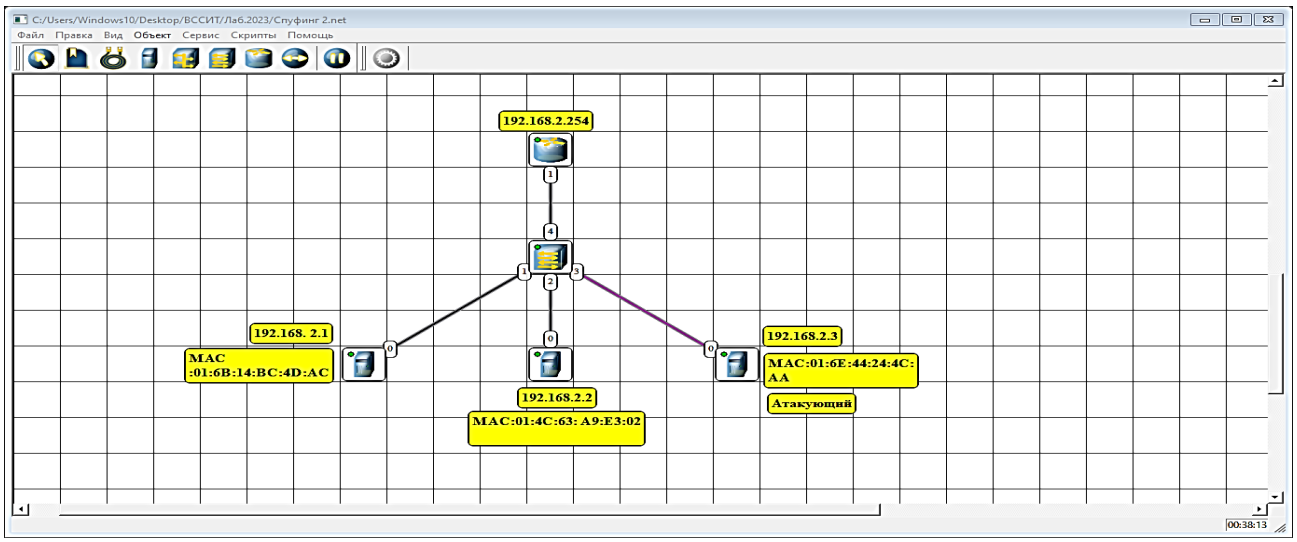


Рисунок 7.3 – Структура ЛВС для ознакомления с ARP протоколом

Задание 2.

Определение MAC-адреса с помощью ARP-запроса

Очистить ARP-таблицу компьютеров (рис.8.4).

1. Выделить компьютер 1 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-запроса для определения MAC-адреса компьютера 2. Помните, что ARP-запрос рассылается широковещательно (MAC-адрес получателя в заголовке Ethernet — FF:FF:FF:FF:FF:FF), а MAC- адрес искомого узла в заголовке ARP приравнивается к нулевому 00:00:00:00:00:00. MAC-адрес компьютера 1 указан в окне «Интерфейсы» длякомпьютера 1.

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

3. Открыть ARP-таблицу компьютера 1 и убедиться, что записьдобавилась в таблицу.

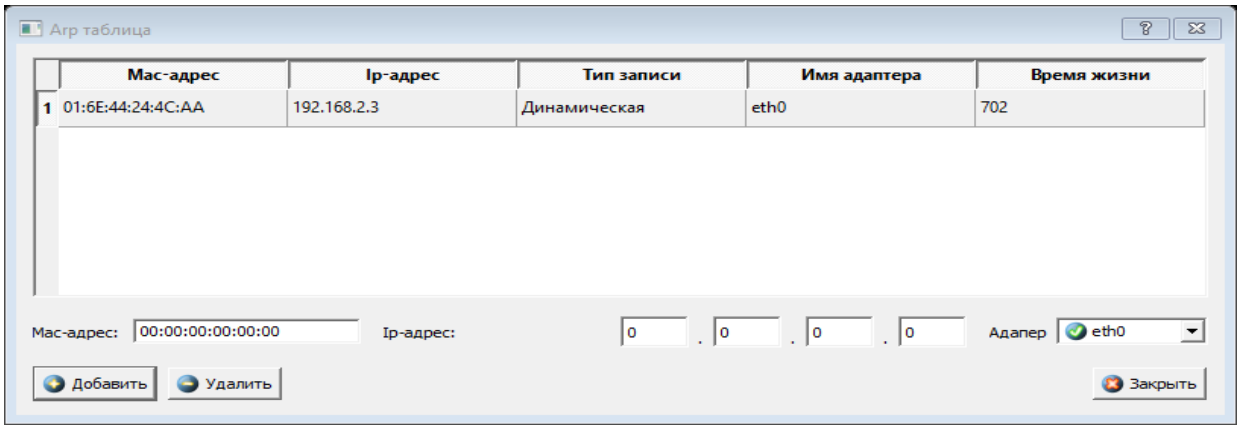


Рисунок 7.4

Тоже самое можно сделать для второго компьютера .

Реализация атаки ARP-спуфинг.

1. Запустить для компьютеров 1 и 2 журналы пакетов (пункт меню «Показать журнал»). При необходимости очистить их.

2. Очистить ARP-таблицу компьютера 1.

3. Выделить компьютер 2 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-ответа, в котором будут указаны:

- MAC отправителя — MAC компьютера 2;
- 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 KB) от компьютера 1 накомпьютер 3. Убедиться, что пакеты вначале приходят на компьютер 2 и лишь потом (если на компьютере 2 включена маршрутизация) отправляются на компьютер 3 (через маршрутизатор).

Атакующий компьютер (ПК3) заходит в свои настройки копирует MAC отправителя (например ПК1 01:6B:14:BC:4D:AC) и подставляет вместо своего (рис.7.5, 7.6,7.7).

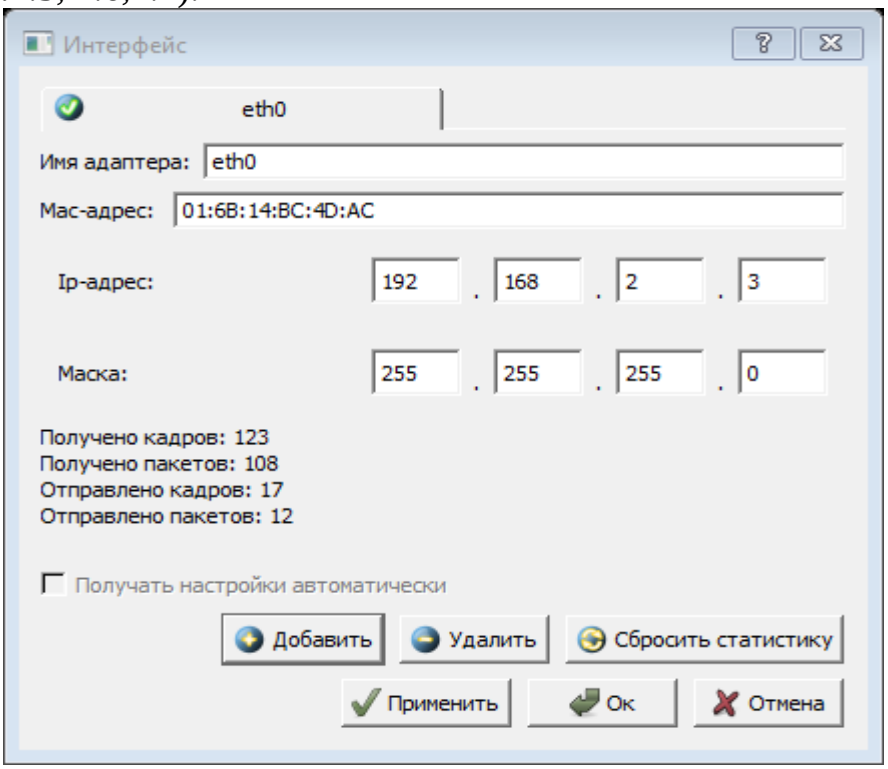
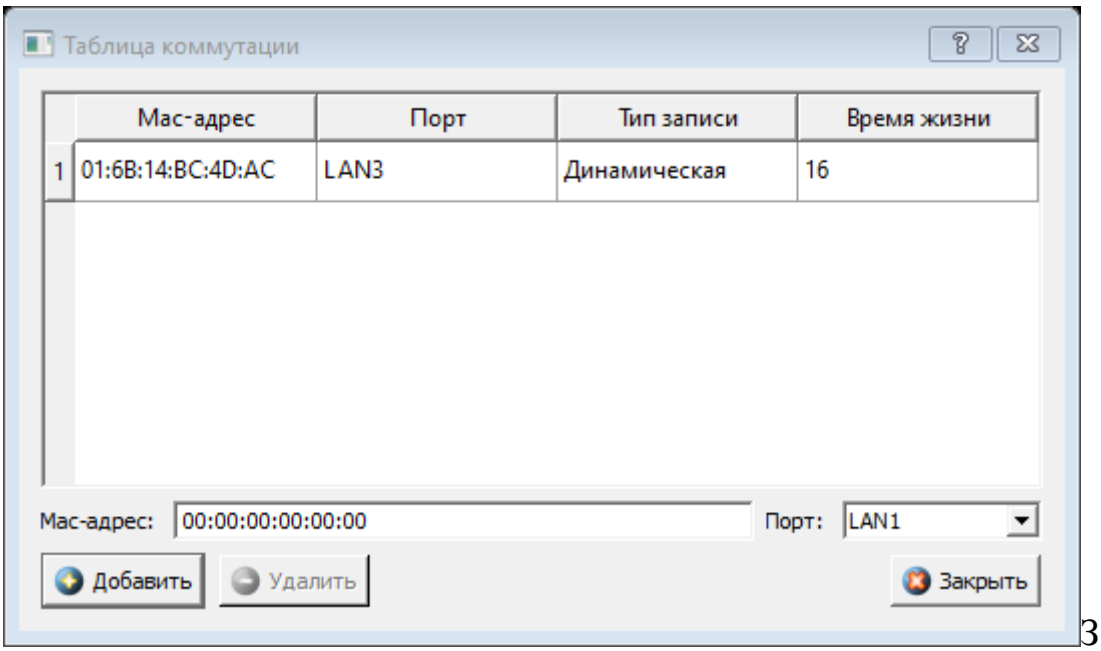


Рисунок 7.5



3

Рисунок 7.6

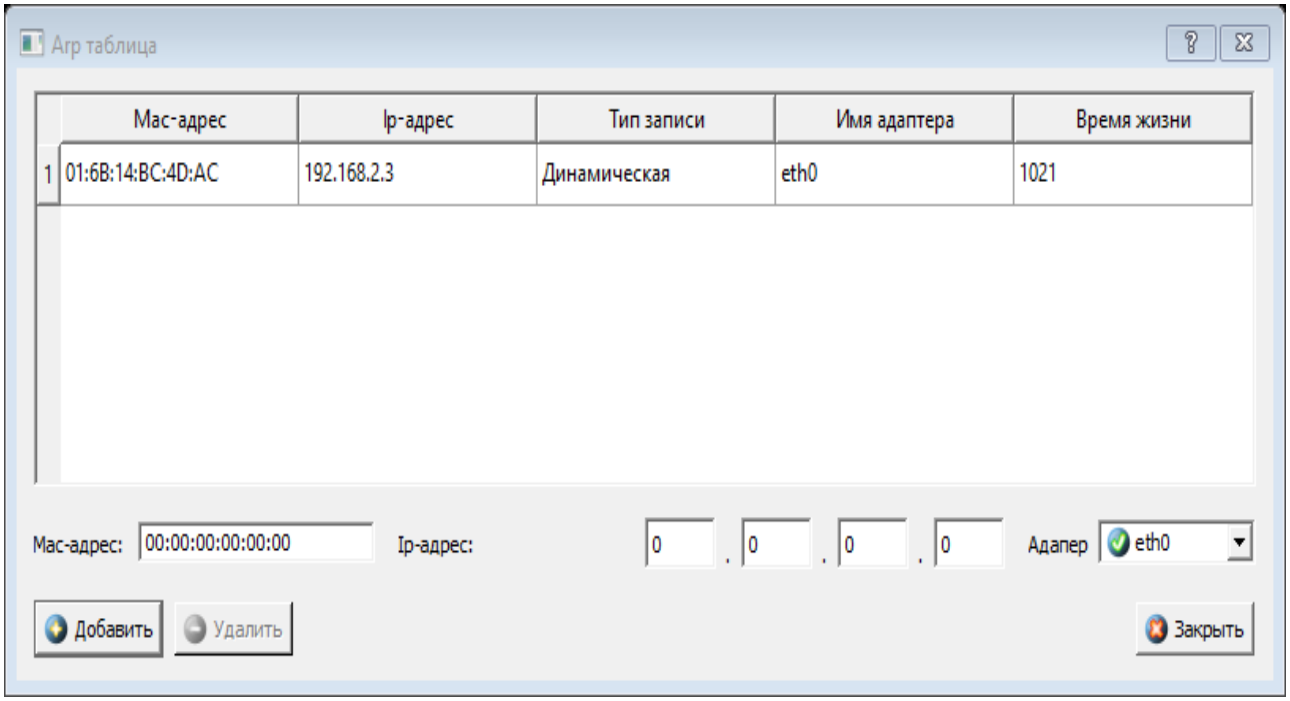


Рисунок 7.7

Нажимаем ПКМ на ПК2, выбираем конструктор пакетов, формируемый пакет для ПК 1 , указываем MAC– адрес отправителя и MAC–адрес получателя (рис.7.8), нажимаем вкладку Кадр, вписываем IP-адрес отправителя и IP-адрес получателя, отправляем UDP пакет (рис. 7.9). Проверяем куда доставлен пакет (хотя указаны адреса ПК1, пакет получает ПК3 (атакующий)) (рис.7.13). Принцип работы: атакующий меняет свой MAC–адрес на MAC адрес жертвы и получает пакеты, адресованные жертве.

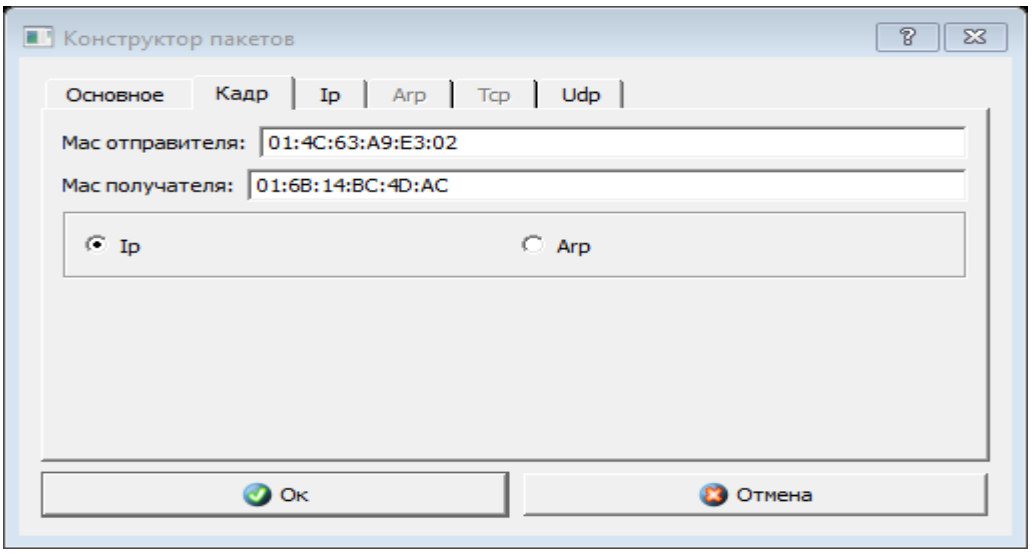


Рисунок 7.8

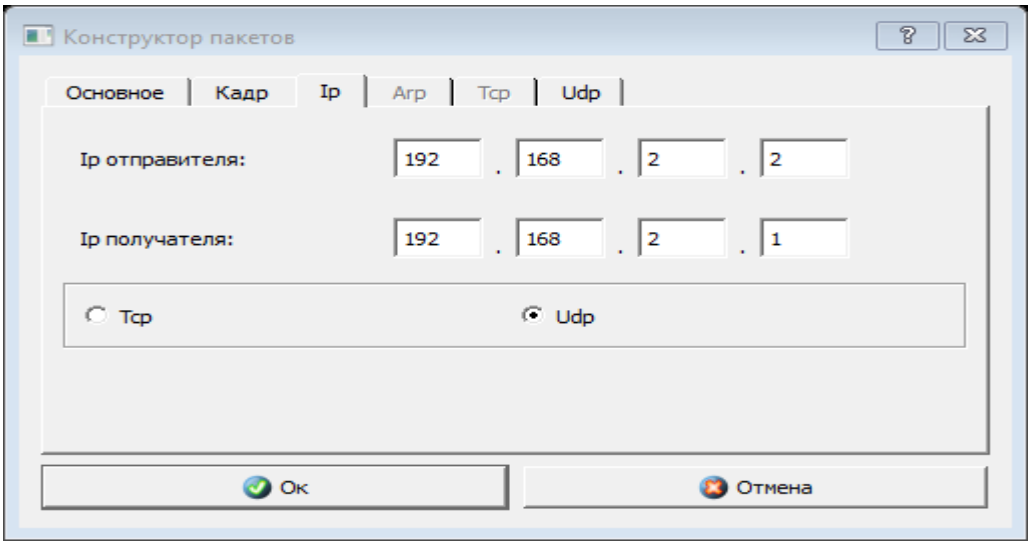


Рисунок 7.9

Задание 3.

1.Дана сеть 198. 160. 1. 0/24. Разбить на две подсети с маской /25 каждая.

2.Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис.7.10. В свойствах маршрутизатора необходимо указать количество интерфейсов, равное 2.

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. Настроить на компьютерах маршруты «по-умолчанию» (IP сети = 0.0.0.0; маска подсети = 0.0.0.0). Можно воспользоваться «Таблицей маршрутизации» либо вызвать свойства компьютера двойным щелчком, указать шлюз по умолчанию и включить маршрутизацию.

5. Включить маршрутизацию на маршрутизаторе.

6. Проверить работоспособность построенной модели ЛВС, передав

пакеты (TCP, 5 KB) от компьютера в левой подсети до компьютера в правой подсети.

7. Задать каждому компьютеру имя-описание, воспользовавшись пунктом контекстного меню «Задать описание».

8.Определить MAC-адреса с помощью ARP-запроса

10.Реализовать атаки ARP-спуфинг.

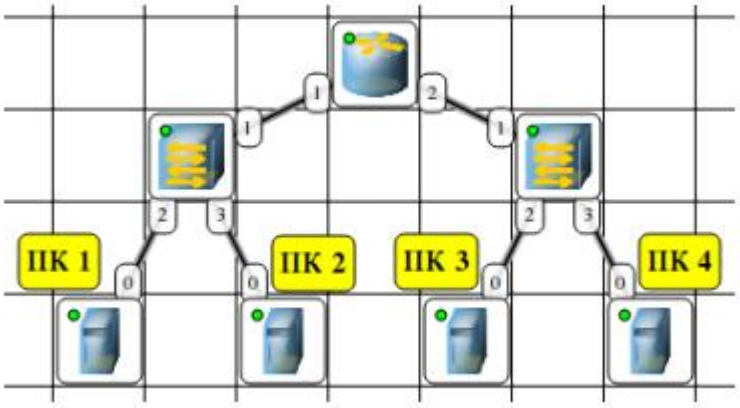


Рисунок 7.10

Содержание отчета:

1. Титульный лист.
2. Цель работы.
3. Разбиение заданной сети /27 на две подсети /28.
4. Схема модели с указанием IP-адресов устройств и номеров интерфейсов.
5. Скриншоты с результатами разрешения адреса и сетевой атаки.
6. По каждому пункту лабораторной должны быть приведены выводы по работе.

Контрольные вопросы:

1. Протокол ARP.
2. Формат пакета ARP.
3. Самопроизвольный ARP.
4. IP-адрес.
5. MAC-адрес.
6. ARP-спуфинг.

ЛАБОРАТОРНАЯ РАБОТА 8
Динамическая маршрутизация по протоколу RIP
Получение сетевых настроек по DHCP

Цель работы: Ознакомиться с механизмом динамической маршрутизации по протоколу RIP. Научиться настраивать компьютеры и серверы для автоматизации получения компьютерами сетевых настроек.

Маршрутизация – процесс определения в сети наилучшего пути, по которому пакет может достигнуть адресата. Динамическая маршрутизация может быть осуществлена с использованием одного и более протоколов (RIP v2, OSPF и др.).

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации заполняется и обновляется автоматически при помощи одного или нескольких протоколов маршрутизации (RIP, OSPF, EIGRP, BGP).

Каждый протокол маршрутизации использует свою систему оценки маршрутов (метрику). Маршрут к сетям назначения строится на основе таких критериев как количество ретрансляционных переходов пропускная способность канала связи задержки передачи данных и др.

Маршрутизаторы обмениваются друг с другом информацией о маршрутах с помощью служебных пакетов по протоколу UDP. Такой обмен информации увеличивает наличие дополнительного трафика в сети и нагрузку на эту сеть. Возможна также ситуация, при которой таблицы маршрутизации на роутерах не успевают согласоваться между собой, что может повлечь появление ошибочных маршрутов и потерю данных.

Протоколы маршрутизации делятся на три типа:

Дистанционно векторные протоколы (RIP)

Протоколы с отслеживанием состояния каналов (OSPF)

Смешанные протоколы (EIGRP)

И др.

Протокол RIP

RIP — протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути алгоритм Беллмана-Форда. Алгоритм маршрутизации RIP- один из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в сеть свою таблицу маршрутизации. Основное отличие протоколов в том, что RIPv2 (в отличие от RIPv1) может работать по мультикасту, то есть, рассылаясь на мультикаст адрес. Максимальное количество "хопов" (шагов до места назначения), разрешенное в RIP1, равно 15 (метрика 15). Ограничение в 15 хопов не дает применять RIP в больших сетях, поэтому протокол наиболее распространен в небольших компьютерных сетях. Вторая версия протокола — протокол RIP2 была разработана в 1994 году и является улучшенной версией первого. В этом протоколе повышена безопасность за счет введения дополнительной маршрутной информации. Принцип дистанционно-векторного протокола: каждый маршрутизатор, использующий протокол RIP периодически

широковещательно рассылает своим соседям специальный пакет-вектор, содержащий расстояния (измеряются в метрике) от данного маршрутизатора до всех известных ему сетей. Маршрутизатор получивший такой вектор, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет вектор информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный вектор маршрутизатор рассылает всем своим соседям. Маршрутизатор выбирает из нескольких альтернативных маршрутов маршрут с наименьшим значением метрики, а маршрутизатор, передавший информацию о таком маршруте помечается как следующий (next hop). Протокол непригоден для работы в больших сетях, так как засоряет сеть интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной информации о состоянии каналов и топологии сети. Сегодня даже в небольших сетях протокол вытесняется превосходящими его по возможностям протоколами EIGRP и OSPF.

Протокол DHCP означает Dynamic Host Configuration Protocol, что в переводе на русский язык означает «протокол динамической настройки узла». Благодаря этой технологии не требуется прописывать на каждом клиенте сетевые параметры, такие как:

IP-адрес;

Маска подсети;

Основной шлюз;

Адрес DNS-сервера.

Клиент (Client) – устройство, с которого происходит выход в интернет;

Сервер (Server) – устройство, предоставляющее возможность выхода в интернет для клиента.

DHCP выполняет всю работу по подбору сетевых настроек автоматически, без необходимости присваивать вручную каждому устройству свой IP-адрес. Это очень упрощает работу системного администратора в случае расширения сети.

Виды

Для выхода в интернет используется протокол IPv4. Для своей работы он применяет IP-адреса. IP у каждого компьютера в рамках одной сети должен быть уникальный.

Определение адресов может быть двух типов:

Статическое (распределение вручную) – IP каждому клиенту присваивается вручную администратором сети;

Динамическое (DHCP) – IP присваиваются автоматически исходя из заданных условий.

Принцип действия

Если то для чего нужен DHCP, понять довольно просто, то с принципом его работы нужно немного разобраться. Присвоение IP посредством DHCP выполняется в 4 действия:

Discover (Поиск сервера). Клиент, которому нужно получить сетевой адрес, отправляет сообщение на все компьютеры в сети с запросом на

присвоение ему IP. Для своей временной идентификации клиенту присваивается адрес 0.0.0.0;

Offer (Предложение сервера). Сервер получает запрос от клиента, анализирует его и, исходя из своих настроек, подбирает конфигурацию и отправляет её клиенту;

Request (Запрос). Получив предлагаемые настройки, клиент отправляет на адрес ответившего ему сервера запрос о предоставлении ему этих настроек;

Acknowledge (Подтверждение). Сервер получает запрос на уже конкретные настройки, предложенные ранее, создаёт привязку для клиента и отправляет ему их.

Ход работы:

Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 8.1.

Добавить возле каждой сети надпись с ее IP-адресом. Настроить IP-адреса и шлюзы компьютеров в каждой сети в соответствии с выбранным распределением.

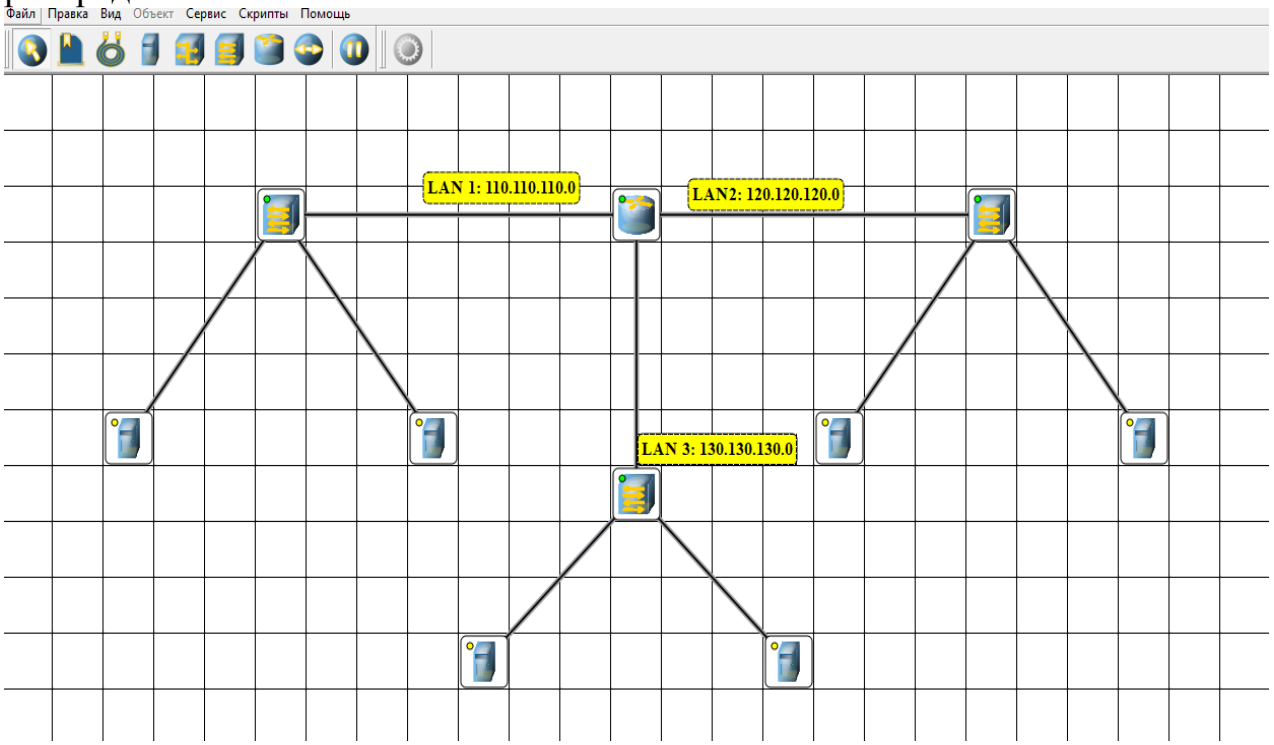


Рисунок 8.1 - Структура сети для знакомства с протоколом RIP

Настройка динамической маршрутизации по протоколу RIP.

1. На маршрутизаторе добавить и запустить программу RIP. Пункт контекстного меню «Программы». Кнопка «Добавить». Не забудьте поставить флаг для активации программы (рис. 8.2-8.4).

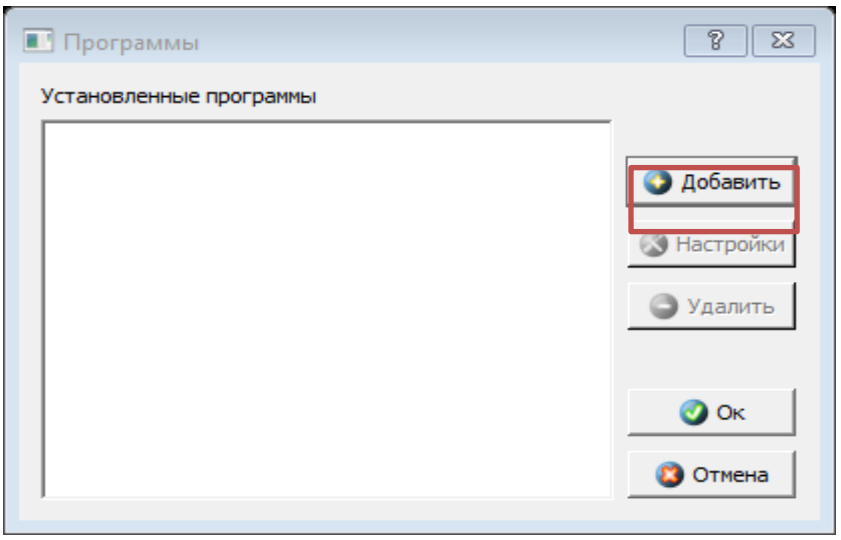


Рисунок 8.2

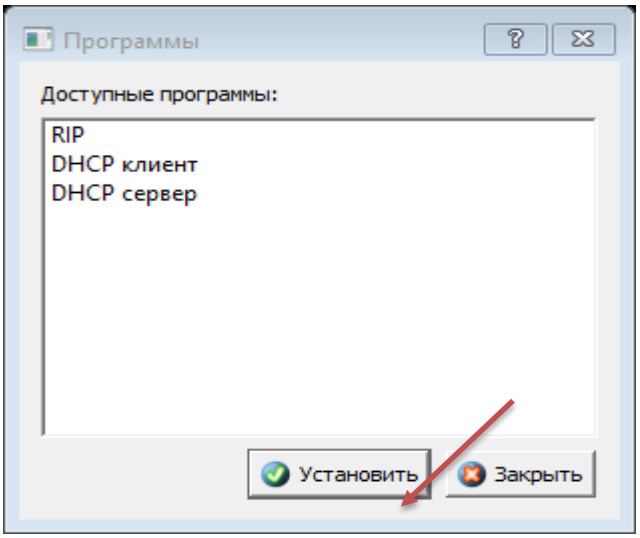


Рисунок 8.3

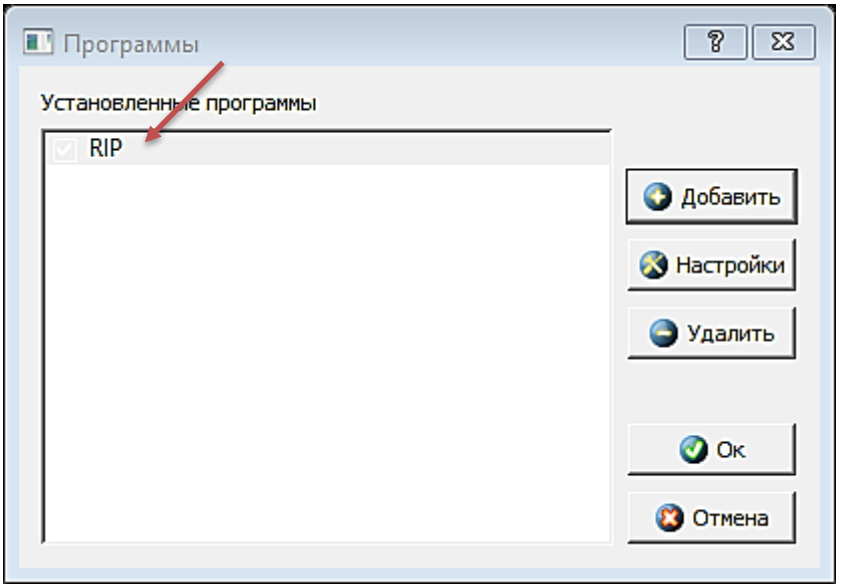


Рисунок 8.4

2. Включить маршрутизацию на маршрутизаторе
3. Просмотреть таблицу маршрутизации (рис.8.5)

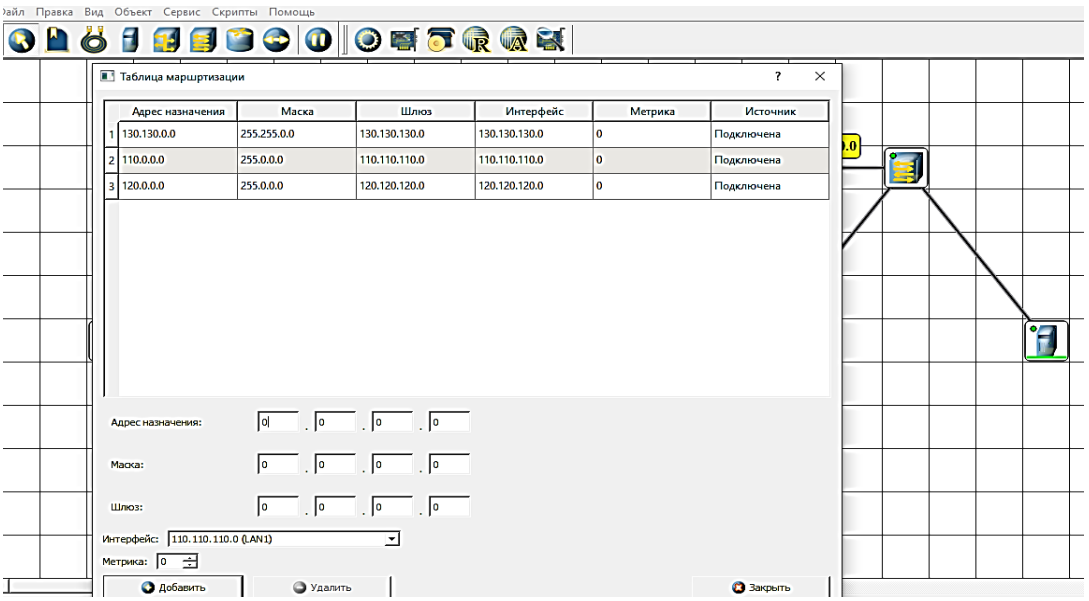


Рисунок 8.5

1. Отправить пакет UDP (рис.8.6, 8.7)

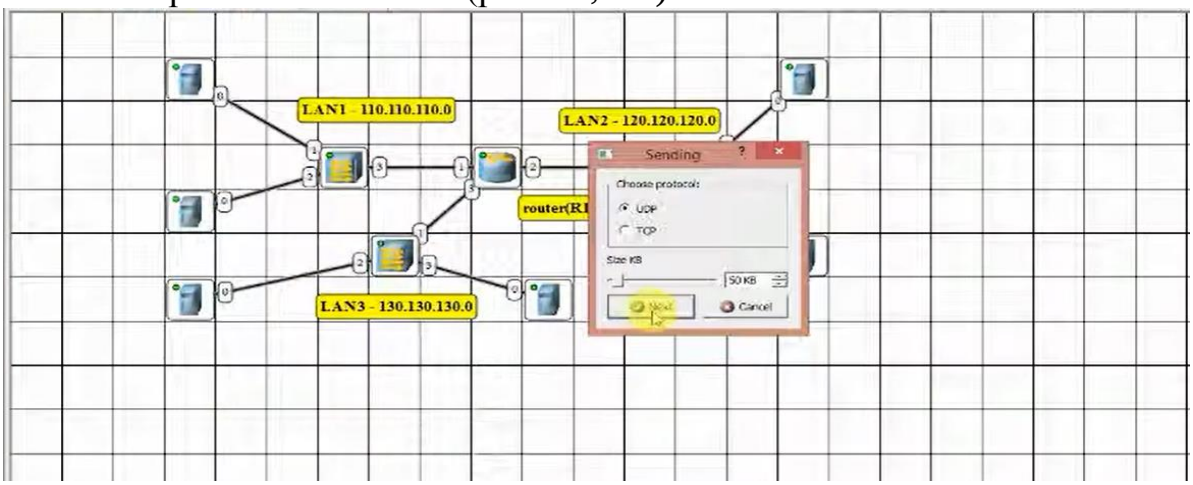


Рисунок 8.6

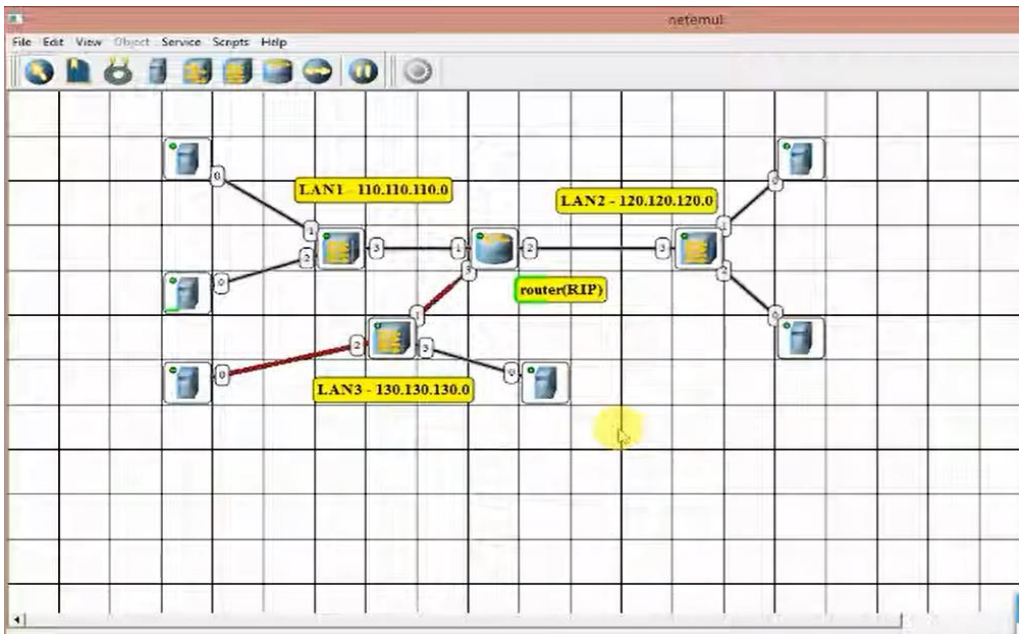


Рисунок 8.7

2. Открыть журнал маршрутизатора. Проследить за перемещением пакетов протокола RIP по сети.

3. Открыть таблицы маршрутизации компьютеров и убедиться, что таблицы заполнились.

4. Отправить пакет TCP. Проследить за перемещением пакетов протокола RIP по сети.

5. Сделать вывод об отличиях передачи пакетов по протоколу UDP и TCP.

Настройка автоматического получения сетевых настроек по протоколу DHCP.

1. На маршрутизаторе, добавить и запустить программу DHCP-сервер. Не забудьте поставить флаг для активациипрограммы рис.8.8).

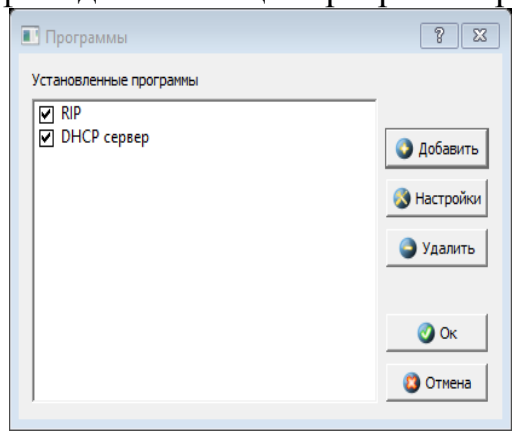


Рисунок 8.8

2. В настройках DHCP-сервера указать интерфейс, LAN1,2 3, тип адресов — динамические, диапазон адресов, выделяемых для динамической адресации, маску подсети и IP-адрес шлюза (рис.8.9).

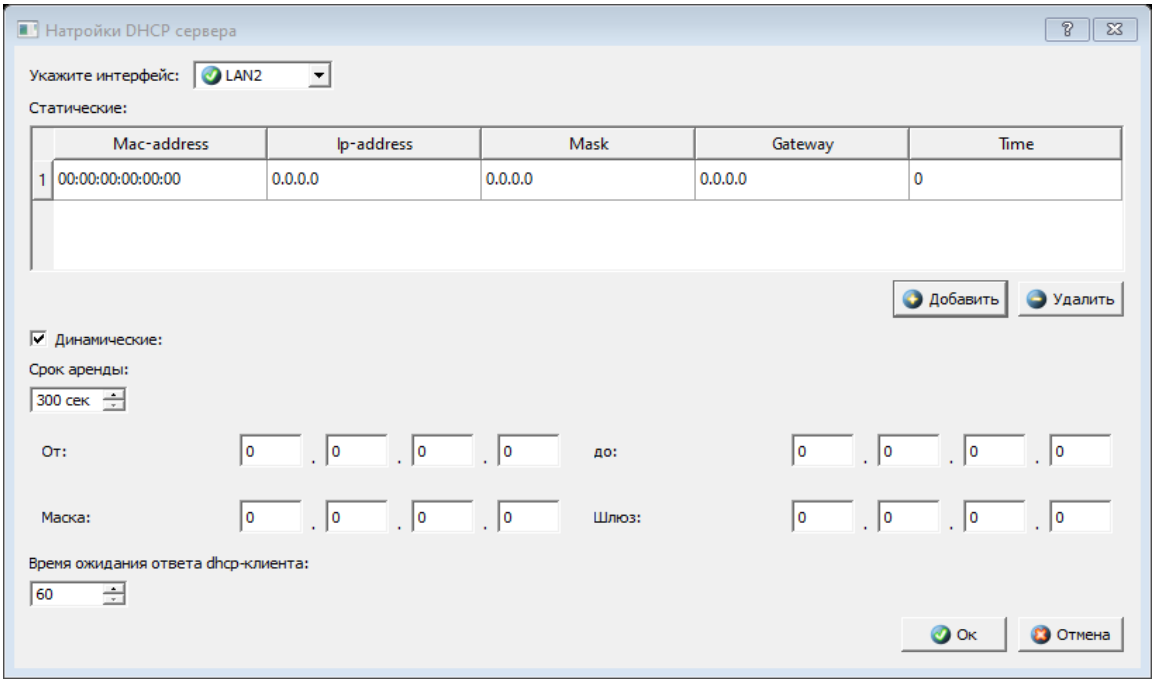


Рисунок 8.9

3. На каждом компьютере добавить и запустить программу DHCP-клиент.Не забудьте поставить флаг для активации программы (рис.8.10).

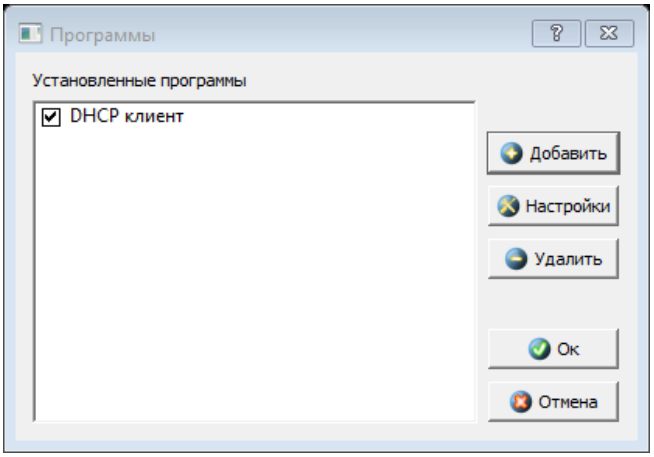


Рисунок 8.10

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

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

6. Дождаться, пока все компьютеры не получат сетевые настройки.

7. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) между компьютерами в разных подсетях.

Содержание отчета:

1. Титульный лист.
2. Цель работы.
3. Схема модели с указанием IP-адресов устройств и номеров интерфейсов.
4. По каждому пункту лабораторной должны быть приведены выводы поработе.

Контрольные вопросы:

1. Протокол RIP.
2. Протокол DHCP.

ВОПРОСЫ К ЭКЗАМЕНУ

1. IP-адреса. Маска подсети
2. TCP/IP. Протоколы управления. Адресация в Internet.
3. Адресация узлов в компьютерных сетях
4. Амплитудный, частотный и фазовый методы модуляции аналогового сигнала.
5. Аналоговые каналы передачи данных. Способы модуляции.
6. Виртуализация вычислительных процессов и системы терминального доступа. FTP, POP3, SMTP и другие протоколы обмена
7. Канальный уровень взаимодействия
8. Классификация вычислительных сетей
9. Классификация информационно-аналитических сетей
10. Сетевой уровень взаимодействия
11. Классы сетей
12. Клиент, сервер. Физическая и логическая сущности сервера.
13. Коммутация каналов, сообщений, пакетов.
14. Корпоративные сети. Организация взаимодействия клиентской части с сетевым приложением: сокеты.
15. Линии связи
16. Локальная сеть организации на основе Fast Ethernet
17. Локальные вычислительные сети. Методы доступа. Множественный доступ с контролем несущей и обнаружение конфликтов.
18. Локальные, региональные и глобальные сети.
19. Межсетевое взаимодействие. IP-адрес, маска, маршрутизация. Функции и протоколы сетевого уровня.
20. Методы доступа к среде передачи данных: MAC-адрес.
21. Модель OSI
22. Модемы. Цифровые каналы передачи данных
23. Общая идеология технологии Ethernet
24. Одноранговые сети и сети с выделенным сервером
25. Основные программные и аппаратные компоненты сети
26. Основы сетей передачи данных
27. Особенности организации сетевых операционных систем. Распределённые вычисления.
28. Особенности технологии Frame Relay, ATM, SDH.
29. Понятие и функции хаба (концентратора).
30. Понятие интерфейса и протокола.
31. Понятие линии, канала, частотной характеристики линии.
32. Понятия «клиент» и «сервер»
33. Преимущества использования компьютерных сетей
34. Принципы Web- технологии, средства разработки
35. Разновидности сети Ethernet. Маркерные методы доступа. Сети Token

Ring и FDDI. Высокоскоростные локальные сети.

36. Режимы передачи данных
37. Сетевые операционные системы. Технологии распределённых вычислений
38. Сетевое оборудование
39. Протоколы файлового обмена, электронной почты, дистанционного управления. Разделение каналов по времени и частоте, кодовое разделение
40. Сетевые приложения
41. Сети Ethernet, Token Ring, FDDI X25, ATM.
42. Спецификации Ethernet по физической среде передачи
43. Способы коммутации. Одноранговые сети и сети с выделенным сервером.
44. Стандартизация протоколов локальных сетей
45. Стандарты компьютерных сетей
46. Технологии глобальных сетей
47. Технологии канального и сетевого уровней
48. Технологии физического уровня
49. Топология компьютерных сетей
50. Уровни и протоколы. Эталонная модель взаимосвязи открытых систем.
51. Уровни модели OSI
52. Формирование подсетей
53. Функции и протоколы канального уровня. Сегментация сети: мосты, коммутаторы.
54. Характеристики линий связи
55. Характеристики проводных линий связи. Спутниковые каналы.
56. Эволюция вычислительных систем
57. Локальная сеть организации. Исполнение структурированных кабельных систем
58. Локальная сеть организации. Технология PoE (Power over Ethernet) Логическое структурирование локальной сети организации
59. Локальная сеть организации. Типовая физическая структура сети предприятия
60. Локальная сеть организации. Логическая структура локальной сети
61. Виртуальные сети (VLAN). Управляемые коммутаторы с поддержкой VLAN.
62. Система выделенных серверов организации. Выделенные серверы
63. Система выделенных серверов организации. Функции выделенного сервера
64. Система выделенных серверов организации. Аппаратная реализация выделенного сервера
65. Система выделенных серверов организации. Размещение выделенных серверов организации

СПИСОК КОМПЬЮТЕРНЫХ ПРОГРАММ

1. Симулятор ЛВС NETEMUL.

СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Буцык, С.В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]: учебное пособие по дисциплине «Вычислительные системы, сети и телекоммуникации» для студентов, обучающихся по направлению 09.03.03 Прикладная информатика (уровень бакалавриата)/ С.В. Буцык, А.С. Крестников, А.А. Рузаков. — Электрон. текстовые данные. — Челябинск: Челябинский государственный институт культуры, 2016. — 116 с. — 978-5-94839-537-1. — Режим доступа:http://www.iprbookshop.ru/56399.html

2. Галас, В.П. Вычислительные системы, сети и телекоммуникации. Часть 2. Сети и телекоммуникации [Электронный ресурс]: электронный учебник/ В.П. Галас. — Электрон. текстовые данные. — Владимир: Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 311 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57364.html

3. Галас, В.П. Вычислительные системы, сети и телекоммуникации. Часть 1. Вычислительные системы [Электронный ресурс]: электронный учебник/ В.П. Галас. — Электрон. текстовые данные. — Владимир: Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 232 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57363.html

4. Чекмарев, Ю.В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]/ Ю.В. Чекмарев. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 184 с. — 978-5-4488-0071-9. — Режим доступа:http://www.iprbookshop.ru/63576.html

Дополнительная литература

1. Антонова, Г.М. Современные средства ЭВМ и телекоммуникаций [Текст]: учеб. пособиедля студ. высш. уч. зав/ Г.М. Антонова, А.Ю. Байков.- М.: Академия, 2010.- 144 с

2. Зиангирова, Л.Ф. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]: учебно-методическое пособие/ Л.Ф. Зиангирова. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2015. — 150 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/31942.html

3. Степанов, А.Н. Архитектура вычислительных систем и компьютерных сетей [Текст]: учеб. пособие/ А.Н.Степанов.- СПб: Питер, 2007.- 493 с.

4. Щербакова, Т.Ф. Вычислительная техника и информационные технологии [Текст]: учеб. пособие для студ. учреждений высш. профобразования/ Т.Ф. Щербаков, С.В. Козлов, А.А. Коробков.- М.: Академия, 2012.- 304 с.

Методическая литература

Учебно-методическое пособие для лабораторных работ по дисциплине «Вычислительныесистемы, сети и телекоммуникации по направлению 09.03.03

Прикладная информатика /В.П. Рядченко, З.Б. Батчаева – БИЦ СевКавГГТА, 2018.

БИДЖИЕВА Сапият Ханапиевна
РЯДЧЕНКО Виктор Петрович

ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ, СИСТЕМЫ И ТЕЛЕКОММУНИКАЦИИ

Лабораторный практикум
для обучающихся 1 курса по направлению подготовки
09.03.03. Прикладная информатика

Корректор Чагова О.Х.
Редактор Чагова О.Х.

Сдано в набор 13.09.2023г.
Формат 60х84/16
Бумага офсетная
Печать офсетная
Усл. печ. 4,18
Заказ № 4783
Тираж 100 экз.

Оригинал макет подготовлен
В библиотечно-издательском центре СКГА
369000, г. Черкесск, ул. Ставропольская, 36