Методические рекомендации по дисциплине

«Аппаратные средства компьютерных сетей»

ЗАДАЧИ

1. Монтаж локальной сети

1. Рассчитать количество необходимого оборудования для создания локальной сети в компьютерном классе (15 компьютеров) на витой паре. Расстояние между компьютерами 2 метра, компьютеры расположены П-образно вдоль стены. Нарисовать план оптимального расположения компьютеров и оборудования.

2. Рассчитать количество необходимого оборудования для создания локальной сети в компьютерном классе (15 компьютеров) на коаксиальном кабеле. Расстояние между компьютерами 2 метра, компьютеры расположены П-образно вдоль стены. Нарисовать план оптимального расположения компьютеров и оборудования.

3. Рассчитать количество необходимого оборудования для создания локальной сети в 2 компьютерных классах (по 18 компьютеров в классе) и сервера (расположен в серверной) на витой паре. Расстояние между компьютерами 2 метра, компьютеры расположены П-образно вдоль стены, расстояние между классами 10 метров расстояние до серверной от первого класса 5 метров. Нарисовать план оптимального расположения компьютеров и оборудования.

4. Рассчитать количество необходимого оборудования для создания локальной сети в 2 компьютерных классах (по 18 компьютеров в классе) и сервера (расположен в серверной) на коаксиальном кабеле. Расстояние между компьютерами 2 метра, компьютеры расположены П-образно вдоль стены, расстояние между классами 10 метров расстояние до сервер-

ной от первого класса 5 метров. Нарисовать план оптимального расположения компьютеров и оборудования.

5. Перечислить необходимое оборудование и провести монтаж кабеля на витой паре.

6. Перечислить необходимое оборудование и провести монтаж кабеля на коаксиальном кабеле.

7. Перечислить преимущества и недостатки сетей на основе:
   а) витой пары;
   б) коаксиального кабеля.

8. Рассчитайте значение PDV и PVV для следующей сети и определите будет ли она работоспособна:

Левый сегмент 1:	10Base-T	100 м
Промежуточный сегмент 2:	10Base-2	180 м
Промежуточный сегмент 3:	10Base-FB	500 м
Промежуточный сегмент 4:	10Base-FB	500 м
Промежуточный сегмент 5:	10Base-FB	500 м
Правый сегмент 6:	10Base-T	100 м

9. Рассчитайте значение PDV и PVV для следующей сети и определите будет ли она работоспособна:

Левый сегмент 1:	10Base-T	100 м
Промежуточный сегмент 2:	10Base-2	180 м
Промежуточный сегмент 3:	10Base-FL	1000 м
Промежуточный сегмент 4:	10Base-FB	500 м
Промежуточный сегмент 5:	10Base-FB	500 м
Правый сегмент 6:	10Base-2	150 м

2. Настройка локальной сети

1. Сеть на основе протокола IPX/SPX. Настроить сетевые карты компьютеров следующим образом:
   - установить протокол IPX/SPX
   - задать имя компьютера ST1 … ST12 (каждый студент задает тот номер, на каком компьютере сидит)
   - задать имя рабочей группы Students
   - проверить работоспособность сети

2. Сеть на основе протокола TCP/IP. Настроить сетевые карты компьютеров следующим образом:
   - установить протокол TCP/IP
   - задать сетевой адрес 192.168.20.1 … 12 (каждый студент задает тот номер, на каком компьютере сидит)
   - задать сетевую маску соответствующую данной сети
   - задать имя компьютера ST1 … ST12 (каждый студент задает тот номер, на каком компьютере сидит)
   - задать имя рабочей группы Students
   - проверить работоспособность сети

3. Настройка доступа к папкам, файлам и периферийным устройствам:
   - Создать с помощью программы «управление компьютером» группу пользователей Ученики
   - Создать с помощью программы «управление компьютером» группу пользователей Учителя
   - Создать четырех пользователей Учитель1, Учитель2, Ученик1, Ученик2
   - создать для каждого пользователя свою папку
   - настроить разрешения доступа для каждой папки (владелец папки имеет полный доступ, Учителя могут просматривать и изменять папки учеников, и просматривать папки друг друга, без права изменения, а учение могут только просматривать папки друг-друга, к папкам учителей для них доступ закрыт)

- сделать папки всех пользователей сетевыми
- установить принтер и сделать его сетевым
- настроить уровень доступа к принтеру (принтером могут пользоваться только учителя)

4. Сеть на основе протокола TCP/IP. Настроить сетевые карты компьютеров следующим образом:
   - установить протокол TCP/IP
   - задать сетевой адрес 192.168.10.1 … 12 (каждый студент задает тот номер, на каком компьютере сидит)
   - задать сетевую маску соответствующую данной сети
   - задать имя компьютера ST1 … ST12 (каждый студент задает тот номер, на каком компьютере сидит)
   - подключить компьютер к домену NetASPU
   - проверить работоспособность сети

3. Работа в сети Интернет

1. Настройте браузер следующим образом:
   - запуск начинается с пустой странице
   - запретить отображение изображений
   - запретить воспроизведение анимации
   - запретить воспроизведение видео
   - запретить воспроизведение звуки
   - настроить прокси-сервер 192.168.100.254 порт 3128

2. Настройте браузер следующим образом:
   - запуск начинается со страницы www.rambler.ru
   - разрешить отображение изображений
   - запретить воспроизведение анимации
   - запретить воспроизведение видео
   - разрешить воспроизведение звуки
   - настроить прокси-сервер 192.168.100.254 порт 3128

3. Создайте в папке «избранное» папку «поисковик» и поместите туда адреса 3 известных вам поисковых систем

4. Создайте в папке «избранное» папку «почта» и поместите туда адреса 3 известных вам бесплатных почтовых серверов

5. Создайте в папке «избранное» папку «инфо» и поместите туда адреса 3 известных вам информационных серверов

6. Создайте в папке «избранное» папку «download» и поместите туда адреса 3 известных вам файловых серверов

7. Используя поисковую систему, найдите сервера, где можно просмотреть прогноз погоды.

8. Используя поисковую систему, найдите информацию, указанную преподавателем

9. Зайдите на сайт GisMeteo.ru и просмотрите прогноз погоды в Армавире на 10 дней. Результат сохраните в папку «отчет»

10. Зайдите на сайт GisMeteo.ru и просмотрите прогноз погоды в Армавире на 3 дня. Результат сохраните в папку «отчет»

11. Зайдите на сайт www.hmn.ru и просмотрите прогноз погоды в Армавире на 5 дней. Результат сохраните в папку «отчет» в формате Web-архива.

12. Зайдите на сайт www.hmn.ru и просмотрите прогноз погоды в Армавире на 14 дней. Результат сохраните в папку «отчет» в формате Web-архива.

13. Зайдите на сайт www.hmn.ru и просмотрите прогноз погоды в Армавире на 3 дня. Результат сохраните в папку «отчет» в формате Web-архива. Запакуйте этот файл под именем погода_номер_компьютера.zip и разместите его для скачивания на сайте www2.webfile.ru и передайте номер файла для скачивания преподавателю.

14. Зайдите на сайт www2.webfile.ru и скачайте файл номер которого вам дал преподаватель

15. Создайте файл с описанием стандарта 10Base-5. И передать его по FTP на сервер.

16. Создайте файл с описанием стандарта 10Base-2. И передать его по FTP на сервер.

17. Создайте файл с описанием стандарта 10Base-T. И передать его по FTP на сервер.

18. Загрузить файл find.txt. с сервера. Выполнить поиск информации заданной в файле find.txt.

19. Создать почтовый ящик на бесплатном сервере.

20. Настроить программу OutLook Express для работы с заданным почтовым ящиком

21. Создать файл, в котором описать алгоритм монтажа коаксиального кабеля и переслать его на указанный преподавателем почтовый ящик.

22. Получить письмо, от преподавателя и выполнить задание из файла, прикрепленного к письму.

ПРИЛОЖЕНИЯ

Приложение 1

Монтаж коаксиального кабеля и кабеля на основе витой пары

1. Монтаж коаксиального кабеля

Для подключения кабеля используются разъемы BNC (bayonet nut connector), устанавливаемые собственно на кабель, и Т-коннекторы, служащие для отвода сигнала от кабеля в сетевую плату. Разъемы типа BNC бывают обжимные и разборные (пример разборного разъема — отечественный разъем СР-50-74Ф). На концах сети устанавливаются 50-омные терминаторы.

Для монтажа сети из N компьютеров необходимо:

1. Т-коннекторов – N шт.
2. BNC-коннекторов – 2*N-2 шт.
3. Терминаторов – 2 шт.
4. Кабель необходимой длины

Для монтажа разъема на кабель вам потребуется либо специальный инструмент для обжимки, либо паяльник и плоскогубцы.

Последовательность монтажа

1. Аккуратно отрежьте так, чтобы его торец был ровным. Наденьте на кабель металлическую муфту, который поставляется в комплекте с BNC-разъемом.
2. Снимите с кабеля внешнюю пластиковую оболочку на длину примерно 20 мм. Будьте аккуратны, чтобы не повредить по возможности ни один проводник оплетки.
3. Оплетку аккуратно расплетите и разведите в стороны. Снимите изоляцию с центрального проводника на длину примерно 5 мм.
4. Установите центральный проводник в штырек, который также поставляется в комплекте с разъемом BNC. Используя

специальный инструмент, надежно обожмите штырек, фиксируя в нем проводник, либо впаяйте проводник в штырек. При пайке будьте особенно аккуратны и внимательны — плохая пайка через некоторое время станет причиной отказов в работе сети, причем локализовать это место будет достаточно трудно.

5. Вставьте центральный проводник с установленным на него штырьком в тело разъема до щелчка. Щелчок означает, что штырек сел на свое место в разъеме и зафиксировался там.
6. Равномерно распределите проводники оплетки по поверхности разъема, если необходимо, обрежьте их до нужной длины. Надвиньте на разъем металлическую муфту.
7. Специальным инструментом (или плоскогубцами) аккуратно обожмите муфту до обеспечения надежного контакта оплетки с разъемом. Не обжимайте слишком сильно — можно повредить разъем или пережать изоляцию центрального проводника. Последнее может привести к неустойчивой работе всей сети. Но и обжимать слишком слабо тоже нельзя — плохой контакт оплетки кабеля с разъемом также приведет к отказам в работе.

2. Монтаж кабеля на основе витой пары

Витая пара (UTP, unshielded twisted pair) в настоящее время является наиболее распространенной средой передачи сигналов в локальных сетях. Кабели UTP используются в сетях Ethernet, Token Ring и ARCnet. Они различаются по категориям (в зависимости от полосы пропускания) и типу проводников (гибкие или одножильные). Для монтажа сетей используют кабель 4-й или 5-й категории. (В кабеле как правило, находится восемь проводников, перевитых попарно)

Для соединения кабеля с сетевой платой и концентратором используют разъем RJ-45 (восьмиконтактный разъем).

Для монтажа сети из N компьютеров необходимо:

1. Разъем RJ-45 – 2*N шт.
2. Концентраторы (в зависимости от количества портов и количества компьютеров)
3. Кабель необходимой длины

Для монтажа разъема на кабель вам потребуется либо специальный инструмент.

Последовательность монтажа

1. Аккуратно обрежьте конец кабеля. Торец кабеля должен быть ровным.
2. Используя специальный инструмент, снимите с кабеля внешнюю изоляцию на длину примерно 25 мм и обрежьте нить, вмонтированную в кабель (нить предназначена для удобства снятия изоляции с кабеля на большую длину). Любые повреждения (надрезы) изоляции проводников абсолютно недопустимы — именно поэтому желательно использовать специальный инструмент, лезвие резака которого выступает ровно на толщину внешней изоляции.
3. Аккуратно разведите, расплетите и выровняйте проводники. Выровняйте их в один ряд, при этом соблюдая цветовую маркировку. Существует два наиболее распространенных стандарта по разводке цветов по парам: T568A (рекомендуемый компанией Siemon) и T568B (рекомендуемый компанией AT&T и фактически наиболее часто применяемый).

Номер пары	Цвет по T586A	Цвет по T586B
1	синяя	синяя
2	оранжевая	зеленая
3	зеленая	оранжевая
4	коричневая	коричневая

На разъеме RJ-45 цвета проводников располагаются так (слева направо):

Раскладка T568A		**B**	
Цвет: основной / полоски	Пара	Цвет: основной / полоски	Пара
бело-зеленый	3	бело-оранжевый	2
зеленый	3	оранжевый	2
бело-оранжевый	2	бело-зеленый	3
синий	1	синий	1
бело-синий	1	бело-синий	1
оранжевый	2	зеленый	3
бело-коричневый	4	бело-коричневый	4
коричневый	4	коричневый	4

Примечание: *Для обжима «прямого» кабеля, иначе говоря «патч корда» (patch cord) используются раскладки одного типа, т.е. T568A или T568B – на обоих концах.*

Для обжима «кроссовера» (crossover) - для соединения 2-х компьютеров или свитчей напрямую – используют раскладки обоих типов на одном проводе, т.е. T568A на одном конце и T568B на другом.

Проводники должны располагаться строго в один ряд, без нахлестов друг на друга. Удерживая их одной рукой, другой ровно обрежьте проводники так, чтобы они выступали над внешней обмоткой на 8-10 мм.

4. Держа разъем защелкой вниз, вставьте в него кабель. Каждый проводник должен попасть на свое место в разъеме и упереться в ограничитель. Прежде чем обжимать разъем,

убедитесь, что вы не ошиблись в разводке проводников. При неправильной разводке помимо отсутствия соответствия номерам контактов на концах кабеля, легко выявляемого с помощью простейшего тестера, возможна более неприятная вещь — появление “разбитых пар” (splitted pairs).

5. Для выявления этого брака обычного тестера недостаточно, так как электрический контакт между соответствующими контактами на концах кабеля обеспечивается и с виду все как будто бы нормально. Но такой кабель никогда не сможет обеспечить нормальное качество соединения даже в 10-мегабитной сети на расстояние более 40-50 метров. Поэтому нужно быть внимательным и не торопиться, особенно если у вас нет достаточного опыта.
6. Вставьте разъем в гнездо на обжимочном приспособлении и обожмите его до упора-ограничителя на приспособлении. В результате фиксатор на разъеме встанет на свое место, удерживая кабель в разъеме неподвижным. Контактные ножи разъема врежутся каждый в свой проводник, обеспечивая надежный контакт.

Приложение 2

Основные ограничения и параметры спецификаций физического уровня для стандарта Ethernet

Таблица 1. Общие ограничения для всех стандартов Ethernet

Номинальная пропускная способность	10 Мбит/с
Максимальное число станций в сети	1024
Максимальное расстояние между узлами в сети	2500 м (в 10Base-FB 2750м)
Максимальное число коаксиальных сегментов в сети	5

Таблица 2. Параметры спецификаций физического уровня для стандарта Ethernet

	10Base-5	**10Base-2**	**10Base-T**	**10Base-F**
Кабель	Толстый коаксиальный кабель RG-8 или RG-11	Тонкий коаксиальный кабель RG-58	Неэкранированная витая пара категорий 3, 4, 5	Многомодовый волоконно-оптический кабель
Максимальная длина сегмента, м	500	185	100	2000
Максимальное расстояние между узлами сети (при использовании повторителей), м	2500	925	500	2500 (2740 для 10Base-FB)
Максимальное число станций в сегменте	100	30	1024	1024
Максимальное число повторителей между любыми станциями сети	4	4	4	4 (5 для 10 Base-FB)

Приложение 3

Данные о задержках, вносимых повторителями и различными средами передачи данных, для самостоятельного

расчета максимального количества повторителей и максимальной общей длины сети

Чтобы сеть Ethernet, состоящая из сегментов различной физической природы, работала корректно, необходимо выполнение четырех основных условий:

- количество станций в сети не более 1024;
- максимальная длина каждого физического сегмента не более величины, определенной в соответствующем стандарте физического уровня;
- время двойного оборота сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети не более 575 битовых интервала;
- сокращение межкадрового интервала IPG (Path Variability Value, PVV) при прохождении последовательности кадров через все повторители должно быть не больше, чем 49 битовых интервала.

Соблюдение этих требований обеспечивает корректность работы сети даже в случаях, когда нарушаются простые правила конфигурирования, определяющие максимальное количество повторителей и общую длину сети в 2500 м.

Таблица 1. Данные для расчета значения PDV

Тип сегмента	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1 м, bt	Максимальная длина сегмента, м
10 Base-5	11,8	46,5	169,5	0,0866	500
10 Base-2	11,8	46,5	169,5	0,1026	185
10 Base-T	15,3	42,0	165,0	0,113	100
10 Base-FB	—	24,0	—	0,1	2000

В таблице используются также такие понятия, как **левый сегмент**, **правый сегмент** и **промежуточный сегмент**.

Левым сегментом называется сегмент, в котором начинается путь сигнала от выхода передатчика конечного узла.

Промежуточный сегмент – сегмент, через который проходит сигнал.

Правый сегмент – наиболее удаленный сегмент (конечный).

Таблица 2. Сокращение межкадрового интервала повторителями

Тип сегмента	Передающий сегмент, bt	Промежуточный сегмент. bt
10Base-5 или 10Base-2	16	11
10Base-FB	—	2
10Base-FL	10,5	8
10Base-T	10,5	8

Приложение 4

Настройка сетевого оборудования

Для настройки сетевого оборудования необходимо:

1. Установить драйвера для сетевой карты, если они не были загружены при установке системы

2. На всех компьютерах установить одинаковый сетевой протокол (например, TCP/IP, IPX/SPX, NetBEUI) ***при установке драйверов сетевой карты по умолчанию устанавливается протокол TCP/IP***

3. Настроить протокол TCP/IP

4. Присвоить каждому компьютеру свое имя и настроить тип сети «Рабочая группа» или «Домен».

5. Настроить доступ к ресурсам компьютера.

1. Для установки драйверов необходимо:

- вставить диск в дисковод или CD-ROM
- открыть в меню «Пуск» «Настройка»-«Панель управления»-«Система»-«Оборудование»-«Мастер оборудования»
- выполнить установку оборудования отвечая на запросы «Мастера оборудования»

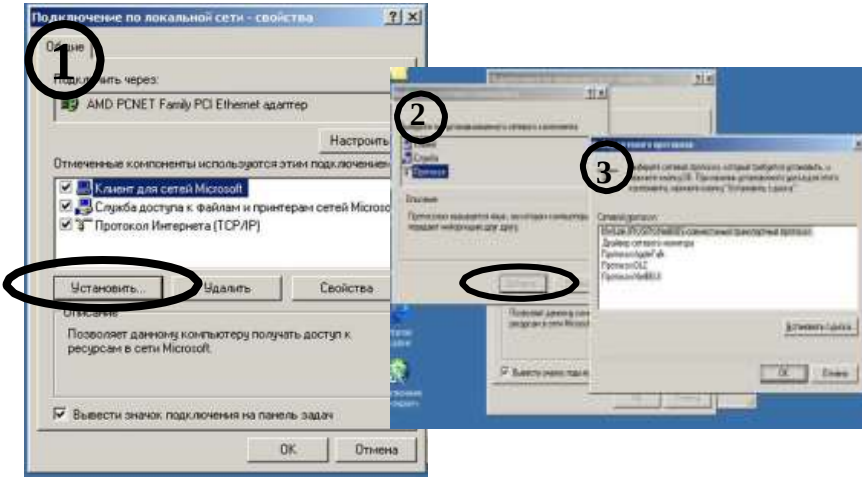
2. Для установки сетевого протокола необходимо:

- открыть в меню «**Пуск**» «**Настройка**»-«**Панель управления**»-«**Сеть и удаленный доступ к сети**», щелкнуть по «**Подключение по локальной сети**» правой кнопкой мыши и выбрать свойства

• в появившемся окне **1** нажать на кнопку «**Установить**» для добавления нового клиента, службы, протокола

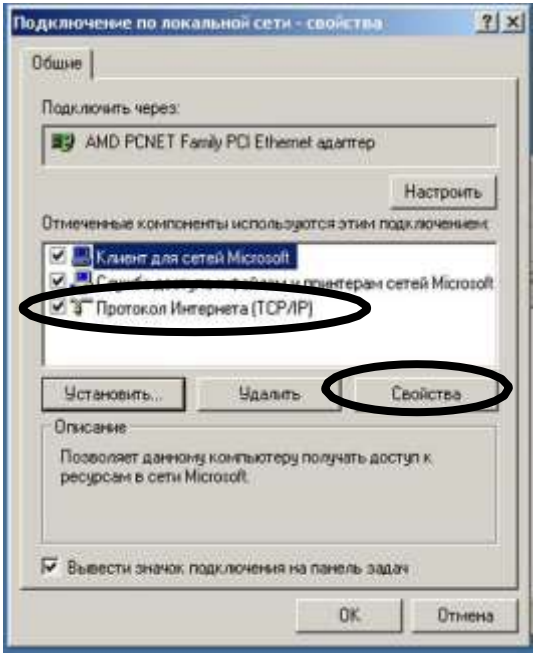
• в появившемся окне **2** выбрать, что будем устанавливать и нажать на кнопку «**Добавить**», например, протокол

• в появившемся окне **3** нажать выбрать необходимый протокол и нажать на кнопку «**Ок**»

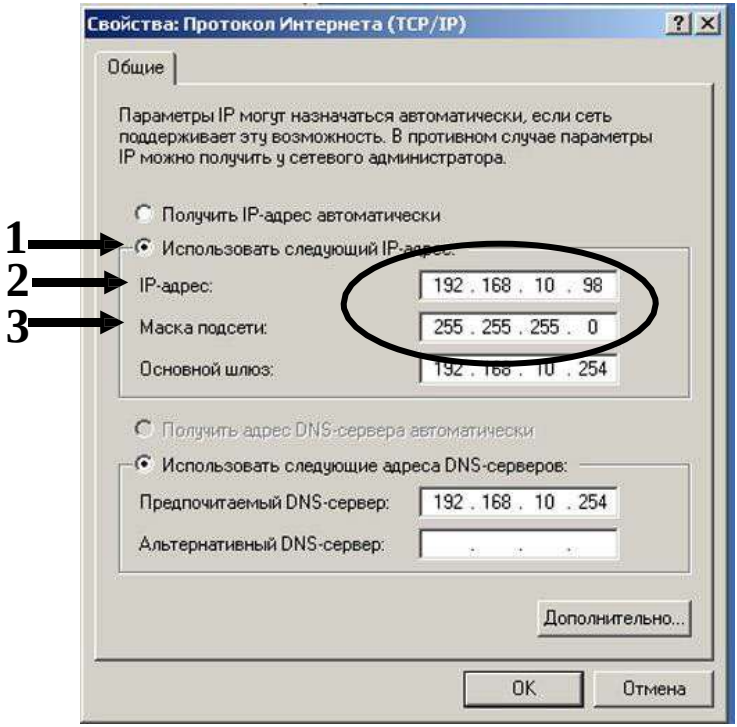


3. Для настройки сетевого протокола TCP/IP необходимо:

- открыть в меню «**Пуск**» «**Настройка**»-«**Панель управления**»-«**Сеть и удаленный доступ к сети**», щелкнуть по «**Подключение по локальной сети**» правой кнопкой мыши и выбрать свойства



- В появившемся окне выбрать настраиваем IP-адрес и щелкнуть по кнопке «**Свойства**»



Параметры 1,2,3 обязательные

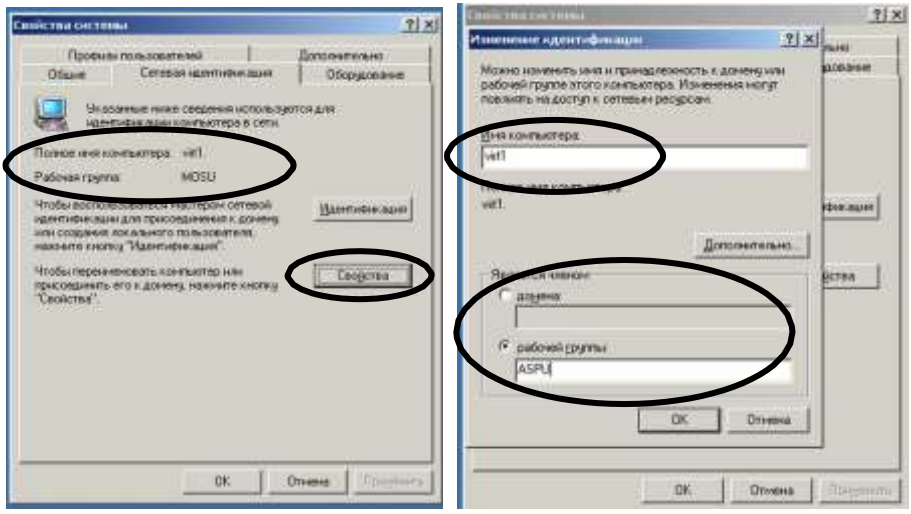
- IP-адрес состоит из адреса **подсети (192.168.10**) и адреса самого компьютера **(98)**
- для небольших сетей (до 254 компьютеров) можно использовать адресацию с 192.0.1.N по 223.255.255.N (где N номер компьютера)
- Стандартная маска подсети для данного типа сети задается 255.255.255.0

Остальные параметры задаются по необходимости.

Протоколы IPX/SPX и NetBEUI дополнительных настроек не требуют (но если сеть построить на их основе, то работать в Интернет будет нельзя, т.к. для работы в Интернет необходим протокол TCP/IP)

4. Для настройки имени компьютера и группы или домена необходимо:

- открыть в меню «**Пуск**» «**Настройка**»-«**Панель управления**»-«**Система**», щелкнуть по «**Сетевая идентификация**» и выбрать «**Свойства**»



- в появившемся окне задаем имя компьютера и указываем рабочую группу или домен, в который входит компьютер (Например, рабочая группа ASPU)

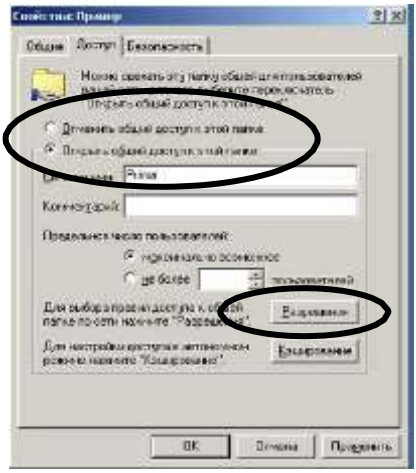
Примечание: *имя компьютера и принадлежность к рабочей группе или домену задается не зависимо от того какой сетевой протокол установлен.*

5. Настройка прав доступа к ресурсам компьютера

Для настройки прав доступа к ресурсам компьютера можно определять как группе пользователей так и каждому пользователю отдельно.

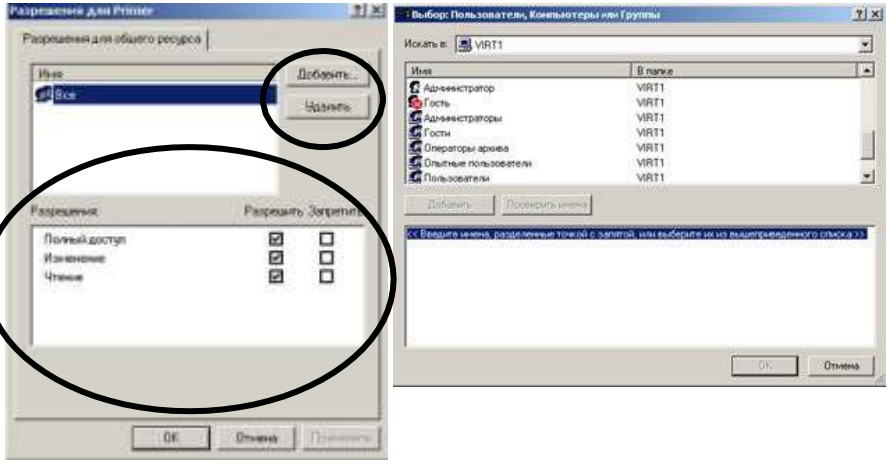
Для повышения эффективности работы с общеиспользуемыми ресурсами удобно создавать группы пользователей, для которых определяются права доступа.

Для открытия общего доступа к папке необходимо щелкнуть правой кнопкой по ней и выбрать пункт «**Доступ**»



Установить переключатель «**Открыть общий доступ к этой папке**»

Настроить правила доступа щелкнув по кнопке «**Разрешения**»



Щелкните по кнопке «**добавить**» для выбора пользователей и с помощью указателей настройте им разрешения

Выберите пользователя и щелкните по кнопке «**Удалить**» если необходимо убрать пользователя из списка.

Например: Если вы хотите разрешить доступ к папке по сети только «Учителям» то вы должны добавить группу «Учителя» и дать им нужный доступ. Затем выделить группу «Все» у щелкнуть по кнопке «**Удалить**»

Лабораторная работа №2

МЕХАНИЗМ АДРЕСАЦИИ В IP-СЕТЯХ

Цель работы – изучить адресацию, общую классификацию адресов в стеке TCP/IP, принцип назначения IP-адресов узлам отдельных подсетей.

Типы адресов стека TCP/IP

В стеке **TCP/IP** используются **три типа адресов**:

1. **локальные** (называемые также аппаратными)
2. **IP-адреса**
3. **символьные доменные имена**

Локальные адреса

Локальный адрес в терминологии **TCP/IP** - это такой тип адреса, который используется средствами **базовой технологии** для доставки данных в пределах **подсети**, которая сама является элементом **составной интерсети**.

В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека **TCP/IP** уже заранее предполагалось наличие **разных типов локальных адресов**.

Если подсетью интерсети является локальная сеть, то **локальный адрес - это MAC - адрес**.

MAC - адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов.

MAC - адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно.

Для всех существующих технологий локальных сетей **MAC - адрес имеет формат 6 байт**, например **11-AO-17-3D-BC-01**.

Надо отметить, что поскольку **протокол IP** может работать и над протоколами **более высокого уровня**. В этом случае **локальными адресами** для **протокола IP** соответственно будут **адреса соответствующих протоколов более высокого уровня**.

Следует учесть, что компьютер в локальной сети может иметь несколько **локальных адресов** даже при одном сетевом адаптере. И наоборот, некоторые сетевые устройства вообще не имеют **локальных адресов**. Например, к таким устройствам относятся глобальные порты маршрутизаторов, предназначенные для соединений типа **"точка-точка"**.

IP-адреса - основной тип адресов сетевого уровня.

На основании IP-адресов сетевой уровень передает пакеты между сетями.
IP-адреса состоят из **4 байт**.

IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: **номера сети** и **номера узла.**

Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения **Internet (InternetNetworkInformationCenter, InterNIC)** , если сеть должна работать как составная часть **Internet.** Обычно поставщики услуг **Internet** получают диапазоны адресов у подразделений **InterNIC**, а затем распределяют их между своими абонентами.

Номер узла в **протоколе IP** назначается **независимо** от **локального адреса** узла!

Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный **IP-адрес**.

Конечный узел также может входить в несколько **IP-сетей.** В этом случае компьютер должен иметь несколько **IP-адресов,** по числу сетевых связей.

Таким образом, **IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение**. Напоминаю, что мы поговорим об этом немного позже более подробно.

Символьные имена

Символьные имена имеют символьный вид и в **IP-сетях** называются **доменными.**

Доменные имена строятся по иерархическому признаку. Полное **символьное имя в IP-сетях** состоит из нескольких составляющих, которые разделяются точкой. Они перечисляются в следующем порядке (сдева-направо):

- сначала простое **имя конечного узла**
- затем**имя группы узлов** (например, имя организации)
- затем**имя более крупной группы (поддомена)**

И так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: **UA** - Украина, **RU** - Россия, **UK** - Великобритания, **SU** - США)

Примеров **доменного имени** может служить имя **base2.sales.zil.ru**. Между **доменным именем** и **IP-адресом** узла **нет никакого соответствия,** поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел интерсети однозначно мог определяться в сети, как по **доменному имени,** так и по **IP-адресу.**

IP адреса. Классы IP адресов

Самое первое, что надо сразу уяснить - **IP-адреса** назначаются не узлам составной сети. **IP адреса** назначаются сетевым интерфейсам узлов составной сети.

Очень многие (если не большинство) компьютеров в **IP сети** имеют единственный сетевой интерфейс (и как следствие один **IP адрес**). Но компьютеры и другие устройства

могут иметь несколько (если не больше) сетевых интерфейсов - и каждый интерфейс будет иметь свой собственный **IP адрес**.

Так устройство с 6 активными интерфейсами (например, маршрутизатор) будет иметь **6 IP адресов** - по одному на каждый интерфейс в каждой сети, к которой он подключен.

Итак, **IP адрес** определяет однозначно **сеть** и **узел**, который подключен к данной сети. **IP адрес** имеет длину **4 байта (8 бит)**, это дает в совокупности **32 бита** доступной информации.

Для улучшения читабельности, **IP адрес** записывается в виде четырех чисел, **разделенных точками**:

например, **128.10.2.30** - десятичная форма представления адреса - **4 (десятичных) числа, разделенных (.) точками**, а **10000000 00001010 00000010 00011110** - двоичная форма представления этого же адреса. **4-ре 8-ми разрядных числа (октета)**

*Так как каждое из четырех чисел - это десятичное представление 8-битного байта, то каждое число может принимать значения от **0 до 255** (что дает **256** уникальных значений - помните, ноль - это тоже величина).*

Здесь надо отметить:

Десятичная форма записи **IP-адреса** используется в основном при в операционных системах, как наиболее удобная при настройке.

Кроме двоичной формы, встречается шестнадцатеричная форма записи **IP-адреса: C0.94.1.3**

Для сведения: использование **32-разрядных** двоичных чисел позволяет создавать **4 294 967 296 уникальных IP-адресов** - более чем достаточно для любой частной **интрасети** (хотя сеть **Internet** скоро может начать испытывать нехватку уникальных адресов).

IP адрес состоит из двух логических частей - номера сети и номера узла в сети.

Конечно же, сразу возникает вопрос: а как определить в одном адресе, где **номер сети**, а где **номер узла**? Можно условится использовать, например, первые **8 бит адреса** для **номера сети**, остальные для **номеров узлов** в той сети, или **первые 16 бит**, или **первые 24 бита**. Но в таком случае адресация получается абсолютно не гибкой, мы будем иметь или много маленьких сетей и мало больших, или наоборот.

Для того чтобы более рационально определиться с величиной сети и при том разграничить какая часть **IP-адреса** относится к **номеру сети**, а какая - к **номеру узла** условились использовать **систему классов**. Система классов использует значения **первых бит адреса**.

Но, таким образом, что значения этих **первых бит адреса** являются признаками того, к какому **классу** относится тот или иной **IP-адрес**.

Классы IP-адресов:

Классы IP -адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов
А	0	1.0.0.0	126.0.0.0	2^{24}
Б	10	128.0.0.0	191.255.0.0	2^{16}
С	110	192.0.1.0	223.255.255.0	2^{8}
Д	1110	224.0.0.0	239.255.255.255	Multicast
Е	11110	240.0.0.0	247.255.255.255	Зарезервирован

Сети класса С являются **наиболее распространенными**.

- 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**. Но об этом мы еще поговорим ниже.

- Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу Е. Адреса этого класса зарезервированы для будущих применений.

Таким образом, можно однозначно определить, что:

Большие сети получают адреса **класса А**, **средние - класса В**, а **маленькие - класса С**. В зависимости от того к какому классу (**А В С**) принадлежит адрес, **номер сети** может быть представлен **первыми 8, 16 или 24 разрядами**, а **номер хоста - последними 24, 16 или 8 разрядами**.

Такова традиционная **система классов**, но и она не достаточно гибко определяет границы между **номером сети** и **номером узла**. С использованием классов границы проходят по **границам байтов**. Существует другой метод, который может проводить разделение границы между **номером сети и номером узла** в одном **IP-адресе по границам битов!** Но всему свое время, и прежде чем, познакомится с этим способом, мы

должны рассмотреть следующий, очень немаловажный момент, который касается "правил исключений" в **IP - адресации**.

Особые IP-адреса

Существуют некоторые значения **IP-адресов**, которые **зарезервированы заранее**, то есть существуют **IP-адреса**, которые предназначены для **особых целей**.

1) Если весь **IP-адрес** состоит **только из двоичных нулей**, то он обозначает **адрес того узла, который сгенерировал этот пакет**;

0 0 0 0 ..... 0 0 0 0

этот режим используется только в некоторых сообщениях **протокола межсетевых управляющих сообщений ICMP**.

2) Если в **поле номера сети** стоят только **нули**, то по умолчанию считается, что **узел назначения принадлежит той же самой сети**, что и **узел, который отправил пакет**.

0 0 0 0 .....0 Номер узла

IP-адрес с **нулевым номером хоста** используется для адресации ко всей сети. Например, в сети **класса С**с номером **199.60.32 IP-адрес 199.60.32.0** обозначает сеть в целом.

3) Если все **двоичные разряды IP-адреса равны 1**, то **пакет с таким адресом назначения должен рассылаться всем узлам**, находящимся в той же сети, что и **источник этого пакета**.

1 1 1 1 .....1 1

Такая рассылка называется **ограниченным широковещательным сообщением (limitedbroadcast)** .

4) Если в **поле номера узла назначения** стоят **только единицы**, то **пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети**. Например, пакет с адресом **192.190.21.255** доставляется всем узлам сети **192.190.21.0**.

Номер сети 1111. 11

Такая рассылка называется широковещательным сообщением (broadcast).

Предположим, например, что один из хостов в сети **класса С** с сетевым адресом **199.60.32.0** собирается направить сообщение всем остальным хостам, находящимся в той же сети. В этом случае сообщение должно быть передано на адрес **199.60.32.255**.

При **адресации** хостов интерсети администратор должен обязательно учитывать все ограничения, которые вносятся **особым назначением некоторых IP-адресов**.

Таким образом, каждый администратор должен знать, что **ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей**. Отсюда следует, что **максимальное количество узлов**, приведенное в таблице для сетей каждого класса, **на практике должно быть уменьшено на 2**.

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес зарезервирован для тестирования программ и взаимодействия процессов в пределах одной машины.

Когда программа посылает данные по **IP-адресу 127.0.0.1**, то образуется как бы "петля". Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые.

Поэтому **в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127! Этот адрес имеет название loopback**.

Можно отнести адрес **127.0.0.0** ко внутренней сети модуля маршрутизации узла, а адрес **127.0.0.1** - к адресу этого модуля на внутренней сети.

На самом деле любой адрес сети **127.0.0.0** служит для обозначения своего модуля маршрутизации, а не только **127.0.0.1**, например **127.0.0.3**.

В **протоколе IP** нет понятия широковещательности в том смысле, в котором оно используется в протоколах **канального уровня** локальных сетей, когда данные должны быть доставлены абсолютно всем узлам.

Как **ограниченный широковещательный IP-адрес**, так и **широковещательный IP-адрес** имеют свои пределы распространения в **интерсети**.

- они ограничены либо сетью, к которой принадлежит **узел-источник пакета**, либо сетью, **номер которой указан в адресе назначения**. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей просто потому, что **нет способа адресовать пакет одновременно всем узлам всех сетей составной сети**.

Нами уже упоминалась выше в таблице форма **группового IP-адреса - multicast**. Так вот именно **IP адрес 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. Члены какой-либо **группы multicast** не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по совершенно различным сетям, находящимся друг от друга на произвольном количестве хопов.

Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Основное назначение **multicast-адресов** - распространение информации по схеме **"один-ко-многим"**.

Она работает следующим образом: хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью **специального протокола IGMP (InternetGroupManagementProtocol)** сообщает о создании в сети новой **мультивещательной группы** с определенным адресом.

Машрутизаторы, поддерживающие **мультивещательность**, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора.

Хосты, которые хотят присоединиться к вновь создаваемой **мультивещательной группе**, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы.

Чтобы маршрутизаторы могли автоматически распространять пакеты с адресом **multicast** по составной сети, необходимо использовать в конечных маршрутизаторах специальные **модифицированные протоколы обмена маршрутной информацией**.

В общем, **групповая адресация** была предназначена для экономичного распространения в **Internet** или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Надо сказать, что если такие средства найдут широкое применение (сейчас они представляют в основном небольшие экспериментальные островки в общем **Internet**), то **Internet** сможет создать серьезную конкуренцию радио и телевидению.

Ну что ж, давайте, сделаем итог, который закрепит наше представление о том, что означает **IP-адрес**:

IP адрес может означать одно из трех:

1. **Адрес IP сети** (группа **IP** устройств, имеющих доступ к общей среде передаче - например, все устройства в сегменте **Ethernet**). **Сетевой адрес** всегда имеет биты интерфейса (**хоста**) адресного пространства **установленными в 0** (если сеть не разбита на подсети - как мы еще увидим);
2. **Широковещательный адрес IP сети** (адрес для 'разговора' со всеми устройствами в **IP сети**). **Широковещательные адреса** для сети всегда имеют **хостовые биты адресного пространства установленными в 1** (если сеть не разбита на подсети - опять же, как мы вскоре увидим).
3. **Адрес интерфейса** (например **Ethernet-адаптер** или **PPP интерфейс** хоста, маршрутизатора, сервера печать итд). Эти адреса могут иметь любые значения **хостовых битов, исключая все нули или все единицы** - чтобы не путать с адресами сетей и **широковещательными адресами**.

Для сети класса A ...

(один байт под адрес сети, три байта под номер хоста)

10.0.0.0 сеть **класса A**, потому что **все хостовые биты равны 0**.

10.0.1.0 адрес хоста в этой сети

10.255.255.255 широковещательный адрес этой сети,
поскольку все сетевые биты установлены в **1**

Для сети класса B...

(два байта под адрес сети, два байта под номер хоста)

172.17.0.0 сеть **класса B**

172.17.0.1 адрес хоста в этой сети

172.17.255.255 сетевой широковещательный адрес

Для сети класса C...

(три байта под адрес сети, один байт под номер хоста)

192.168.3.0 адрес сети **класса C**

192.168.3.42 хостовый адрес в этой сеть

192.168.3.255 сетевой **широковещательный адрес**

Едва ли не все доступные сетевые **IP** адреса принадлежат **классу C**.

Маски в IP адресации

Итак, рассмотрена традиционная схема деления **IP-адреса** на **номер сети**, и **номер узла**, которая основана на понятии **класса**. **Класс** определяется значениями нескольких **первых бит адреса**. Теперь, например, можно определить, что поскольку первый байт адреса **185.23.44.206** попадает в диапазон **128-191**, то этот адрес относится к **классу B**, а значит, номером сети являются первые два байта, дополненные двумя нулевыми байтами **- 185.23.0.0**, а номером узла - **0.0.44.206**.

Очевидно, что определение **номеров сети** по первым байтам адреса также не вполне гибкий механизм для адресации. А что если использовать какой-либо другой признак, с помощью которого можно было бы более **гибко** устанавливать границу между **номером сети** и **номером узла**?

В качестве такого признака сейчас получили широкое распространение **маски**.

Маска - это тоже **32-разрядное** число, она имеет такой же вид, как и **IP-адрес**. Маска **используется в паре с IP-адресом**, но не совпадает с ним.

Принцип отделения **номера сети** и **номера узла** сети с использованием **маски** состоит в следующем:

Двоичная запись маски содержит *единицы* в тех разрядах, которые в IP-адресе должны представляться как номер сети и *нули* в тех разрядах, которые представляются как номер хоста.

Каждый класс **IP-адресов** (**A, B и C**) имеет свою **маску**, используемую по умолчанию.

Поскольку **номер сети** является цельной частью адреса, **единицы в маске** также должны представлять непрерывную последовательность.

Таким образом, для стандартных **классов сетей маски** имеют следующие значения:

- **класс A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0)** ;
- **класс B - 11111111. 11111111. 00000000. 00000000 (255.255.0.0)** ;
- **класс C - 11111111.11111111.11111111.00000000 (255.255.255.0)** .

Например:

Если адресу **185.23.44.206** назначить **маску 255.255.255.0**, то смотрим, что единицы в маске заданы в трех байтах, значит**номер сети** будет **185.23.44.0**, а не **185.23.0.0**, как это определено правилами системы классов.

Для записи **масок** используются и другие форматы, например, удобно интерпретировать значение **маски**, записанной в **шестнадцатеричном коде**:

FF.FF.00.00 - маска для адресов класса B.

Часто встречается и такое обозначение: IP-адрес/префикс сети. Например, **185.23.44.206/16** - эта запись говорит о том, что **маска** для этого адреса содержит **16 единиц** (префикс сети), или что в указанном **IP-адресе** под **номер сети** отведено **16** двоичных разрядов.

Нотация с префиксом сети также известна как бесклассовая междоменная маршрутизация (ClasslessInterdomainRouting -CIDR).

Таким образом, очень легко, снабжая каждый IP-адреспроизвольной маской **(**не обязательно кратной 8**),** отказаться от понятий **классов адресов** и тем самым сделать более гибкой систему IP адресации.

Рассмотрим пример: для IP-адреса **129.64.134.5** назначим **маску 255.255.128.0,** что в двоичном виде будет выглядеть так:

IP-адрес 129.64. 134.5 - 10000001.01000000.1 0000110.00000101
Маска 255.255.128.0 - 11111111.11111111.1 0000000.00000000

Здесь **17 последовательных единиц в маске**, "накладываются" на IP-адрес, и определяют номер сети : **10000001. 01000000. 10000000. 00000000**или **129.64.128.0**, аномер узла **0000110.00000101** или **0.0.6.5**.

Механизм масок очень широко распространен в **IP-маршрутизации**, причем **маски** могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, **не требуя от поставщика услуг дополнительных номеров сетей!**

На основе этого же механизма поставщики услуг могут **объединять адресные пространства нескольких сетей** путем введения так называемых **"префиксов"** с целью уменьшения объема **таблиц маршрутизации**, и повышения за счет этого производительности маршрутизаторов. (Создание надсетей).

Маски при записи всегда "неразлучны" с соответствующими адресами, **IP-адрес маска подсети** - именно так теперь и мы будем описывать адрес любого хоста сети.

Порядок назначения IP адресов. Автономные IP адреса. Автоматизация назначения IP адресов

Номера сетей могут назначаться либо **централизованно**, если сеть является частью **Internet**, либо **произвольно**, если сеть работает **автономно**. **Номера узлов** и в том и в другом случае администратор назначает самостоятельно по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона.

Главную роль в **централизованном распределении IP-адресов** до некоторого времени играла организация **InterNIC** (NetworkInformationCenter), однако с ростом сети задача распределения адресов стала слишком сложной. **InterNIC** делегировала часть своих функций другим организациям и крупным поставщикам услуг **Internet - провайдерам**. В частности распределением **IP-адресов** для подключения к сети Internet теперь занимаются **провайдеры**.

С тех пор, как появилась и стала широко распространяться сеть **Internet**, уже прошло не мало времени. И теперь уже становится актуальным вопрос о **дефиците IP-адресов**. Если говорить о реальной обстановке при распределении адресов для пользователей **Internet**, то сейчас очень трудно получить адрес **класса B** и уже практически невозможно стать обладателем адреса **класса A**! При этом всем надо сказать, что **дефицит IP-адресов** вызван не совсем постоянным ростом сетей, а просто нерациональным их использованием. Очень часто владельцы сети **класса C** расходуют лишь небольшую часть из имеющихся у них **254 адресов**.

Рассмотрим пример, когда две сети необходимо соединить глобальной связью.

В таких случаях в качестве канала связи используют два маршрутизатора, соединенных по схеме **"точка-точка"**.

В ситуации, которая приведена в примере, для вырожденной сети, образованной каналом, связывающим порты двух смежных маршрутизаторов, приходится выделять **отдельный номер сети**, хотя в этой сети имеются всего **2 узла**.

Давайте рассмотрим другую ситуацию: какие **IP-адреса** может использовать администратор, если провайдер услуг **Internet** не назначил ему никакого адреса? Если, к примеру, мы точно знаем, что сеть, которую мы администрируем никогда в будущем не будет подключаться к **Internet** (работает в **"автономном режиме"**), тогда мы можем использовать любые **IP-адреса**, соблюдая правила их назначения, о которых шла речь выше. Для простоты можно использовать адреса **класса С**: в этом случае не придется вычислять значение **маски** подсети и вычислять адрес для каждого хоста.

В этом случае мы должны будем просто назначить каждому сегменту нашей локальной сети его собственный сетевой номер **класса С**.

Если все сегменты нашей локальной сети имеют собственные сетевые номера **класса С**, то в каждом сегменте можно создать по **254** номера хостов.

Однако если у нас есть хотя бы небольшая вероятность того, что когда-либо в будущем наша сеть может быть подключена к Internet, не следует использовать такие IP-адреса! Они могут привести к конфликту с другими адресами в Internet. Чтобы избежать таких конфликтов, нужно использовать IP-адреса, **зарезервированные для частных сетей**.

Для этой цели зарезервированы специально несколько блоков **IP-адресов**, которые называются **автономными**.

Автономные IP адреса

Автономные адреса зарезервированы для использования **частными сетями**. Они обычно используются организациями, которые имеют свою частную большую сеть - **intranet** (локальные сети с архитектурой и логикой **Internet**), но и маленькие сети часто находят их полезными.

Эти адреса не обрабатываются маршрутизаторами Internet, ни при каких условиях. Эти адреса выбраны из разных классов.

Класс	**От IP-адреса**	**До IP-адреса**	**Всего узловадресов в диапазоне**
A	**10.0.0.0**	**10.255.255.255**	16 777 216-2

B	**172.16.0.0**	**172.31.255.255**	65 536-2
C	**192.168.0.0**	**192.168.255.255**	256-2

Эти адреса являются зарезервированными для **частных сетей.** Таким образом, если в будущем мы решим все-таки подключить свою сеть к **Internet**, то даже если трафик с одного из хостов в нашей сети и попадет каким-либо образом в **Internet**, конфликта между адресами произойти не должно. Маршрутизаторы в **Internet** запрограммированы так, чтобы не транслировать сообщения, направляемые с зарезервированных адресов или на них.

Надо сказать, что использование **автономных** IP-адресов имеет и недостатки, которые состоят в том, что если мы будем подключать свою сеть к **Internet**, то нам придется заново настроить конфигурацию хостов, соединяемых с **Internet**.

Можно сказать, что **подсеть** - это метод, состоящий в том, чтобы взять **сетевой IP адрес** и **локально** разбить его так, чтобы этот **один сетевой IP адрес** мог в действительности **использоваться в нескольких взаимосвязанных локальных сетях**.

О**дин сетевой IP адрес может использоваться только для одной сети! Самое важное**: разбиение на **подсети** - это **локальная настройка**, она не видна "снаружи". Разбиение одной большой сети на **подсети**, значительно разгружает общий трафик и позволяет повысить безопасность всей сети в целом.

Алгоритм разбиения сети на подсети

1) Устанавливаем физические соединения (сетевые кабели и сетевые соединители - такие как маршрутизаторы);
2) Принимаем решение насколько большие/маленькие **подсети** вам нужны, исходя из количества устройств, которое будет подключено к ним, то есть, сколько **IP адресов** требуется использовать в каждом сегменте сети.
3) Вычисляем соответствующие **сетевые маски** и **сетевые адреса**;
4) Раздаем каждому интерфейсу в каждой сети свой **IP адрес** и соответствующую **сетевую маску**;
5) Настраиваем каждый маршрутизатор и все сетевые устройства;
6) Проверяем систему, исправляем ошибки.
Сейчас наша задача разобраться с тем, как выполнить 2-й и 3-й шаги.

Пример 1

Предположим, что мы хотим разбить нашу сеть на подсети, но имеем только один **IP-адрес сети 210.16.15.0**.

Решение:

IP-адрес 210.16.15.0 - это адрес **класса C**. Сеть **класса C** может иметь до **254** интерфейсов (хостов) плюс **адрес сети (210.16.15.0)** и **широковещательный адрес (210.16.15.255)**.
Первое: определить **"размер" подсети**.

Существует зависимость между количеством создаваемых **подсетей** и "потраченными" **IP адресами**.

Каждая отдельная **IP сеть** имеет **два адреса, неиспользуемые для интерфейсов (хостов)**:

- **IP адрес собственно сети и широковещательный адрес**.

При разбивке на подсети **каждая подсеть требует свой собственный уникальный IP адрес сети и широковещательный адрес** - и они должны быть корректно выбраны из диапазона адресов **IP сети**, которую мы делим на **подсети**.

Итак, если при разбивке **IP сети** на **подсети**, в каждой из которых есть **два сетевых адреса** и **два широковещательных адреса** - надо помнить, что каждая из них уменьшит количество используемых интерфейсных (хостовых) адресов на два.

Это мы должны всегда учитывать при вычислении **сетевых номеров**. Следующий шаг - **вычисление маски подсети и сетевых номеров**.

Сетевая маска - это то, что выполняет все логические манипуляции по разделению **IP сети на подсети**.

Для всех трех классов **IP сетей** существуют стандартные сетевые **маски**:

- **Класс А** (8 сетевых битов) :**255.0.0.0**
- **Класс В** (16 сетевых битов): **255.255.0.0**
- **Класс С** (24 сетевых бита): **255.255.255.0**

Чтобы создать **подсеть,** нужно изменить маску подсети для данного класса адресов.

Номер подсети можно задать, позаимствовав нужное для нумерации подсетей количество разрядов в номере хоста. Для этого берутся левые (старшие) разряды из номера хоста, в маске же взятые разряды заполняются единицами, чтобы показать, что эти разряды теперь нумеруют не узел а подсеть. Значения в остающихся разрядах маски подсети оставляются равными **нулю;** это означает, что оставшиеся разряды в номере хоста в **IP-адресе** должны использоваться как новый (меньший) номер хоста.

Например, чтобы **разбить сетевой адрес** на **две** подсети, мы должны позаимствовать **один хостовый бит**, установив **соответствующий бит в сетевой маске первого хостового бита в 1**.

Если нам нужно **четыре подсети** - используем **два хостовых бита**, если **восемь подсетей** - **три бита** и т.д. Однозначно, что если нам нужно **пять подсетей**, то мы будем использовать **три хостовых бита**. Соответствующим образом изменяется и **маска подсети**:

Для адресов **класса С**, при разбиении на **2 подсети** это дает **маску** -
11111111.11111111.11111111.10000000 или **255.255.255.128**
при разбиении на **4 подсети** маска в двоичном виде -
11111111.11111111.11111111.11000000, или в десятичном **255.255.255.192**. и т.д.

Для нашего адреса сети класса С **210.16.15.0**, можно определить следующих несколько способов разбивки на **подсети**: -

Число подсетей	Число хостов	Сетевая маска
2	126	255.255.255.128 (11111111.11111111.11111111.10000000)
4	62	255.255.255.192 (11111111.11111111.11111111.11000000)
8	30	255.255.255.224 (11111111.11111111.11111111.11100000)
16	14	255.255.255.240 (11111111.11111111.11111111.11110000)

32	6	255.255.255.248 (11111111.11111111.11111111.11111000)
64	2	255.255.255.252 (11111111.11111111.11111111.11111100)

Теперь нужно решить вопрос об **адресах сетей и широковещательных адресах,** и о диапазоне **IP адресов** для каждой из этих сетей.
Снова, принимая во внимание только сетевые адреса **класса C.** и показав только последнюю (хостовую) часть адресов, мы имеем:

Сетевая маска	Подсети	Сеть	Broadcast	MinIP	MaxIP	Хосты	Всего хостов
128	2	0	127	1	126	126	
		128	255	129	254	126	252
192	4	0	63	1	62	62	
		64	127	65	126	62	
		128	191	129	190	62	
		192	255	193	254	62	248
224	8	0	31	1	30	30	
		32	63	33	62	30	
		64	95	65	94	30	
		96	127	97	126	30	
		128	159	129	158	30	
		160	191	161	190	30	
		192	223	193	222	30	
		224	255	225	254	30	240

Из этой таблицы сразу можем увидеть, что **увеличение количества подсетей сокращает общее количество доступных хостовых адресов**. Теперь, вооруженные этой информацией, мы готовы назначать **хостовые и сетевые IP адреса и сетевые маски**.

Пример 2

Определим, сколько нужно подсетей для нашей сети **класса C**, чтобы разбить ее на подсети по **10 хостов** в каждой.

Решение:

Сеть **класса C** может обслуживать всего **254** хоста плюс адрес сети и широковещательный адрес.
Для адресации **10-ти** хостов **3-х** разрядов недостаточно, поэтому необходимо **4-е** разряда. Итак, из восьми возможных для класса **C**, нам нужно только **4** разряда для адресации **10** хостов, остальные можно использовать как сетевые для адресации **подсетей**. Мы уже знаем, что каждая подсеть уменьшает количество возможных хостовых адресов в два раза. Для адресации **16 подсетей** необходимо использовать **4 разряда**. Итак, посчитаем теперь количество узлов в каждой из **16 подсетей**: 2^4 **- 2 = 14 хостов**. Это количество с запасом удовлетворяет условие задачи.

Вычислим **маску подсети**, в этом случае она имеет вид:

11111111.11111111.11111111.11110000 или
255.255.255.240

Мы должны будем указать эту маску при настройке конфигурации каждого хоста в нашей сети (независимо от того, в какой подсети находится хост).
Теперь, например, мы можем сказать, адрес **192.168.200.246** с маской **255.255.255.240** - означает номер сети **192.168.200.240** и номер узла **0.0.0.6**.

Пример 3

Теперь, для всех трех классов определим соответственно маски подсети, и максимальное количество узлов возможное в каждой из этих подсетей, если необходимо разбить соответственно сеть **класса А**, сеть **класса В**, сеть **класса С** на отдельные **4 подсети**.

Решение:

Для сети **класса А**:

Максимальное количество узлов **16 777 216**. Для адресации 4-х подсетей необходимо **2** разряда, значит остается **22 разряда** для адресации **хостов**. Таким образом, каждая из четырех подсетей способна обслуживать $2^{22} - 2 = 4\ 194\ 302$ хоста в каждой из подсетей.

Число подсетей	Число хостов	Сетевая маска
4	4 194 302	255.192.0.0 (11111111. 11000000.00000000.00000000)

Для сети **класса В**

Максимальное количество узлов - **65 536**. Для адресации **4-х** подсетей в сетевом адресе **класса В** также нужно использовать **2 разряда**, но теперь свободными остается **14 разрядов**. Таким образом, каждая из подсетей может обслуживать $2^{14} - 2 = 16\ 382$ хостов.

Число подсетей	Число хостов	Сетевая маска
4	16 382	255.255.192.0 (11111111.11111111. 11000000.00000000)

Пример с сетью **класса С** мы уже рассматривали. Итак, теперь самое главное уметь в **двоичном виде** читать **IP адреса**, а с помощью маски легко можно определить **номер сети** и **номер узла**. Вот теперь, можно сказать, теория заканчивается, для нашей работы очень важно "окрепнуть" в навыках работы с **IP адресами**, уметь разделять сети на **подсети**, вычислять **маски подсети**, и назначать возможные **адреса сетей**, и **адреса хостов** - это прямая обязанность сетевых администраторов.

Надо сказать, что назначение **IP-адресов** узлам сети даже при не очень большом размере сети представляет для администратора очень утомительную процедуру. Поэтому сразу вторым шагом в **IP адресации** разработчики решили автоматизировать этот процесс.

С этой целью был разработан протокол **DynamicHostConfigurationProtocol (DHCP)**, который освобождает администратора от этих проблем, **автоматизируя процесс назначения IP-адресов**.

DHCP может поддерживать способ **автоматического динамического распределения адресов**, а также **более простые способы ручного и автоматического статического назначения адресов**. **Протокол DHCP** работает в соответствии с моделью **клиент-сервер**.

Во время старта системы компьютер, являющийся **DHCP-клиентом**, посылает в сеть **широковещательный запрос** на получение **IP-адреса**. **DHCP - сервер** откликается и посылает сообщение-ответ, содержащее **IP-адрес**. Предполагается, что **DHCP-клиент и DHCP-сервер находятся в одной IP-сети**.

При **динамическом** распределении адресов **DHCP-сервер** выдает адрес клиенту на **ограниченное время**, оно называется **временем аренды (leaseduration)** . Это дает возможность впоследствии повторно использовать этот **IP-адрес** для назначения **другому** компьютеру.

Основное преимущество DHCP - автоматизация рутинной работы администратора по конфигурированию стека TCP/IP на каждом компьютере. Иногда **динамическое** разделение адресов позволяет строить **IP-сеть**, количество узлов которой превышает количество имеющихся в распоряжении администратора **IP-адресов**.

В **ручной процедуре** назначения **статических адресов** активное участие принимает администратор, который предоставляет **DHCP - серверу** информацию о **соответствии IP-адресов физическим адресам** или другим идентификаторам клиентов. **DHCP-сервер**, пользуясь этой информацией, всегда выдает определенному клиенту назначенный администратором адрес.

При **автоматическом статическом** способе **DHCP-сервер** присваивает **IP-адрес** из **пула наличных IP-адресов** без вмешательства оператора. А границы **пула назначаемых адресов** задает администратор при конфигурировании **DHCP-сервера**.

Адрес дается клиенту из **пула** в **постоянное пользование**, то есть с **неограниченным сроком аренды**. Между **идентификатором клиента** и его **IP-адресом** по-прежнему, как и при **ручном** назначении, существует постоянное соответствие. Оно устанавливается в момент **первого** назначения **DHCP-сервером IP-адреса** клиенту. При всех последующих запросах сервер возвращает тот же самый **IP-адрес**.

DHCP обеспечивает надежный и простой способ конфигурации сети **TCP/IP**, **гарантируя отсутствие дублирования адресов за счет централизованного управления их распределением**.

Администратору в этом случае остается только управляет **процессом назначения адресов** с помощью параметра **"продолжительность аренды"**, которая определяет, как долго компьютер может использовать назначенный **IP-адрес**, перед тем как снова запросить его от **DHCP-сервера** в аренду.

Задания

1) **IP-адрес 190.235.130.N**(где N-номер варианта согласно таблице, данной ниже), сетевая маска **255.255.192.0**. Определите, **адрес сети** и **адрес узла.**

2) Определите **маски подсети** для случая разбиения сети с номером **192.0.0.0** на **32 подсети**.

3) Существует единая корпоративная сеть, количество узлов сети - **50 450**. Этой сети выделен адрес для выхода в **Internet192.124.0.0**. Вы решили не требовать от провайдера дополнительных адресов и организовать **8** филиалов в этой сети. Спрашивается:
- Какое максимальное количество узлов может быть в каждом из филиалов? Вычислите **сетевые маски** и возможный диапазон **адресов хостов** для каждого из филиалов.

4) Вы являетесь администратором корпоративной сети из **6 подсетей**, в каждой подсети по 25 компьютеров. Необходимо используя один номер сети **класса С 192.168.10.0**, определить правильно ли выбран **размер подсети**, и назначить маски и возможные **IP-адреса** хостам сети.

5)Разделить IP-сеть на подсети в соответствии с вариантом из таблицы. Для каждой подсети указать широковещательный адрес.

Таблица 5.

Вариант	**Сеть**	**Подсети**
1.	192.168.16.0/24	5 подсетей с 100, 20, 10, 6 и 40 узлами
2.	194.45.27.0/24	5 подсетей с 34, 20, 62,10 и 40 узлами
3.	56.1.1.0/16	4 подсети с 65, 22, 10 и 30 узлами
4.	147.168.0.0/16	5 подсетей с 56, 16, 10 и 70 узлами
5.	193.68.61.0/24	5 подсетей с 100, 20, 10 и 40 узлами
6.	192.100.0.0/24	4 подсети с 80, 20, 12 и 20 узлами
7.	195.18.11.0/24	4 подсети с 110, 11, 10 и 40 узлами
8.	207.15.0.0/24	4 подсети с 28, 80, 10 и 40 узлами
9.	222.11.0.0/24	4 подсети с 110, 20, 10 и 50 узлами
10.	200.2.2.0/24	4 подсети с 100, 20, 10 и 40 узлами
11.	201.111.32.0/16	5 подсетей с 170, 590, 1500, 800 и 254 узлами
12.	128.200.1.0/16	5 подсетей с 115, 300, 200, 128 и 420 узлами
13.	53.11.0.0/16	5 подсетей с 165, 222, 128, 110 и 430 узлами
14.	146.77.0.0/16	5 подсетей с 550, 116, 200, 256 и 170 узлами
15.	194.54.45.0/24	4 подсети с 103, 39, 10 и 16 узлами
16.	142.51.0.0/16	4 подсети с 180, 120, 12 и 30 узлами
17.	43.0.0.0/16	4 подсети с 151, 211, 16 и 70 узлами

Контрольные вопросы

1. Какие бывают классы IP-адресов.
2. Как по первому байту адреса определить его класс?
3. Что такое маска, на что она указывает?
4. Для чего нужны маски переменной длины?
5. Изложите алгоритм деления сетей на подсети с помощью VLM (variable length mask).

Лабораторная работа №3

Тема: "Программа для изучения компьютерных сетей Netemul"

Бесплатная программа Netemul была создана в учебных целях и служит для визуализации работы компьютерных сетей, для облегчения понимания происходящих в ней процессов. Программа одинаково хорошо работает как в ОС Windows XP, так и в ОС Windows 7.

Интерфейс программы

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

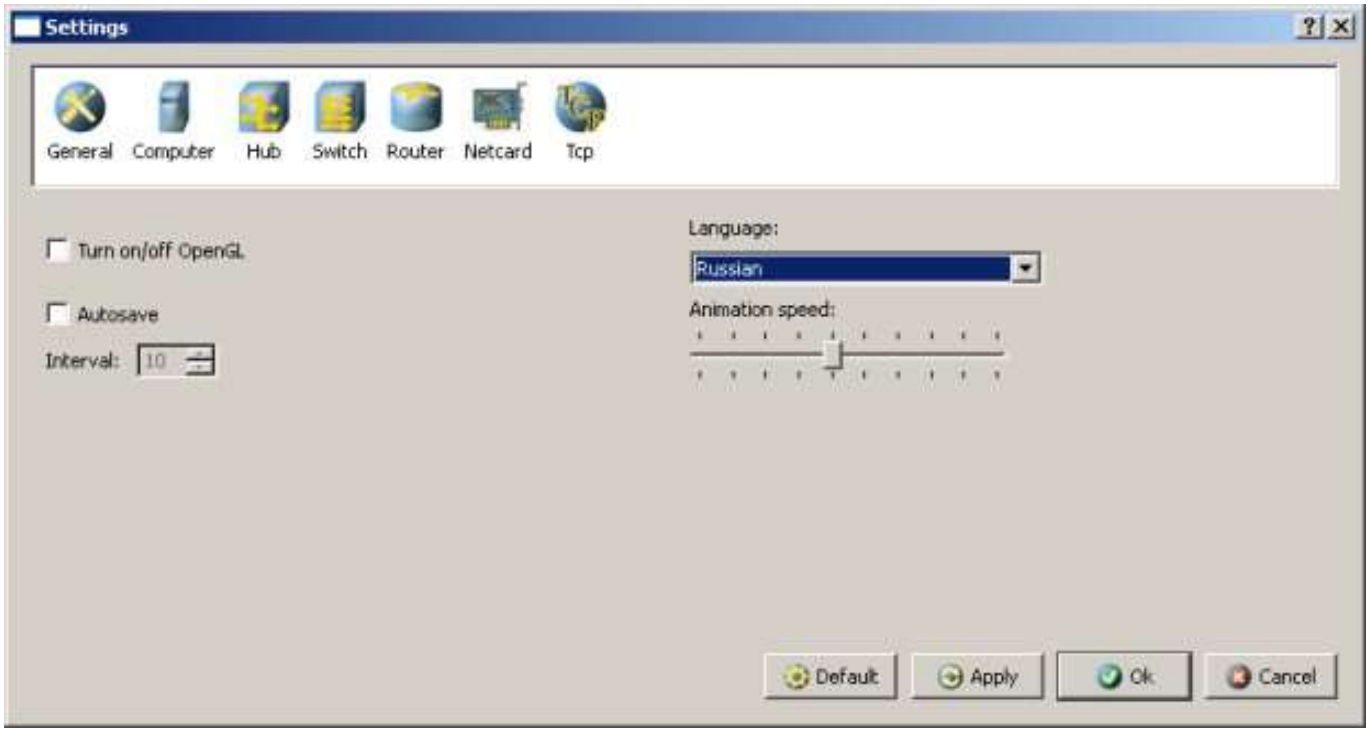


Рис. 5.1. Русифицируем интерфейс программы

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 так же 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).

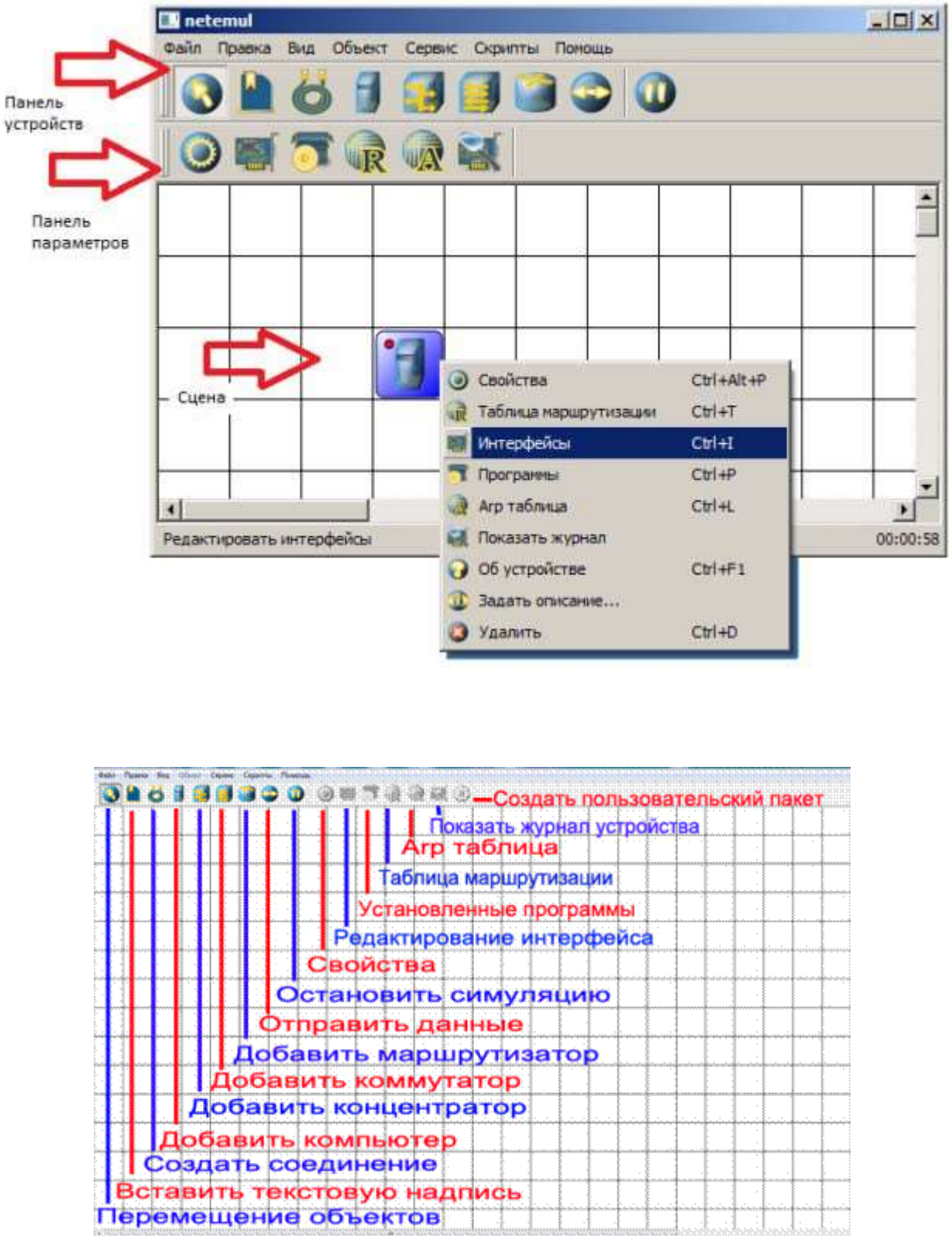


Рис. 5.2. Интерфейс программы Netemul

Пример 1. Строим сеть из двух ПК и коммутатора

Для начального знакомства с программой давайте построим простейшую локальную сеть и посмотрим, как она работает. Для этого выполните команду **Файл-Новый** и нарисуйте схему сети как на рис. 5.3.

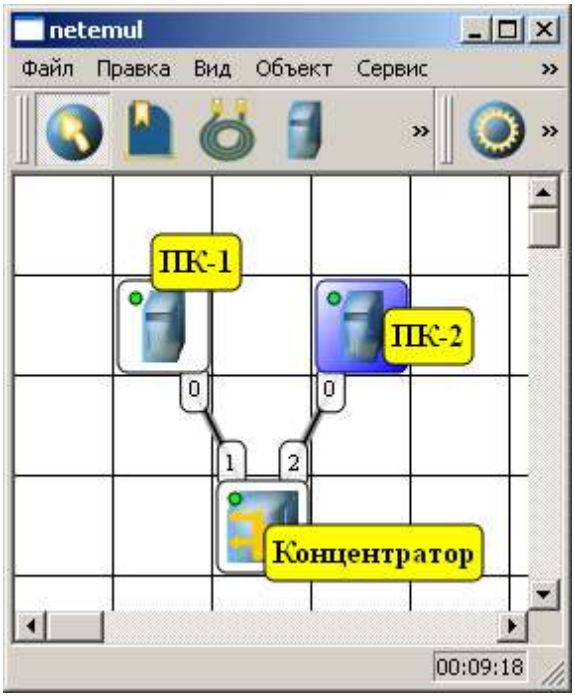


Рис. 5.3. Схема из двух ПК и концентратора

После рисования двух ПК и концентратора создадим их соединение (рис. 5.4).

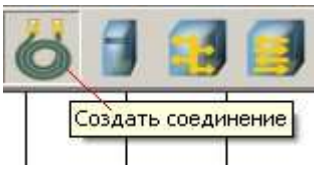


Рис. 11.4. Инструмент создания соединений сетевых устройств

В процессе рисования связей между устройствами вам потребуется выбрать соединяемые интерфейсы и нажать на кнопку **Соединить** (рис. 11.5 и 6).

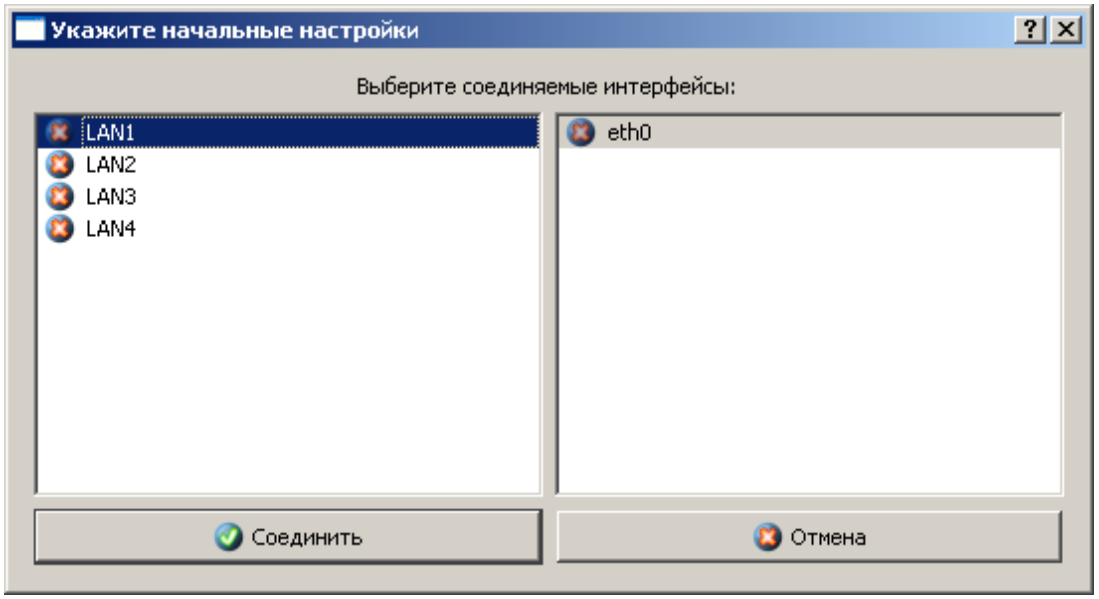


Рис. 11.5. Выбор начальных настроек соединения

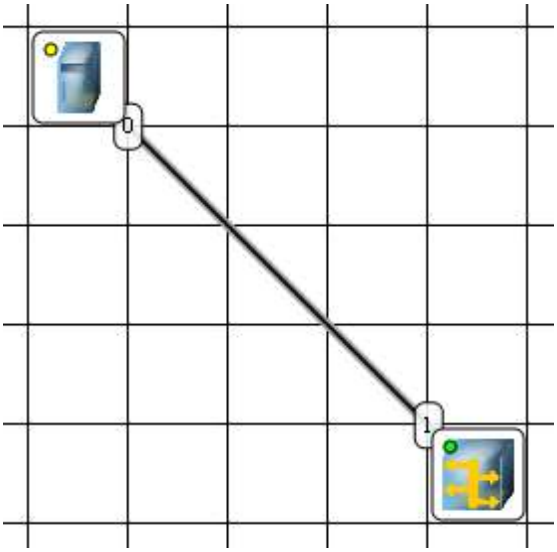


Рис. 11.6. Соединение устройств произведено

Теперь настроим интерфейс (сетевую карту) на наших ПК ее – рис. 11.6 и рис. 11.7.

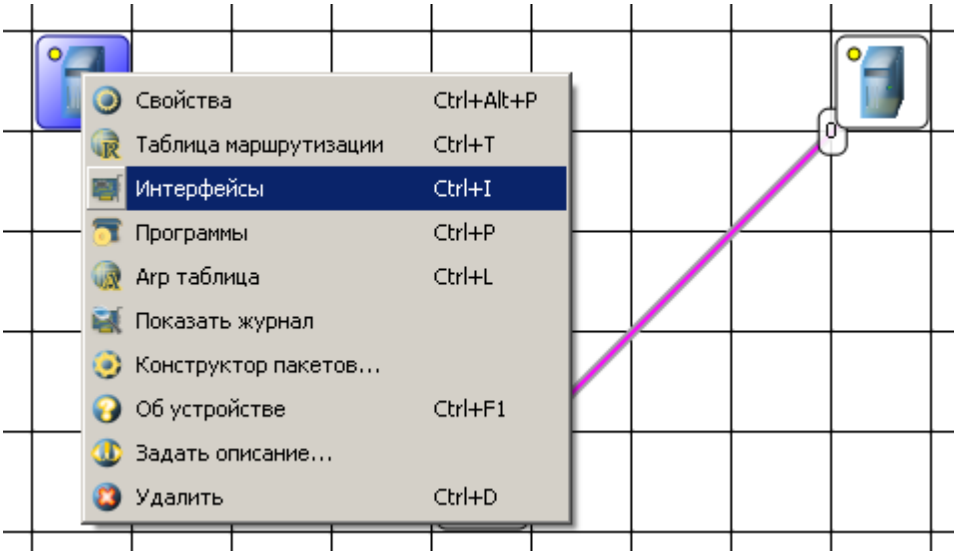


Рис. 11.6. Добавляем интерфейс

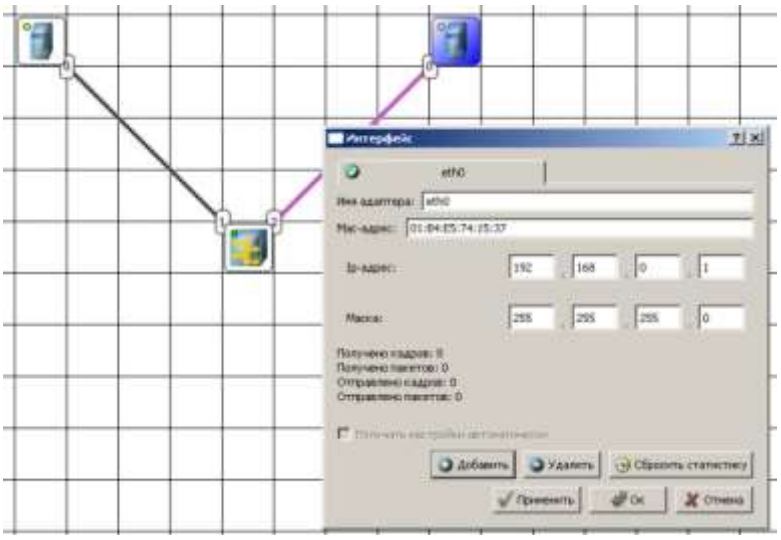


Рис. 11.7. Вводим IP адрес и маску сети

Примечание

Обратите внимание: после того, как вы напишете 192.168.0.1 маска появляется автоматически. После нажатия на кнопки **Применить** и **ОК** – появляется анимация движущихся по сети пакетов информации.

Все - сеть создана и настроена. Отравляем данные по протоколу TCP (рис. 11.8 и рис. 11.9).

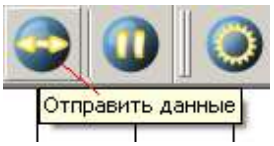


Рис. 11.8. Кнопка Отправить данные

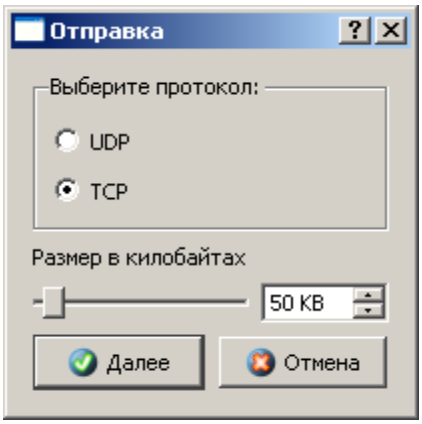


Рис. 11.9. Выбор протокола

Если вы где-то ошиблись, то появиться соответствующее сообщение, а если все верно – то произойдет анимация движущихся по сети пакетов (рис. 11.10).

Рис. 11.10. Движение пакетов по сети

И еще один момент. По умолчанию каждый ПК имеет одну сетевую карту, но их может быть и несколько. Для того, чтобы добавить для ПК адаптер нужно щелкнуть на нем правой кнопкой мыши и выбрать пункт меню **Интерфейсы**. В результате откроется следующее диалоговое окно (рис. 11.11).

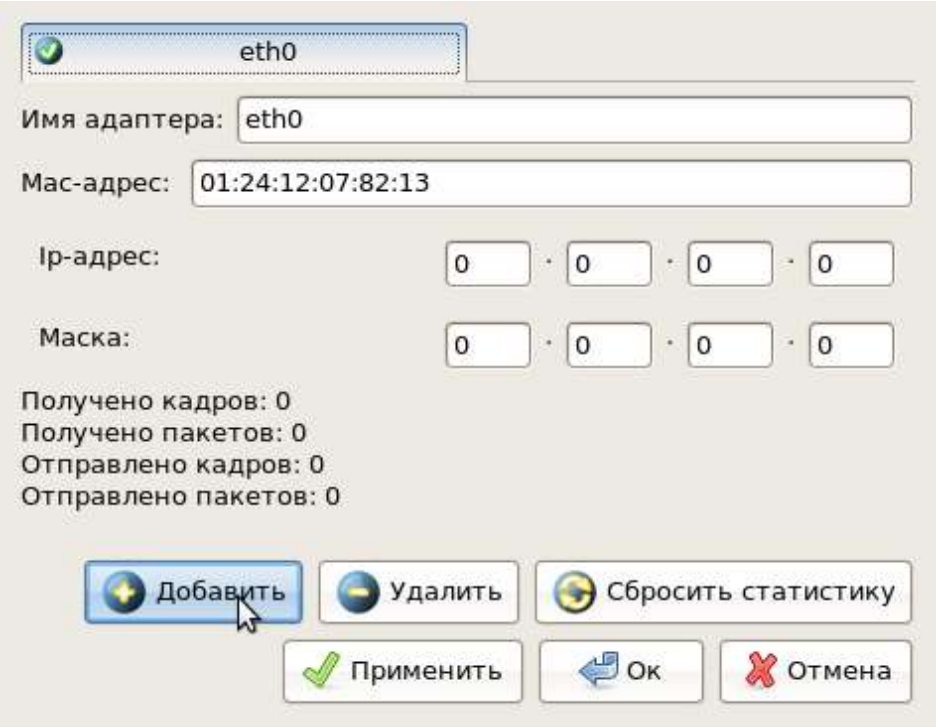


Рис. 11.11. Диалоговое окно работы с сетевым интерфейсом ПК

Нажимаем на кнопку **Добавить**, выбираем тип нового адаптера, нажимаем OK, и у нас есть еще один интерфейс. В качестве примера на рис. 11.12 изображен ПК, имеющий три сетевых карты.

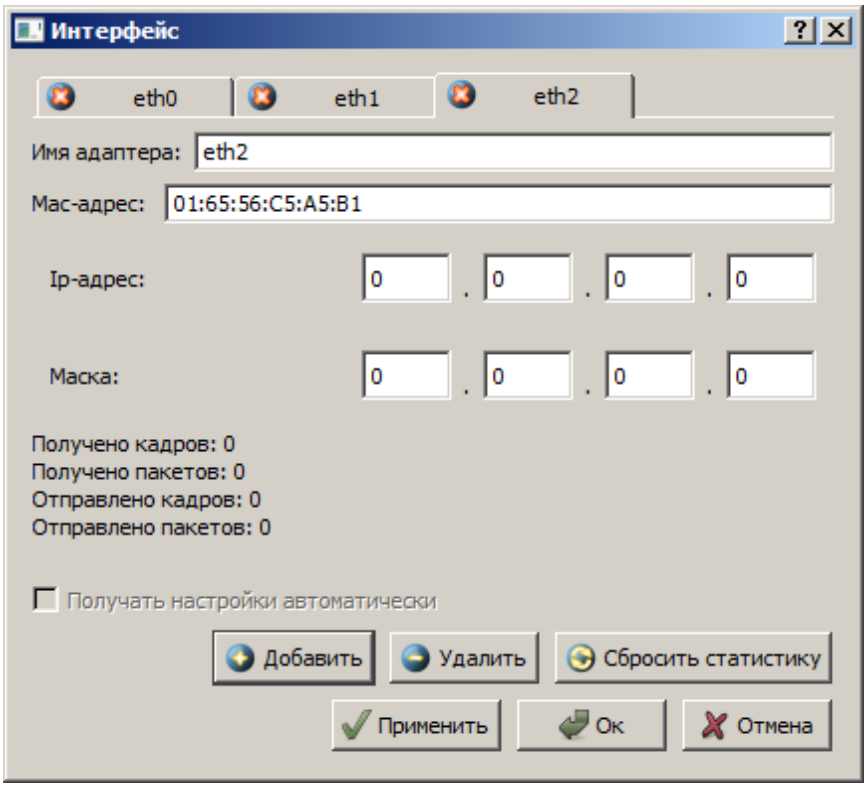


Рис. 11.12. В этом ПК установлены адаптеры eth0-eth3

Примечание

Каждый сетевой интерфейс (сетевой адаптер) имеет свой собственный mac-адрес. В программе Netemul в строке "Мас-адрес" можно задать новый адрес, но по умолчанию, при создании интерфейса, ему автоматически присваивается этот уникальный номер.

Задание 1. Построить сеть из двух ПК и свитча, изучить таблицу коммутации

В приведенной в этом примере схеме замените хаб на свитч и посмотрите у него таблицу коммутации (рис. 11.13).

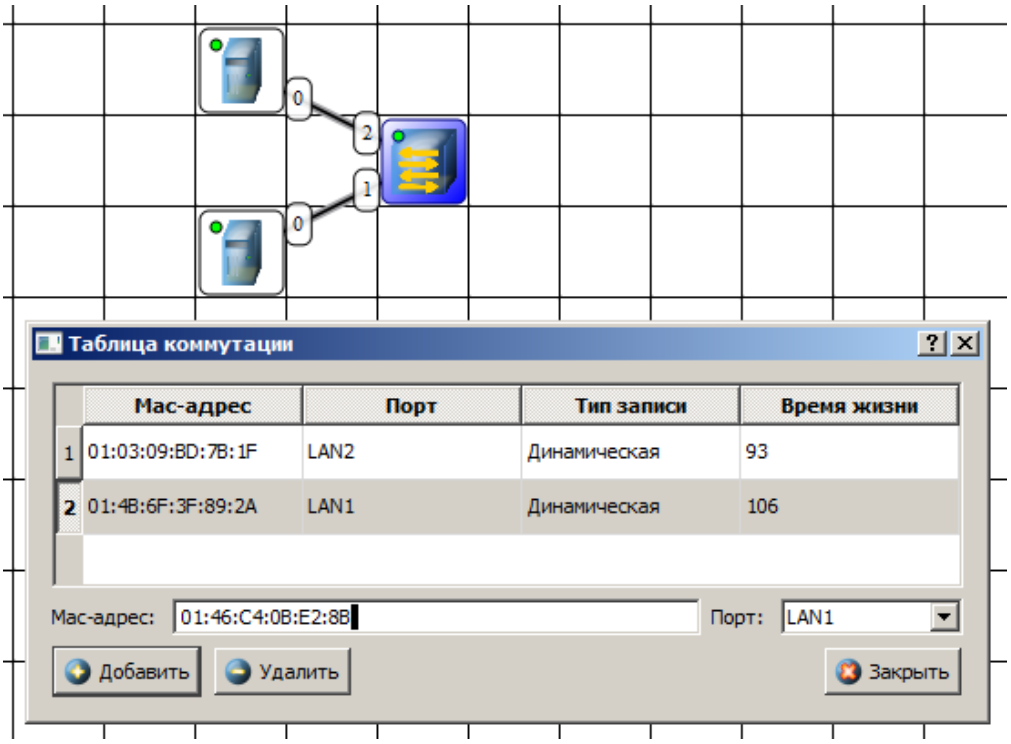


Рис. 11.13. Схема сети по топологии звезда построена

На рисунке:

- красный индикатор означает, что устройство не подключено;
- желтый - устройство подключено, но не настроено;
- зеленый - знак того, что устройство подключено, настроено и готово к работе.

Пример 2. Изучаем сеть из двух подсетей и маршрутизатора

Постройте новую сеть (рис. 11.14). Разобьем нашу сеть на 2 подсети. Допустим, у нас есть пул адресов сети класса С. Разобьем его на 2 части: 192.168.1.0-192.168.1.127 (слева) и 192.168.1.128-192.168.1.255 (справа) с маской 255.255.255.128.

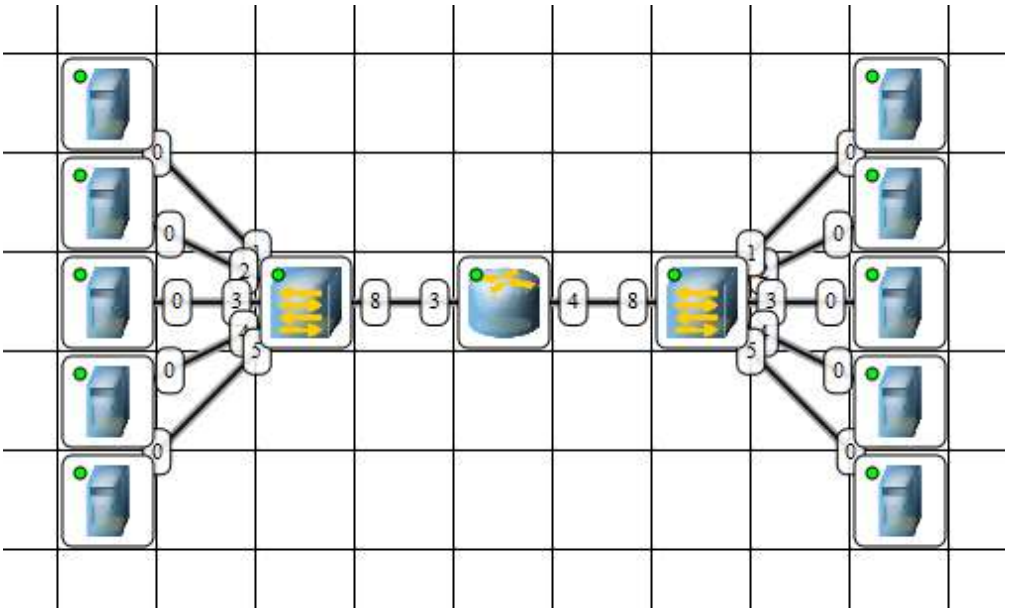


Рис. 11.14. Вариант сети из двух подсетей, соединенных маршрутизатором

Обратите внимание на то, что число портов у коммутатора можно задавать. У нас на рисунке коммутатор шестипортовый.

Настройка компьютеров

Для настройки ip-адреса интерфейса ПК из меню правой кнопки мыши открываем окно **Интерфейсы** и для левой (первой), подсети выставляем ip-адреса от 192.168.1.1 до 192.168.1.5 и маску подсети 255.255.255.128. Затем для правой (второй) подсети выставляем ip-адреса от 192.168.1.129 до 192.168.1.133 и маску подсети 255.255.255.128. После нажатия на кнопку "ОК" или "Применить", мы можем наблюдать, как индикатор поменял цвет с желтого на зеленый и от нашего устройства, которому сейчас дали адрес, побежал кадр Arp-протокола. Это нужно для того, чтобы выявить, нет ли в нашей сети повторения адресов. В поле "Описание" необходимо имя каждому компьютеру. Оно в дальнейшем будет всплывать в подсказке при наведении мыши на устройство, а также при открытии журнала для устройства заголовок будет содержать именно это описание.

Настройка маршрутизатора

Пока послать сообщения из одной такой подсети в другую мы не можем. Необходимо дать IP адреса каждому интерфейсу маршрутизатора, а на конечных узлах установить шлюзы по умолчанию. В подсети левее маршрутизатора у всех узлов должен быть шлюз 192.168.1.126, правее - 192.168.1.254 (рис. 11.15 и рис. 11.16).

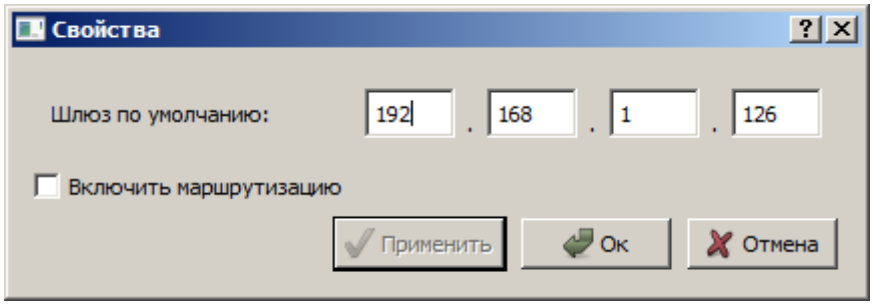


Рис. 11.15. Настройка шлюза по умолчанию, а также IP и маски для LAN3 (для левой подсети)

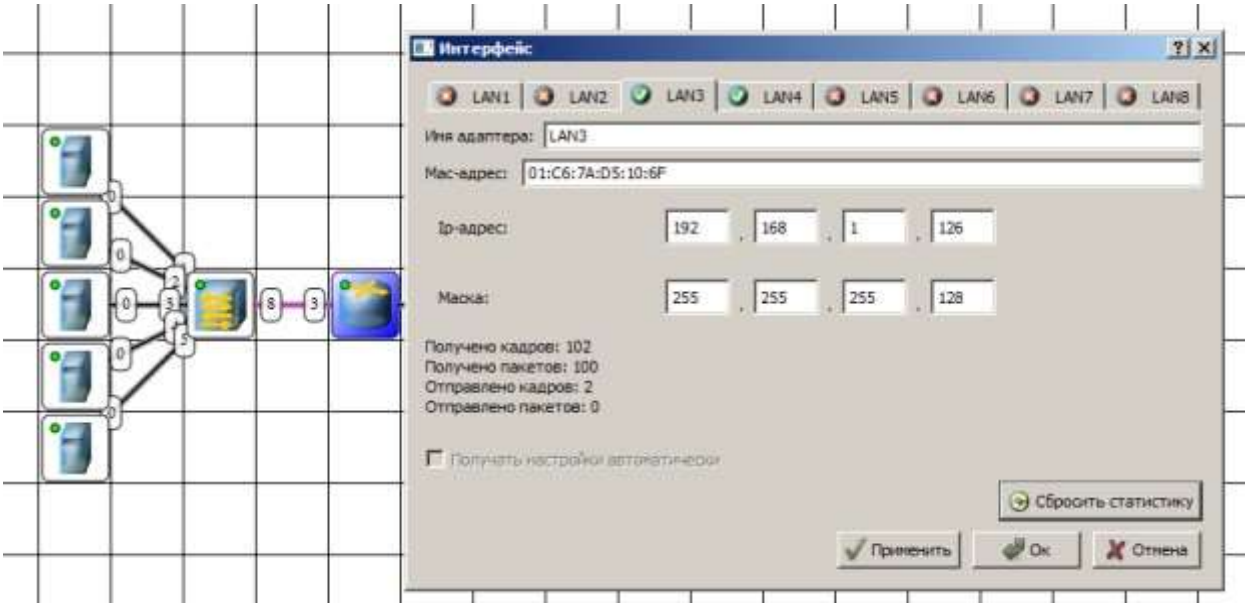


Рис. 11.16. Настройка шлюза по умолчанию, а также IP и маски для LAN4 (для правой подсети)

Шлюзы мы задали и теперь у нас полностью рабочая сеть. Давайте рассмотрим свойства ее

объектов.

Свойства коммутатора. Откроем его таблицу коммутации (рис. 11.17). Сейчас она абсолютно пустая, т.к. не было ни одной передачи данных. Но при этом у нас есть возможность добавить статическую запись, для этого необходимо заполнить все поля соответствующими данными и нажать кнопку "Добавить".

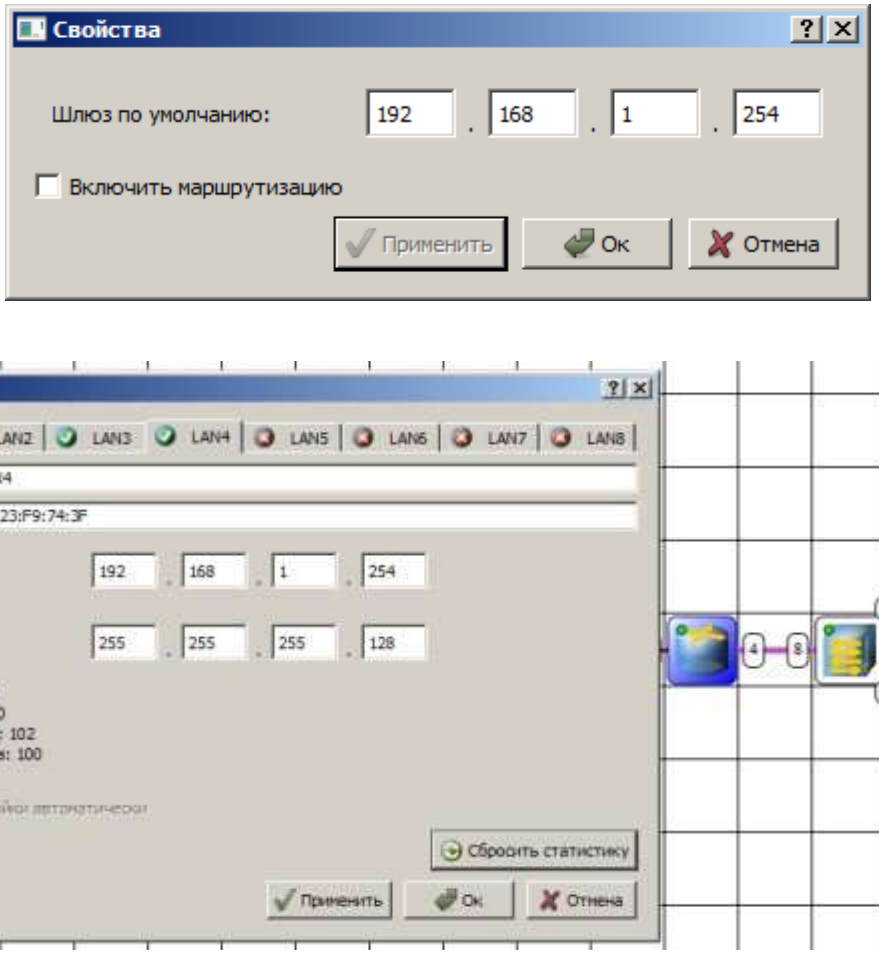


Рис. 11.17. Таблица коммутации коммутатора

Свойства маршрутизатора

В контекстном меню изучим пункты: Таблица маршрутизации, Arp-таблица, Программы. **Arp-таблица** пуста (по той же причине, что и таблица коммутации), но в нее также можно добавить

статические записи. В **таблице маршрутизации** мы видим 2 записи (рис. 11.18). Эти записи соответствуют нашим подсетям, о чем говорят надписи в столбце **Источник**. В качестве источника может быть протокол RIP, установить который можно с помощью пункта **Программы**. В столбец **Шлюз** заносится адрес следующего маршрутизатора (или адрес шлюза, если другого маршрутизатора нет). В столбце **Интерфейс** адрес порта, с которого будем отправлять данные. В эту таблицу тоже можно занести статические записи, а в столбце **Источник** появится надпись **Статическая**.

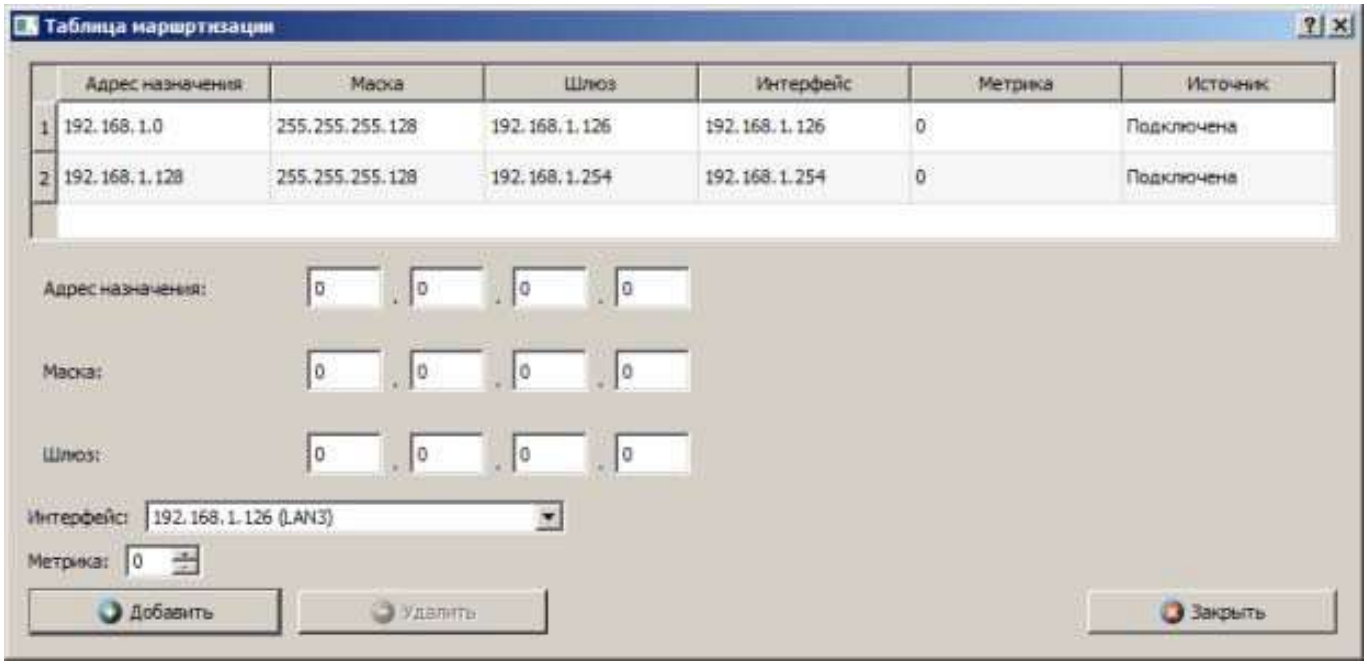


Рис. 11.18. Таблица маршрутизации маршрутизатора

Тестирование сети (Отправка пакетов)

Давайте проверим, насколько правильно функционирует сеть. Для того, чтобы отправить пакеты, выберите на панели инструментов значок  . При наведении мыши на рабочую область вы увидите оранжевый кружок, это значит, что надо указать от какого компьютера данные будут отправлены. Мы пошлем данные от компьютера, отмеченного на рисунке стрелкой (рис. 11.19).

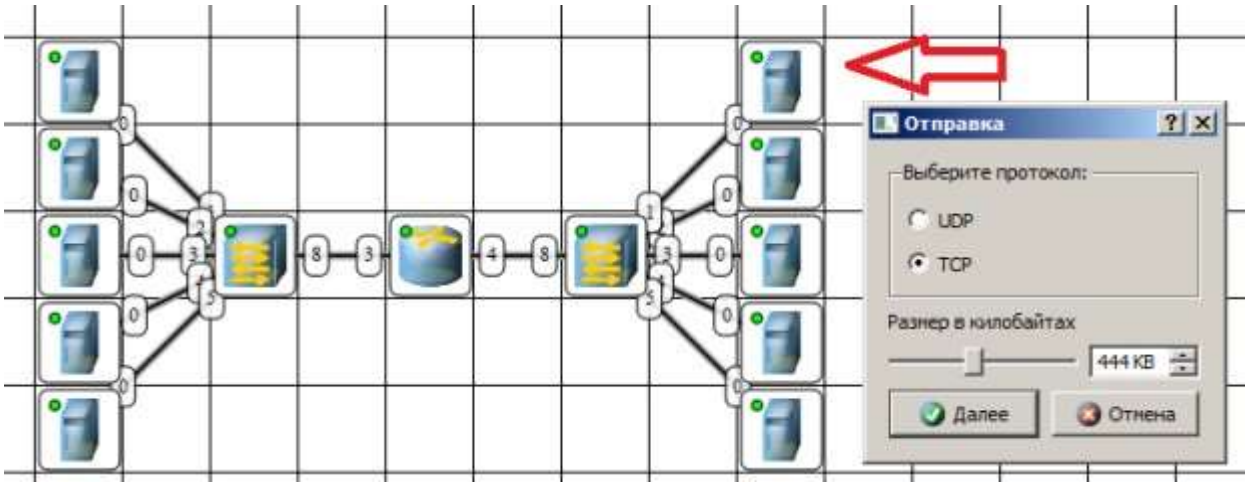


Рис. 11.19. Показан ПК, оправляющий данные

Нажимаем на кнопку **Далее**. Теперь вам надо выбрать получателя (рис. 11.20).

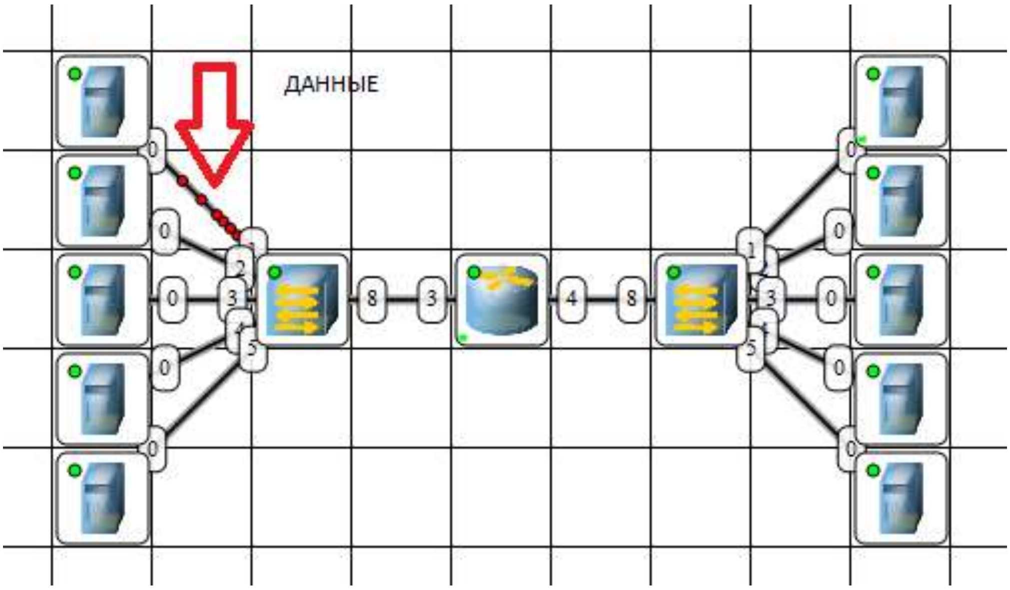


Рис. 11.20. Показан ПК, получающий данные

Далее нажимаем кнопку **Отправка** и наблюдаем бегущие по сети кадры (рис. 11.21).

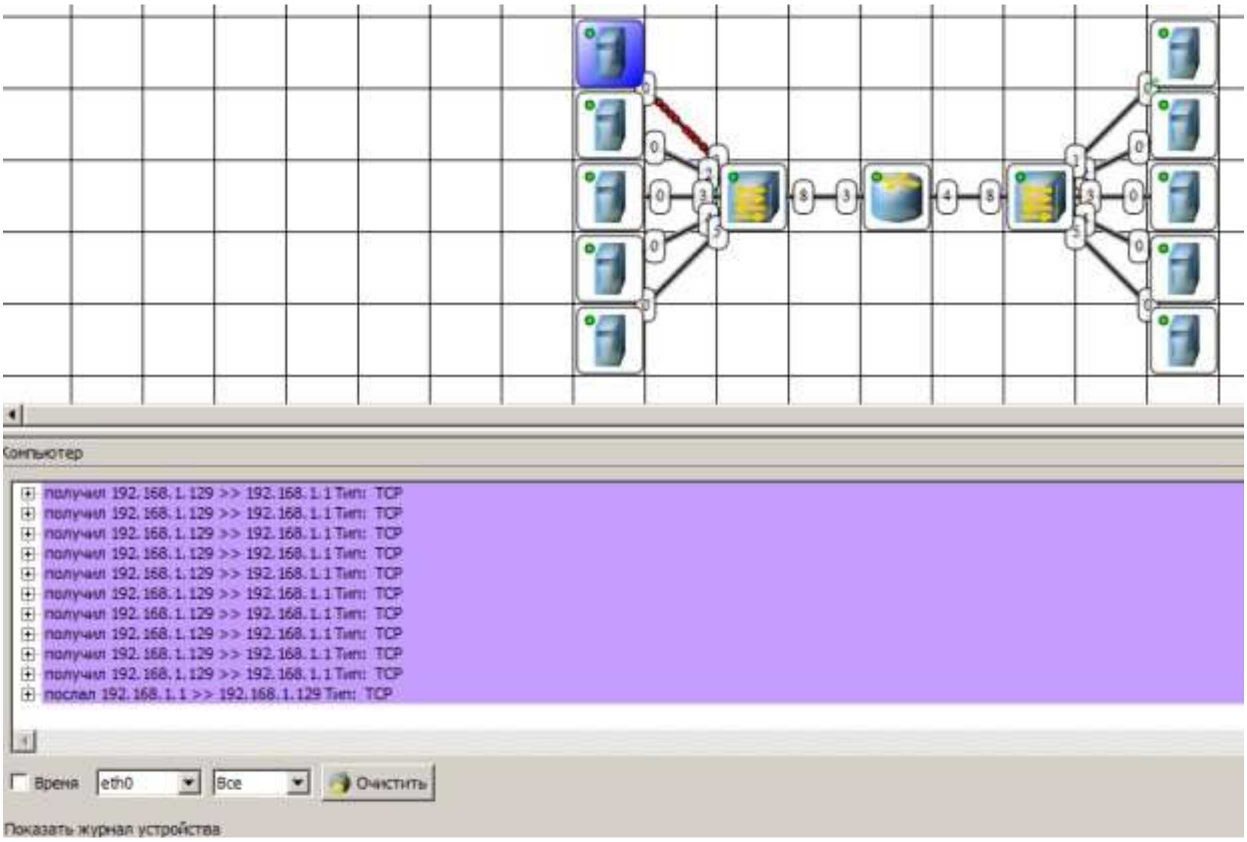


Рис. 11.21. По сети идут кадры данных

У каждого устройства в контекстном меню есть пункт "Показать журнал", можно открыть этот журнал и увидеть всю необходимую информацию о пакете, пришедшем (или отправленном), и его содержимое.

Рис. 11.22. Журнал устройства показывает, какую информацию содержали кадры данных

Задание 2. Построить сеть из восьми ПК, хаба, коммутатора и роутера. Настроить ее правильную работу

Построить сеть как на рис. 11.23 и настройте ее работу.

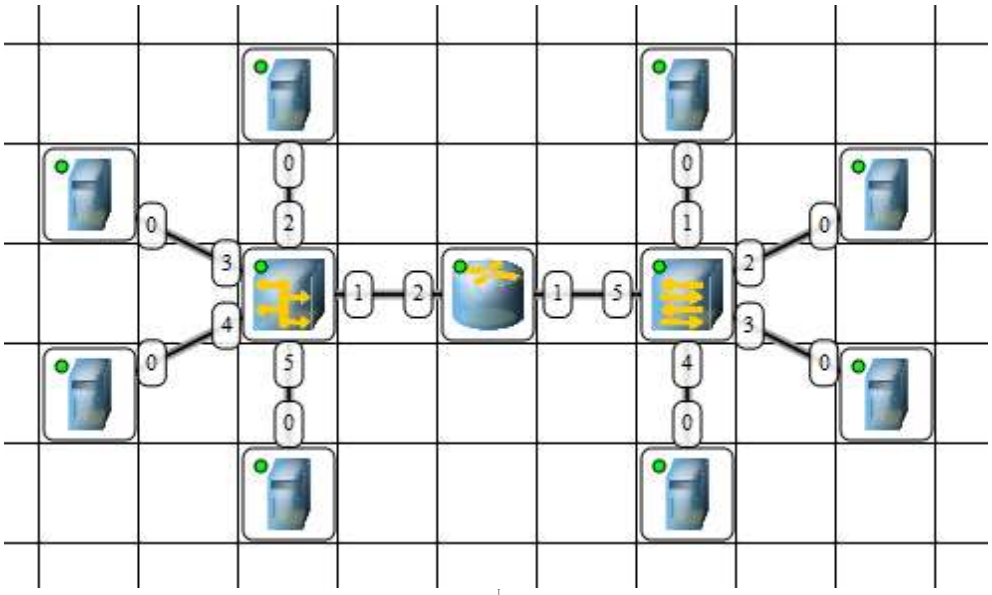


Рис. 11.23. Две подсети по топологии звезда

Оформить отчет в электронном виде и выслать преподавателю