МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Колледж экономики, управления и права

Методические указания по организации практической работы студентов по учебной дисциплине Компьютерные сети

09.02.05 Прикладная информатика (по отраслям)

Ростов-на-Дону

2017

Методические указания по учебной дисциплине Компьютерные сети разработаны с учетом ФГОС среднего профессионального образования специальности 09.02.05. Прикладная информатика (по отраслям), предназначены для студентов и преподавателей колледжа.

Методические указания определяют этапы выполнения работы на практическом занятии, содержат перечень вопросов для самопроверки знаний, а также список рекомендуемой литературы.

Составитель: А.С. Пегливанова преподаватель колледжа ЭУП

Рассмотрены на заседании предметной (цикловой) комиссии специальности 09.02.05 Прикладная информатика (по отраслям)

Протокол № 1 от «30» августа 2017г

Председатель П(Ц)К специальности _____ Л.А.Шевченко
личная подпись

и одобрены решением учебно-методического совета колледжа.
Протокол № 1 от «31» 08 2017г

Председатель учебно-методического совета колледжа
_____ С.В.Шинакова
личная подпись

Рекомендованы к практическому применению в образовательном процессе.

Рецензенты:

Содержание:

Практическая работа №1.

Тема: «Присвоение имени компьютеру и рабочей группе. Установка дополнительных сетевых настроек.»

Цель работы: приобретение знаний и практических навыков, необходимых для присвоения имени компьютеру и рабочей группе, а также установки дополнительных сетевых настроек.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения.

Каждый компьютер в сети должен иметь свое уникальное имя, чтобы компьютеры могли однозначно идентифицировать друг друга и взаимодействовать. Целесообразно присваивать компьютерам короткие (не более пятнадцати символов) и понятные имена.

Для имени компьютера рекомендуется использовать только стандартные символы Интернета. Такими символами являются числа от 0 до 9, заглавные и строчные буквы от A до Z, а также символ переноса (-). Имена компьютеров не могут состоять из одних цифр и содержать пробелы. Кроме того, в имена нельзя

включать специальные знаки, например:

< > ; : " * + = \ | ? ,

При настройке сети системой Windows автоматически создается рабочая группа, которой присваивается имя. Можно как присоединиться к уже существующей рабочей группе в сети, так и создать новую.

Домены, рабочие группы и домашние группы представляют разные методы организации компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.

Рабочая группа – это группа компьютеров, подключенных к сети, которые совместно используют ресурсы. При настройке сети операционная система Windows автоматически создает рабочую группу и присваивает ей имя по умолчанию.

Домен — это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.

Рабочие группы служат основой для общего доступа к файлам и принтерам, но не осуществляют фактическую настройку общего доступа.

1. **Ход выполнение работы.**

1. Присвоение имени компьютеру.

1. Откройте Панель управления - Система – Просмотр имени этого компьютера – Изменить параметры
2. При появлении запроса пароля администратора или подтверждения введите пароль или предоставьте подтверждение.
3. На вкладке Имя компьютера нажмите Изменить.

2. Присвоение имени рабочей группе.

1. Открыть окно «Система».
2. В группе Имя компьютера, имя домена и параметры рабочей группы нажмите кнопку Изменить параметры. При появлении запроса пароля администратора или подтверждения введите пароль или предоставьте подтверждение.
3. В диалоговом окне Свойства системы перейдите на вкладку Имя компьютера и затем нажмите кнопку Изменить.

4. В диалоговом окне Изменение имени компьютера или домена щелкните в разделе Член групп пункт Рабочая группа и выполните одно из следующих действий.

- Чтобы присоединиться к существующей рабочей группе, введите имя рабочей группы, к которой будет присоединен компьютер, а затем нажмите ОК.
- Чтобы создать новую рабочую группу, введите имя новой рабочей группы, а затем нажмите ОК.

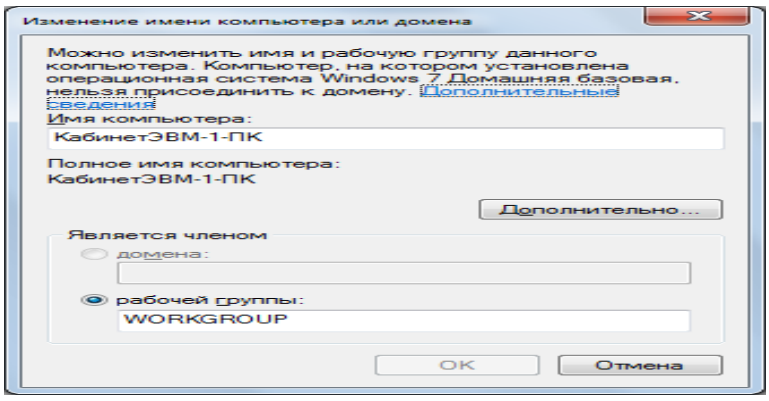


Рис.1. Диалоговое окно «Изменение имени компьютера или домена»

Если перед присоединением к рабочей группе компьютер входил в домен, то он будет удален из него, а учетная запись компьютера в домене будет отключена.

4. Присвойте старое имя компьютеру и рабочей группе.

5. Установка дополнительных сетевых настроек.

Настройке сетевого подключения на компьютере с Windows 7.

Зайдите в Панель управлении - Система и безопасность, а в нем — пункт Система.

Чтобы изменить имя рабочей группы или компьютера, нажмите на ссылку Изменить параметры (она находится справа). Лучше, если имена рабочих групп в обоих компьютерах совпадают, а имена самих компьютеров — нет.

Вернитесь в Панель управления и выберите пункт Сеть и Интернет, а в нем — Центр управления сетями и общим доступом. В боковом меню будет пункт Изменение параметров адаптера, выберите его. В нем должен быть ярлык под названием Подключение по локальной сети. Если он имеет серый цвет и подписан Отключено, кликните правой кнопкой мыши и выберите пункт Включить. Затем в контекстном меню ярлыка выберите пункт Свойства. В диалоговом окне выберите пункт Протокол Интернета версии 4 (TCP/IPv4), снова нажмите на кнопку Свойства. Впишите IP-адрес (192.168.35.68.) и маску подсети (255.255.255.0), сохраните изменения.

Вернитесь в Центр управления сетями и общим доступом, в левом нижнем углу будет ссылка —Домашняя группа, нажмите на нее. В появившемся окне нажмите на ссылку Что такое расположение в сети?. В окне настроек сетевого размещения вам нужно выбрать расположение сети Неопознанная сеть — выберите пункт Домашняя сеть. Затем появится окно для настройки общего доступа к папкам — можно пропустить этот шаг, сняв все галочки и нажав кнопку Далее. Пароль для домашней группы настраивать тоже не обязательно, просто нажмите на кнопку Готово.

Снова зайдите в Центр управления сетями и общим доступом, сверху в левой колонке нажмите на ссылку Изменить дополнительные параметры общего доступа. Текущим профилем должен быть Домашний или рабочий. В этом профиле найдите последний пункт (Подключения домашней группы), установите переключатель на Использовать учетные записи пользователей и

пароли для подключения к другим компьютерам, сохраните изменения, выйдите из системы и зайдите снова (Пуск — Завершение работы — Выйти из системы).

Для того, чтобы окончательно настроить сеть между Windows XP и Windows 7, зайдите в проводник и расшарьте папки на компьютере с Windows 7. Для этого щелкните по папке правой кнопкой мыши, выберите пункт контекстного меню Общий доступ, в нем — Конкретные пользователи. Здесь выбираются учетные записи Windows 7, с помощью которых можно будет подключиться к компьютеру с Windows XP. Нажмите кнопку Общий доступ

Практическая работа № 2.

Тема: «Настройка доступов к ресурсам ПК для других участников сети. Установка паролей»

Цель работы: научиться устанавливать и настраивать доступ к ресурсам ПК других участников сети.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения

Первым этапом будет создание пустой папки в корне диска. Ей нужно дать удобное для вас имя на английском языке, к примеру SHARE_foto. Далее кликаем правой кнопкой мыши по папке и в открывшемся диалоговом окне выбираем пункт «Свойства». В этом окне переходим к вкладке «Доступ», здесь нам нужно отметить птичками (галочка) пункты «Открыть общий доступ к этой папке», а так же «Разрешить изменение файлов по сети». После этого кликаем по кнопке «Ок».

Осуществив настройки таким образом, мы открыли доступ к этой папке другим пользователями подключенных к сети. Название папки с такими функциями «расширенная папка» (от англ. «share»). Так же измениться иконка, она примет вид папки с рукой, вот так:

Хочу дополнить что при этих настройка другим пользователям будет открыт доступ просмотра этой папке («по умолчанию»). Если вы хотите чтобы другие пользователи могли изменять содержимое данной папке (изменять, удалять, копировать файлы и вставлять свои), необходимо изменить ещё одну настройку, которая позволит дать этой папке такую возможность. Для этого перейдем в меню «Сервис» в окне локального диска (это там где была созданная расшаренная папка) переходим во вкладку «Вид» и убираем галочку возле пункта «Использовать простой общий доступ к файлам (рекомендуется)». И кликаем по кнопке «Ок».

Далее мы снова переходим к редактированию нашей папки и кликаем правой кнопкой мыши и в открывшемся диалоговом окне выбираем пункт «Свойства». И вы сможете наблюдать большее количество вкладок. Переходим во вкладку «Доступ». Тут вы увидите новые настройки: в поле «Примечание» мы вводим что то вроде комментария к данной папке которое будут видеть другие пользователи, оно обязательное для заполнения, после мы вводим число пользователей которое могут одновременно просматривать данную папке (в поле «Предельное число пользователей»).

Теперь мы можем перейти к настройкам «Расширения», кликните по этой кнопке и в открывшемся диалоговом окне поставьте галочку напротив пункта «Изменение». Этими действиями вы открываете доступ другим пользователям на изменение данных в этой папке, а не только просмотра (пункт «Чтение»). Для того чтобы настройки вступили в силу, кликаем по кнопке «Ок».

Порядок выполнения работы:

Создать у себя на компьютере папку с названием группы.

1. Настроить к ней общий доступ с полными правами.
2. В ней создать текстовый файл со следующими характеристиками: имя файла – фамилия (или фамилии студентов, работающих за этим компьютером), содержимое – IP адрес компьютера, его имя в сети, имя рабочей группы, перечислить все компьютеры в этой рабочей группе.
3. Передать свой файл по сети всем студентам на занятии.
4. Забрать такой же файл с компьютера справа, добавив к его имени знак «+».
5. Создать папку с ограниченными правами (только для чтения). Протестируйте свою папку с чужого компьютера на возможность записи в ней.
6. Задайте пароль для доступа к своей папке.

Вопросы к защите:

1. Каким образом внешний компьютер идентифицируется на вашем компьютере?
2. Дайте определение одноранговых локальных вычислительных сетей.
3. Как осуществить доступ к Вашим каталогам с другого ПК?

Практическая работа №3.

Тема: «Подключение ресурса сети в качестве сетевого диска. Ограничение доступа к ресурсам.»

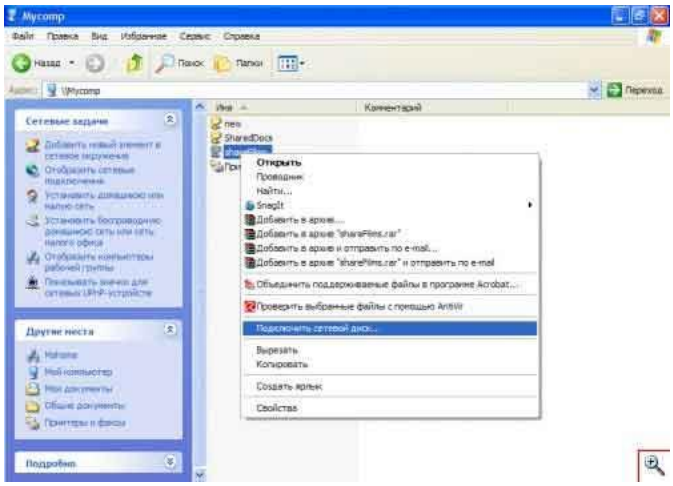
Цель работы: приобретение знаний и практических навыков, необходимых для присвоения подключения ресурса сети в качестве сетевого диска.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

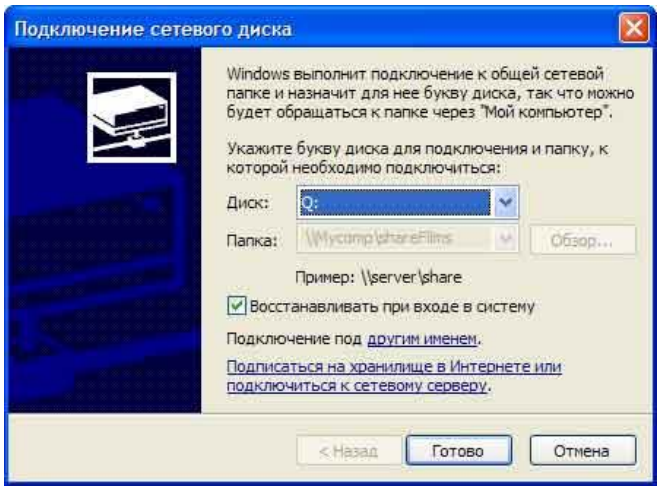
Теоретические сведения.

Как вы уже заметили, поиск сетевой папки занимает длительное время, а так же нагружает систему. Более практичным вариантом будет подключение сетевого диска к вашему компьютеру. Если сделать это, то вы будет видеть его в списке локальных дисков в папке «Мой компьютер». Так же это позволить ускорить процесс работы с расширенными папками.

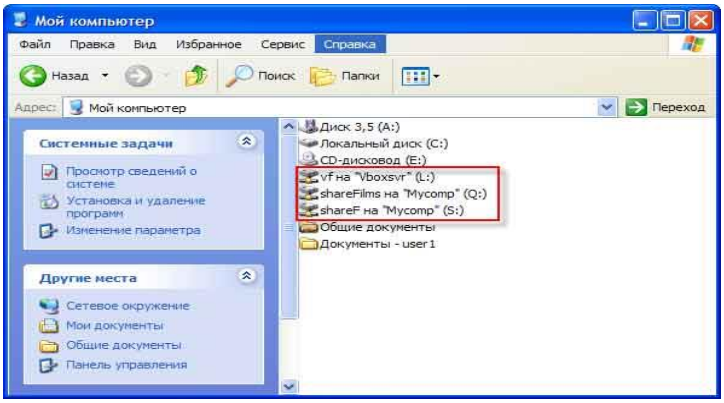
Для этого, мы переходив в «Сетевое окружение», по этому пути: «Пуск» -> «Сетевое окружение», здесь выберем интересующий нас компьютер который подключен к локальной сети и зайдя в него найдем папку с общим доступом, которую мы и будет подключать к вашему компьютеру как сетевой локальный диск. Кликаем по этой папке правой кнопкой мыши и в открывшемся диалоговом окне выбираем пункт «Подключить сетевой диск».



Далее откроется ещё одно окно, где нам будет предложено выбрать букву сетевого локального диска. Знайте, что два диска с одинаковыми именами на вашем ПК не может быть! Ещё нам нужно выделить пункт «Восстанавливать при входе в систему», этот пункт позволит автоматически производить процесс поиска данной папки и включать его в список ваших дисков в папке «Мой компьютер».



Теперь простым входом в «Мой компьютер» вы просто можете увидеть и воспользоваться локальным сетевым диском. Любую расширенную папку локальной сети можно подключить к вашему компьютеру в качестве локального сетевого диска. Так же вы можете их различить по иконкам, они имеют вот такой вид:



Чтобы произвести отключение локального сетевого диска, нужно кликнуть по нему правой кнопкой мыши и в открывшемся диалоговом окне выбрать пункт «Отключить». Так следует дополнить, что отключив компьютер на котором находиться данный локальный диск, то этот диск будет недоступен на других компьютерах.

Ход выполнение работы.

Подключите 3 сетевых диска с других ПК.

1. Покажите преподавателю.
2. Удалите, созданные вами диски.

Практическая работа №4

Тема: «Подключение и настройка сетевого адаптера»

Цель работы: приобретение знаний и практических навыков, необходимых для подключение и настройки сетевого адаптера

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения.

Как установить новый сетевой адаптер

1. Прикоснитесь антистатическим наручным браслетом на вашем запястье к корпусу компьютера для снятия электростатистического заряда.
2. Убедитесь, что компьютер выключен, а силовой кабель отключен от сети.
3. Откройте корпус компьютера. Попросите преподавателя помочь вам и проконсультировать вас, как открыть корпус компьютера.

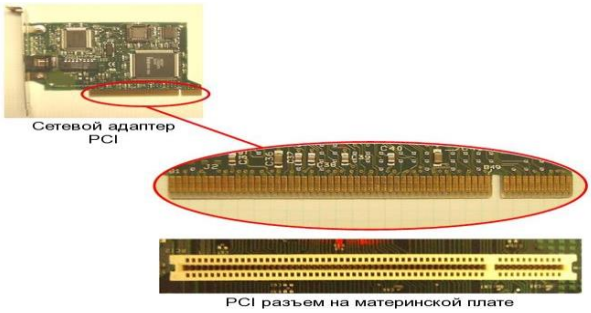


Схема 4.2

4. Найдите свободный PCI разъем в материнской плате. Разъемы PCI легко отличимы за счет своего белого или бежевого цвета. Посмотрите на схему 4.2.
5. Открутите винт и извлеките металлическую заглушку разъема из компьютера. Посмотрите на схему 4.3.

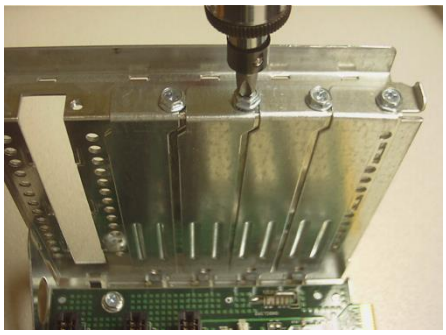


Схема 4.3

6. Вставьте сетевой адаптер в свободный PCI разъем. Убедитесь, что он полностью вошел в разъем. Посмотрите на схему 4.4.

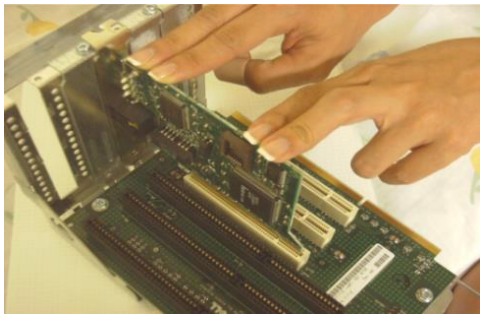


Схема 4.4

7. Надежно прикрутите плату к корпусу компьютера откученным ранее винтом. Заглушку слота, извлеченную из корпуса, следует сохранить. Посмотрите на схему 4.5.

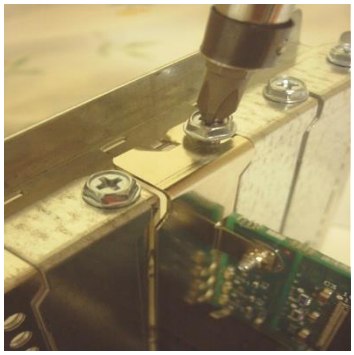


Схема 4.5

8. . Закройте корпус компьютера.

Как сконфигурировать новый установленный сетевой адаптер

9. Включите компьютер и войдите в систему, используя имя пользователя и пароль, предоставленные вам преподавателем.

10. Драйверы Windows XP поддерживают много различных типов аппаратного обеспечения. Если Windows XP имеет подходящий драйвер для установленного сетевого адаптера, драйвер будет установлен автоматически. Вы можете получить или не получить сообщение о том, что драйвер был установлен.

11. Для того, чтобы проверить, успешно ли система Windows XP сконфигурировала и установила новое оборудование, правой кнопкой мыши щелкните на **Мой компьютер** и выберите **Управление**. Щелкните дважды по **Диспетчер устройств** и найдите компонент **Сетевые платы**. Раскройте компонент **Сетевые платы,** при этом должен появиться установленный сетевой адаптер. Если установленный сетевой адаптер не появился в списке, драйвер для него необходимо установить вручную. Переходите к следующему шагу нашей инструкции для того, чтобы установить драйвер вручную. Если у вас не возникло проблем с установкой драйвера, переходите к следующей секции нашей инструкции. Посмотрите на схему 4.6.

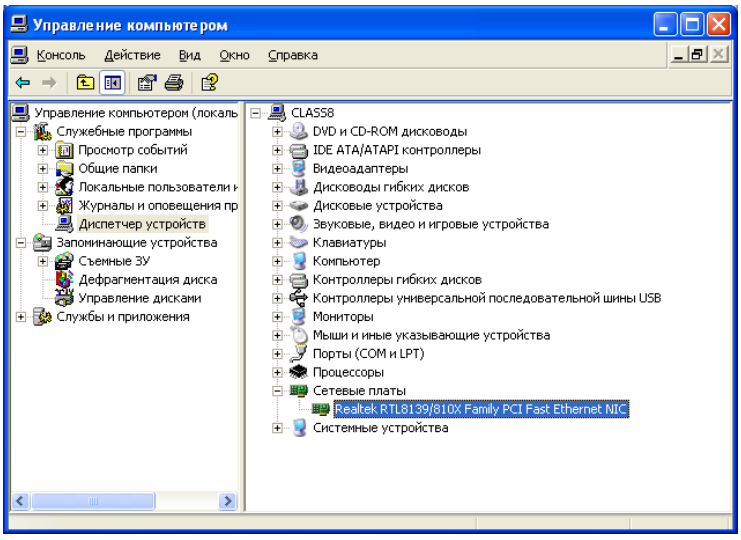


Схема 4.6

12. Щелкните **Пуск**, щелкните **Панель управления,** затем щелкните **Принтеры и другое оборудование**.

13. В левой части окна щелкните **Установка оборудования**.

14. Запустится **Мастер установки оборудования**. Следуйте инструкциям, и когда получите запрос на дискету или CD, содержащий драйверы, предоставьте правильные файлы

драйвера. Преподаватель может выдать учащимся требуемые файлы драйвера, если их нет в списке известных устройств Windows XP.

Как присоединить компьютер к рабочей группе

1. Правой кнопкой мыши щелкните **Мой компьютер,** затем выберите **Свойства**. Появится окно **Свойства системы**. Щелкните по вкладке **Имя компьютера**. Щелкните по кнопке **Изменить…** для того, чтобы начать процесс присоединения к рабочей группе. Посмотрите схему 4.7.

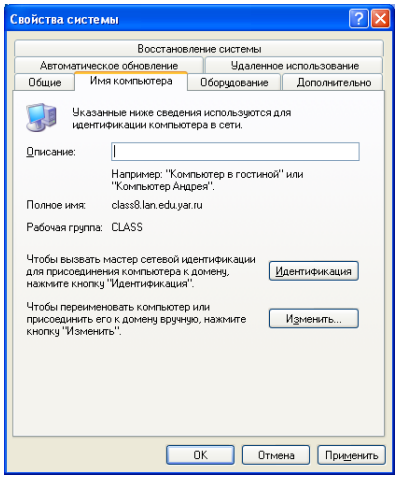


Схема 4.7

Появится окно Изменение имени компьютера. Выберите опцию Является членом рабочей группы. По умолчанию Windows XP использует WORKGROUP в качестве названия рабочей группы. Каждый компьютер должен иметь свое уникальное имя Имя компьютера. Посмотрите на схему 4.8.

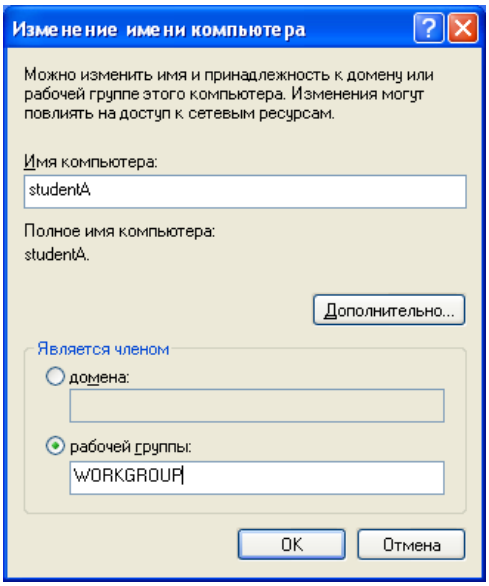


Схема 4.8

2. Щелкните **OK** для того, чтобы закрыть окно.
3. Щелкните **OK** для запуска процесса подсоединения к рабочей группе **WORKGROUP**.
4. Если процесс присоединения к рабочей группе прошел успешно, всплывет сообщение **Добро пожаловать в рабочую группу WORKGROUP**. Щелкните **OK** для того, чтобы закрыть его. Посмотрите на схему 4.9.

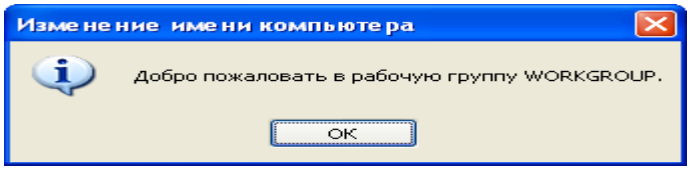


Схема 4.9

5. Далее система спросит вас, перезагрузить ли компьютер для завершения процесса. Щелкните **Да** для перезагрузки системы.

Как настроить конфигурацию сетевого адаптера для получения доступа к Интернет

Войдите в систему с соответствующим **Именем пользователя** и **Паролем**, который вы получите от преподавателя.

1. Правой кнопкой мыши щелкните **Сетевое окружение** на вашем рабочем столе, затем выберите **Свойства**. Появится окно **Сетевые подключения**, показывающее имеющиеся соединения локальной сети или соединения с Интернет. (Обратите внимание: схема 4.10 показывает два соединения **Подключение по локальной сети,** в вашем случае может быть только одно соединение.)

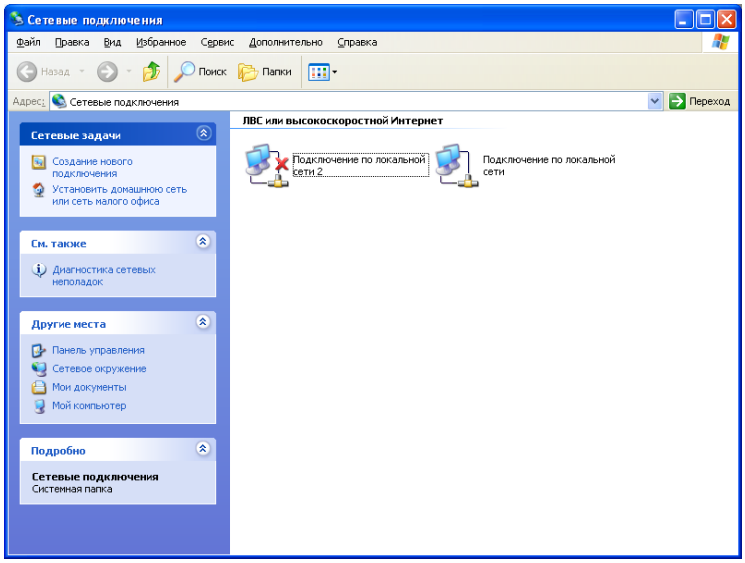


Схема 4.10

2. Правой кнопкой мыши щелкните **Подключение по локальной сети,** затем выберите **Свойства**. Появится окно **Подключение по локальной сети - свойства**. В окне **Отмеченные компоненты используются этим подключением:** щелкните **Протокол Интернета**, затем щелкните **Свойства.** Посмотрите на схему 4.11.

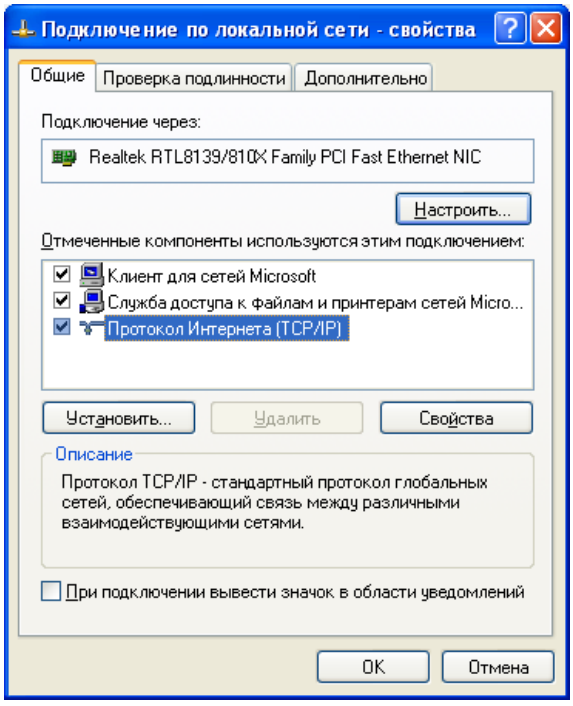


Схема 4.11

3. Появится окно **Свойства: Протокол Интернета (TCP/IP)**. Обратите внимание на вкладку **Общие**, где уже выбрано **Получить IP-адрес автоматически**. Щелкните **Использовать следующий IP-адрес**, при этом обратите внимание, что **Использовать следующие адреса DNS-серверов** также уже выбрано. Посмотрите на схему 4.12.

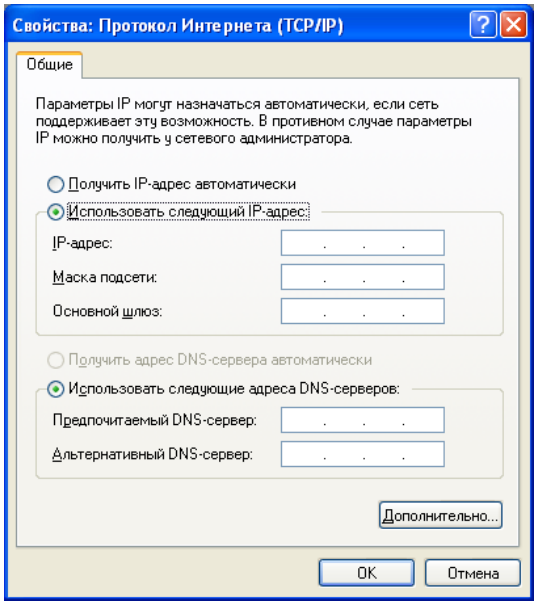


Схема 4.12

4. Используйте **IP-адрес, Маску подсети, Основной шлюз, Предпочитаемый DNS-сервер** и **Альтернативный DNS-сервер,** предоставленные вашим преподавателем. Посмотрите пример на схеме 4.13.

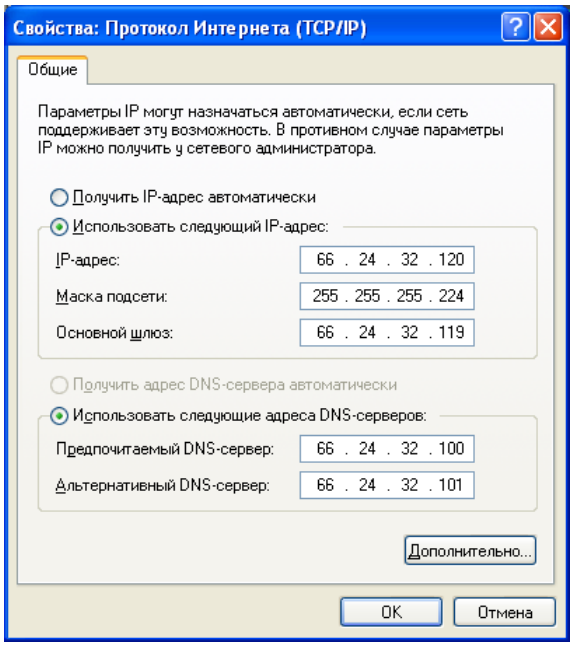


Схема 4.13

5. Щелкните **OK** в окне **Свойства: Протокол Интернета (TCP/IP)**, затем щелкните **OK** в **Подключение по локальной сети - свойства.**

6. Теперь ваше местное подсоединение настроено для связи с провайдером услуг Интернет и доступа к сети Интернет. Закройте все имеющиеся окна.

Проверьте свое подключение к Интернет

7. Для проверки Интернет-подключения откройте **Internet Explore.** Введите **http://www.microsoft.ru/** в адресную строку. Нажмите **Переход** или **Enter** для загрузки веб-страницы.

Практическая работа № 5

Тема: «Оценка пропускной способности каналов связи»

Цель работы: приобретение знаний и практических навыков, необходимых для оценки пропускной способности каналов связи.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения.

Пропускная способность канала связи - Наибольшая скорость передачи информации по каналу связи. Скорость передачи зависит от физических свойств канала связи, статистических свойств помех, способа передачи и приема сигналов и др.

Пропускная способность двоичного канала

Нарисуем схему передачи информации.

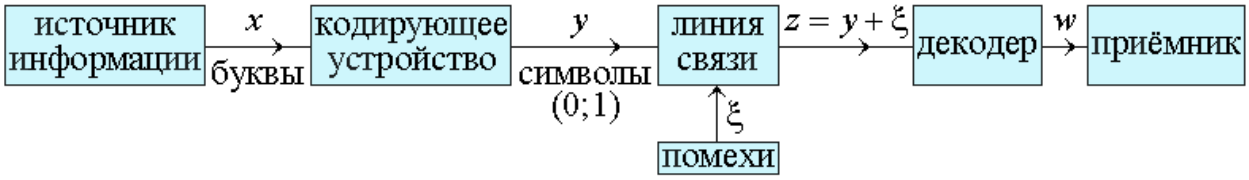


Рис. 2.9

Будем передавать по линии связи последовательность двоичных символов, состоящую из нулей и единиц. Помехи в линии связи могут превратить ноль в единицу и наоборот. Представим себе модель двоичной линии связи.

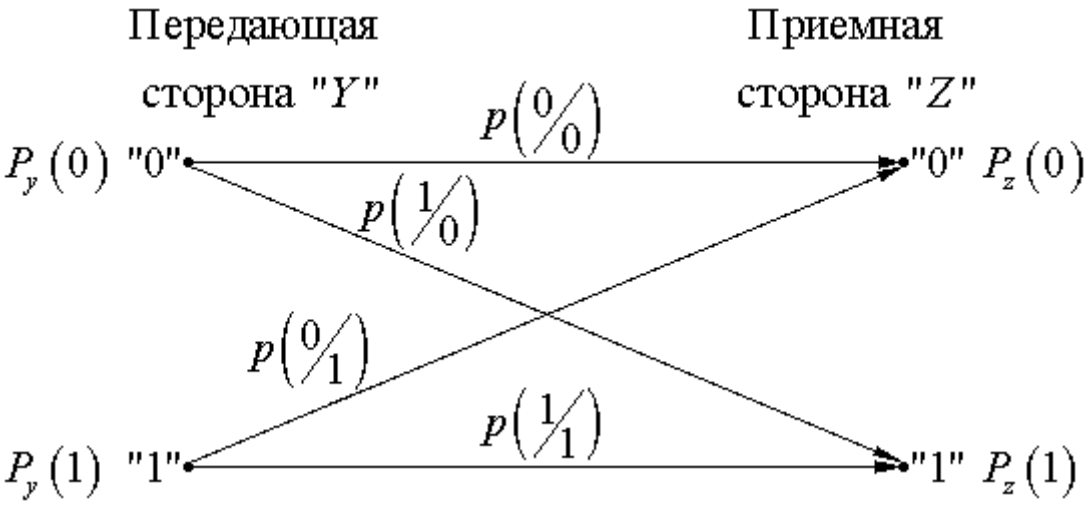


Рис. 2.10

Введены следующие обозначения:

вероятность безошибочной передачи "0" – , т.е. вероятность получения "0" на приёмной стороне, если передавался "0";

$p(1/0)$ – вероятность получения единицы на приёмной стороне, если передавался "0";

аналогично введем и ;

$P_y(0)$ и $P_y(1)$ – вероятности встречаемости нуля и единицы на передающей стороне;

$P_z(0)$ и $P_z(1)$ – вероятности встречаемости нуля и единицы на приёмной стороне.

Конечно, выполняются условия:

$$P_y(0)+P_y(1)=1;\quad p\left(\frac{0}{0}\right)+p\left(\frac{1}{0}\right)=1;$$

$$P_z(0)+P_z(1)=1;\quad p\left(\frac{1}{1}\right)+p\left(\frac{0}{1}\right)=1.$$

Подсчет пропускной способности линии связи будем вести по формуле:

$$C_{\text{лс}}=\max_{p_y(0)} I_{\text{на1 символ}}(Z;Y)V_{\text{лс max}},\quad (2.1)$$

где $V_{\text{лс max}}$ – максимальная скорость передачи импульсов по данной линии связи;

$\max_{p_y(0)} I_{\text{на1 символ}}(Z;Y)$ – максимальное количество информации, приходящееся в среднем на один символ.

$V_{\text{лс max}}$ считается по формуле

$$V_{\text{лс max}}=\frac{1}{\Delta t_{\min}}\left[\text{имп}/\text{сек}\right],\ (2.2)$$

где Δt_{min} – минимально допустимый интервал времени для передачи по данной линии связи. Он определяется физическими свойствами линии связи (тонкий или толстый коаксиал; витая пара; оптический канал). Δt_{min} определяется по формуле Котельникова В.А. (будет рассмотрена в главе 8) по формуле:

$$\Delta t_{\min}=\frac{1}{2F_{\max}}[\text{сек}],\ (2.3)$$

где F_{max} – максимальная частота, пропускаемая этим каналом. Она определяется экспериментально путём подачи на вход канала сигнала постоянной амплитуды и переменной частоты. http://peredacha-informacii.ru/ Если амплитуда на выходе канала упадет до , то эта частота и принимается за максимальную (см. рис. 2.11).

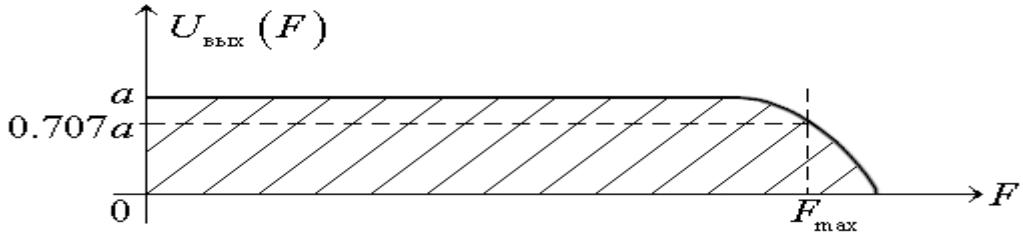


Рис. 2.11

$\max_{p_y(0)} I_{\text{на1 символ}}(Z;Y)$

зависит от помех и от вероятностей встречаемости нулей и единиц на передающей стороне

$$I_{\text{нал символ}}(Z;Y) = H_{\text{апр}}(Z) - H_{\text{апост}}\left(Z/Y\right). \quad (2.4)$$

$$H_{\text{апр}}(Z) = -P_z(0)\log P_z(0) - P_z(1)\log P_z(1). \quad (2.5)$$

$$H_{\text{апост}}\left(Z/Y\right) = \sum_{i=1}^{2} P_y(i)\cdot H\left(Z/i\right) = P_y(0)\cdot H\left(Z/0\right) + P_y(1)\cdot H\left(Z/1\right) =$$
$$= P_y(0)\cdot\left[-P\left(0/0\right)\log P\left(0/0\right) - P\left(1/0\right)\log P\left(1/0\right)\right] + \quad (2.6)$$
$$+\left[1-P_y(0)\right]\cdot\left[-P\left(1/1\right)\log P\left(1/1\right) - P\left(0/1\right)\log P\left(0/1\right)\right].$$

$H_{\text{апост}}(Z)$ – это остаточная неопределенность на приёмной стороне, если известно какой символ со стороны Y передавался.

$P_z(0)$ и $P_z(1)$ – определяют априорную неопределенность на стороне "Z". При этом

$$P_z(0) = P_y(0)\cdot P\left(0/0\right) + P_y(1)\cdot P\left(0/1\right); \quad (2.7)$$

$$P_z(1) = P_y(1)\cdot P\left(1/1\right) + P_y(0)\cdot P\left(1/0\right). \quad (2.8)$$

Все необходимые для расчета пропускной способности линии связи формулы приведены.

Рассмотрим три частных случая.

1. Отсутствие ошибок, т.е. .

Тогда $P_z(0) = P_y(0)$ и $P_z(1) = P_y(1)$; ;

$$\boxed{C_{\text{пс}}} = \max_{p_y(0)} I_{\text{нал символ}}(Z;Y)\cdot V_{\text{пс max}} = \max_{p_y(0)} H_{\text{апр}}(y)\cdot V_{\text{пс max}} = \quad (2.9)$$
$$= \underbrace{\max_{p_y(0)}\left(-P_y(0)\log P_y(0) - \left(1-P_y(0)\right)\log\left(1-P_y(0)\right)\right)}_{1}\cdot V_{\text{пс max}} = \boxed{V_{\text{пс max}}}.$$

То есть в этом случае максимальная пропускная способность линии связи равна максимальной скорости передачи нулей и единиц по этой линии связи при условии, что вероятность передачи нулей и единиц на передающей стороне одинакова, т.е.$P_y(0) = P_y(1) = 1/2$.

2. Имеет место , т.е. доля ошибок при передаче нулей и единиц одинакова. Это двоичный симметричный канал.

Подставив $p_{\text{ош}}$ в формулу 2.6, имеем:

$$H_{\text{апост}}\left(Z/Y\right) = \quad (2.10)$$
$$= P_y(0)\underbrace{\left[-p_{\text{ош}}\log p_{\text{ош}} - \left(1-p_{\text{ош}}\right)\log\left(1-p_{\text{ош}}\right)\right]}_{H(p_{\text{ош}})} + \left[1-P_y(0)\right]\cdot H\left(p_{\text{ош}}\right) =$$
$$= H\left(p_{\text{ош}}\right),$$

а формула 2.1 может быть видоизменена

$$\boxed{C_{\text{лс}}} = \max_{p_y(0)} I_{\text{на1 символ}}(Z;Y)\cdot V_{\text{лс max}} = V_{\text{лс max}}\cdot \max_{p_y(0)}\left[H_{\text{апр}}(z) - H(p_{\text{ош}})\right] =$$
$$= V_{\text{лс max}}\cdot\left[\max_{p_y(0)} H_{\text{апр}}(z) - H(p_{\text{ош}})\right] = \overline{V_{\text{лс max}}\left[1 - H(p_{\text{ош}})\right]}. \qquad (2.11)$$

3. При придётся воспользоваться всем набором формул от 2.1 до 2.8. Лучше решать задачу не в общем виде, а подставлять числовые значения и .

Вероятность $P_y(0)$, дающую $\max_{p_y(0)} I_{\text{на1 символ}}(Z;Y)$, искать через приравнивание $I'_{\text{на 1 символ}}(Z; Y)$ нулю. Решение уравнения $I'(Z; Y) = 0$ получить графически, задавая различные значения $P_y(0)$.

Задача для самостоятельного решения:

Задавшись разными значениями и , подсчитайте пропускную способность двоичного ассиметричного канала. В расчётах примите

$$p\left(\frac{1}{0}\right) = 2p\left(\frac{0}{1}\right) = 0.001\cdot n,$$

где n – ваш номер в списке группы.

При расчетах должно получиться $p(0) > 0.5$, если и наоборот.

Пропускная способность канала должна лежать между

$[1 - H(p_{\text{ош min}})]V_к$ и $[1 - H(p_{\text{ош max}})]V_к$.

Расчет приведите в рабочей тетради.

Практическая работа № 6

Тема: «Преобразование форматов ip–адресов»

Цель: обобщение и систематизация знаний по теме «Адресация в сетях»

Задания к работе:

Задание 1. Переведите следующие двоичные числа в десятичные.

Двоичное значение

1. 1111011
2. 1001001101
3. 101101111
4. 1011110001
5. 10101100.00101000.00000000.00000000
6. 01011110.01110111.10011111.00000000
7. 10010001 0110000 10000000 00011001
8. 01111111 00000000 00000000 00000001

Задание 2. Переведите следующие десятичные числа в двоичные.

Десятичное значение	
1. 250 2. 19 3. 348 4. 93	5. 874 6. 109.128.255.254 7. 131.107.2.89 8. 129.46.78.0

Задание 3. Укажите классы следующих IP-адресов.

Адрес	
1 126.102.128.0 2 1.191.248.0 3 185.74.41.184 4 96.247.128.0	5 168.224.0.1 6 201.76.98.5 7 186.112.0.10 8 28.0.0.0

Задание 4. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

1. 131.107.256.80 2. 222.222.255.222 3. 31.200.1.1 4. 126.1.0.0	5. 190.7.2.0 6. 127.1.1.1 7. 198.121.254.255 8. 255.255.255.255

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?

Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?

3. Когда необходим уникальный идентификатор сети?

4. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Практическая работа № 7

Тема: «Адресация в IP сетях. Подсети и маски»

Цель:

- Изучить принципы адресации в IP-сетях
- Выяснить назначение масок в IP-адресации.

Ход работы

- Изучение теоретического материала
- Задание 1
- Задание 2
- Задание 3
- Задание 4

Теоретическая часть

"Принципы IP-адресации"

- Типы адресов стека TCP/IP
- Классы IP-адресов
- Особые IP-адреса
- Порядок распределения IP-адресов

Типы адресов стека TCP/IP

В стеке TCP/IP используются три типа адресов: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена.

В терминологии TCP/IP под локальным адресом понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP 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.

Классы IP-адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

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 бит адреса. Значения этих бит являются также признаками того, к какому классу относится тот или иной IP-адрес.

На рис. 1 показана структура IP-адреса разных классов.

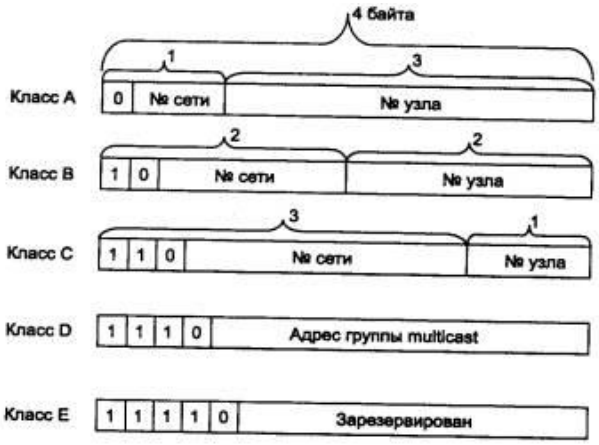


Рис. 1. Структура IP-адреса

Если адрес начинается с 0, то сеть относят к классу A и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) Сетей класса A немного, зато количество узлов в них может достигать 2^{24}, то есть 16 777 216 узлов.

Если первые два бита адреса равны 10, то сеть относится к классу B. В сетях класса B под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса B является сетью средних размеров с максимальным числом узлов 2^{16}, что составляет 65 536 узлов.

Если адрес начинается с последовательности 110, то это сеть класса C. В этом случае под номер сети отводится 24 бита, а под номер узла - 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 28, то есть 256 узлами.

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 значит, что данный адрес относится к классу E, Адреса этого класса зарезервированы для будущих применений.

В табл. 1 приведены диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей.

Таблица 1. Характеристики адресов разного класса

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Большие сети получают адреса класса A, средние - класса B, а маленькие класса C.

Задание1. Выясните, каков будет порядок отправки информацию по адресам 192.168.193.31 и 192.167.192.3 для хоста с адресом 192.167.12.3 и маской подсети 255.255.0.0. Решение задачи запишите в отчет.

Как происходит передача данных

1. IP-адрес в двоичном представлении разбивается на 2 части - адрес сети (левая часть адреса) и адрес хоста (правая часть адреса).

Например, в адресе 190.167.34.2 первые 24 бита могут быть адресом сети, а последние 8 – адресом хоста.

Тогда наш адрес будет выглядеть как 10111110101001110010001000000010, где зеленым цветом выделена сетевая часть адреса (она одинакова для всех хостов локальной сети), а красным - часть адреса, адресующая хост внутри локальной сети.

Для того, чтобы быстро вычислять по IP-адресу адрес сети или хоста, используется понятие **маски подсети (subnet mask)**. Это двоичное число, в котором все биты адреса сетевой части адреса равны 1, а все остальные биты равны нулю. В нашем случае для адреса 10111110101001110010001000000010 получим маску подсети 11111111111111111111111100000000.

1. Маску подсети принято записывать в том же десятичном формате, что и IP-адрес. Для этого нужно каждый байт маски перевести в десятичное число и записать полученные десятичные числа через точки. Ванашемаслучае

Ответ:

$11111111_2=255$
$11111111_2=255$
$11111111_2=255$
$00000000_2=0$

255.255.255.0 - маска подсети.

Маску подсети в настоящее время все чаще называют маской сети, что точней отображает ее смысл.

3. Информационные пакеты пересылаются напрямую от компьютера-отправителя к компьютеру-получателю только в пределах одной сети. Если компьютер-получатель находится в другой сети, то информация пересылается специальному компьютеру сети, который называется шлюзом (gateway). Его адрес всегда известен. Об этом заботится системный администратор. Компьютер-шлюз имеет связь с как минимум с одной другой сетью и ретранслирует информацию в нужном направлении. Этот процесс называется маршрутизацией (routing).

4. Если ваш компьютер, имеющий IP адрес 192.169.204.12 и маску подсети 255.255.192.0 должен отправить информацию компьютеру с адресом 192.169.198.15, то прежде всего ваш компьютер проверит, находится ли получатель информации в той же сети. Для этого двоичное представление адреса получателя он побитовоумножит на двоичное представление маски подсети, то в результате получится адрес сети:

11000000101010001100011000001100 (адрес компьютера - получателя)
*
11111111111111111100000000000000 (текущая маска подсети)

11000000101010001100000000000000 (адрес сети получателя)

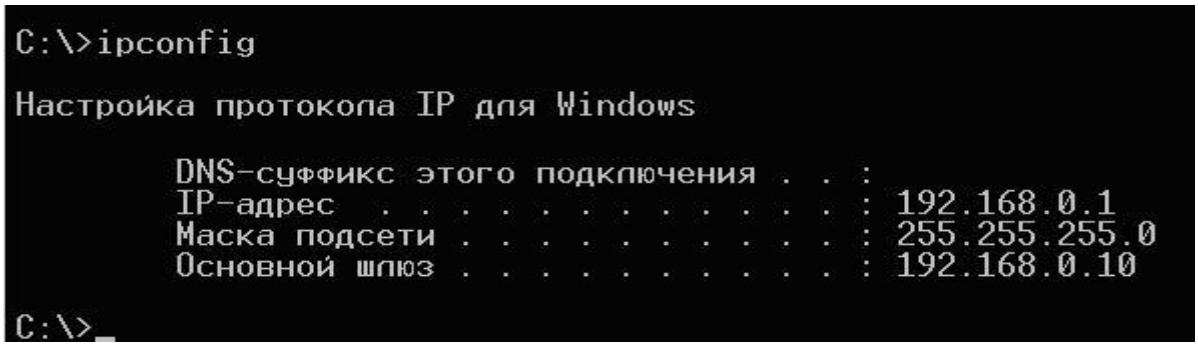
Аналогичную процедуру компьютер проделает со своим адресом для того, чтобы узнать адрес своей собственной сети:

11000000101010011100110000001100 (адрес компьютера - отправителя)
*
11111111111111111100000000000000 (текущая маска подсети)

11000000101010011100000000000000 (адрес своей собственной сети)

Если адрес сети получателя совпадает с адресом собственной сети, следовательно, получатель находится в локальной сети, и информация может быть послана напрямую. Если бы совпадения нет, то информация будет отправлена шлюзу (с адресом, например,192.168.192.2) с указанием адреса получателя 192.169.204.12, а он переслал бы ее в другую сеть. Этот процесс будет продолжаться до тех пор, пока информация не дойдет до получателя.

Задание2. Определение настроек протокола IP вашего компьютера
Для этого достаточно запустить программу ipconfig (в Windows 9X есть еще программа с графическим интерфейсом winipcfg). Получить доступ к командной строке и напечатайте ipconfig. Нажмите клавишу :



Занесите полученные параметры в отчет.

Примечание. Настройка протокола IP на каждом компьютере локальной сети - одна из задач системного администратора. Он может в принципе задать все параметры вручную. Но если число компьютеров в сети больше десятка, то удобней назначать настройки автоматически в момент загрузки компьютера. Для этого разработан специальный протокол DHCP (Dynamic Host Configuration Protocol). Наличие у компьютера правильного IP-адреса является совершенно необходимым условием его работы в Интернет.

Задание 3. Дополнить конспект лекции "Принципы адресации в IP-сетях" по плану:

1. Классы IP-адресов
2. Особые IP-адреса
3. Порядок распределения IP-адресов
4. Использование масок в IP-адресации

Задание 4. По IP -адресу определить идентификатор сети и идентификатор узла (подразумеваются стандартные классы IP-адресов):

192.168.1.1
126.15.25.5
221.186.52.65
125.14.7.8
Занести в отчет

Вопросы:

2. IP-адрес, формат записи
3. Классы IP-адресов
4. Значения выделенных IP-адресов
5. Порядок распределения IP-адресов
6. Использование масок в IP-адресации
7. Утилита ipconfig. Назначение.

Практическая работа № 8-10

Тема: «Настройка протоколов tcp/ip в операционных системах»

Цель работы*:*

1. Изучить порядок конфигурирования сетевых протоколов в ОС Windows.
2. Изучить принципы адресации компьютеров в IP– сетях.
3. Научиться правильно использовать механизм масок при назначении адресов сетевым интерфейсам.

Теоретические сведения:

Стек протоколов TCP/IP является основным набором протоколов сети Интернет. В настоящее время стек протоколов поддерживается всеми без исключения операционными системами общего назначения и является наиболее широко распространенным стеком, используемым как в глобальных, так и локальных сетях любого масштаба.

Замечание: Настройки требует только протокол IP. Однако в документации на ОС семейства Windows практически повсеместно употребляется оборот "протокол TCP/IP", что является неточным, так как аббревиатуру TCP/IP часто используют либо для обозначения всего стека протоколов Интернет, либо для обозначения пары протоколов TCP и IP, работающих на транспортном и сетевом уровнях семиуровневой модели OSI [3]. Протокол TCP в процессе работы ОС в IP– сетях обычно никаких настроек не требует, хотя такая возможность имеется.

Установка протокола TCP/IP

Установка TCP/IP в ОС Windows XP достаточно проста и понятна из [4]. Имеется несколько способов выполнения данной процедуры. В различных ОС семейства Windows число этих вариантов различно. Рассмотрим основной способ установки, поддерживаемый всеми без исключения типами ОС семейства Windows, – установку с помощью панели **Управления** (**Control Panel**). Необходимо вызвать панель управления (**Пуск/Настройка/Панель управления**), а затем дважды щелкнуть значок **Network** ("**Сеть**" или "**Сетевые подключения**").

В появившемся окне "**Сетевые подключения**" найти настраиваемый сетевой интерфейс, в контекстном меню интерфейса выбрать пункт "**Свойства**". Откроется окно свойств сетевого подключения (рисунок 3).

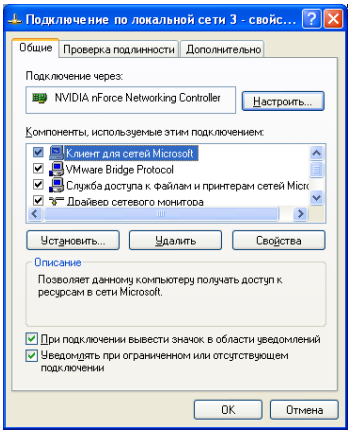


Рис. 3 Окно свойств сетевого подключения

Если для сетевого интерфейса отсутствует протокол TCP/IP, то необходимо выбрать кнопку "**Установить**" (кнопка "**Добавить**" в более ранних версиях ОС Windows) и затем найти

нужный протокол и подтвердить сделанный выбор. Протокол будет установлен в операционную систему, которая будет осуществлять поддержку.

После включение модулей, реализующих функции протоколов TCP/IP в состав операционной системы семейства ОС Windows, необходимо выполнить настройку протоколов.

Параметры настройки протокола IP

Для настройки протокола IP необходимы следующие три параметра конфигурации: IP– адрес, маска подсети и шлюз по умолчанию:

IP– адрес

IP– адрес – это логический 32–битный адрес, используемый для идентификации TCP/IP–хоста. IP– адрес состоит из двух частей: идентификатора (ID) сети и ID хоста. ID сети (адрес сети) идентифицирует все хосты (самостоятельные машины, либо их сетевые интерфейсы, если машина имеет несколько сетевых адаптеров), которые находятся в одной физической сети. ID хоста (адрес хоста) идентифицирует конкретный хост в сети, а точнее конкретный сетевой интерфейс, имеющий свой собственный IP– адрес. Для выделения адреса сети из IP– адреса используется механизм сетевых масок, изначально предусмотренный стандартом адресации в IP сетях.

Сетевая маска (маска подсети)

Сетевая маска представляет собой 32–х битное число, содержащее непрерывную последовательность единиц в разрядах соответствующих адресу сети. Все остальные разряды маски содержат нулевые значения.

Шлюз по умолчанию

Протокол IP обеспечивает доставку пакетов в пределах всей составной IP– сети. IP– сеть называется составной, так как предполагается, что отдельные IP– сети объединяются друг с другом с помощью средств сетевого уровня, которые реализуются специальным устройством, называемым шлюзом.

Подготовка к выполнению заданий:

Сетевые параметры, необходимые для выполнения практического задания, уточните у преподавателя.

Задания для выполнения:

Изменение параметров настройки протокола IP.

1.1 Подключиться к виртуальной машине Windows .Перейти в окно конфигурирования сетевых подключений: открыть окно "**Сетевые подключения**": **Пуск/Настройка/Сетевые подключения**. Кликнуть правой клавишей мыши по значку "подключение по локальной сети" и выбрать пункт "**Свойства**".

1.2 В появившемся окне выберите сетевой адаптер, затем "**Свойства**", затем **Протокол Интернета** (**TCP/IP**) и его свойства.

* Если доступ к настройке параметров сети запрещен административными настройками ОС, то перейдите к выполнению дополнительного задания, описанного в п.6.

1.3 Запишите значения сетевых параметров, установленных на Вашей машине:

- IP– адреса;
- Сетевой маски;
- Адреса шлюза по умолчанию;
- Адреса 1– го и 2– го серверов DNS (если они установлены). Занесите значения этих параметров в отчет.

1.4 Удалите протокол NetBUI, если он установлен на Вашей машине.

1.5 Установите сетевые параметры протокола IP в соответствии с таблицей 2.

Таблица 2. Сетевые параметры протокола IP

IP– адрес**	Сетевая маска	Шлюз
192.168.20Y.G+XX	255.255.0.0	Использовать значение, которое было установлено ранее, либо значение, указанное преподавателем.
Где Y, G, XX – десятичные числа; Y – год поступления (одна цифра 0-9). G = номер группы. 00 – для группы УИР-1; 50 – для группы УИР-2; 100 – для группы УИР-3. XX = – порядковый номер студента в группе. Пример. Студент номер 21 (по журналу); группы УИР-2; год поступления 2003. XX=21; G=50; Y=3. Получим сетевой адрес машины: 192.168.203.71 Где 203 = 200+3 71 = 50+21.		

1.6 Если в результате изменения параметров настройки протокола IP будет выдано сообщение о необходимости перезагрузки, ни в коем случае не делайте этого, просто откажитесь.

1.7 Открыть консоль системы (соответствующая процедура описана в приложении 2). В командной строке выполнить команду:

> ipconfig /all

Сохраните результат выполнения этой команды в отчете.

1.8 В командной строке консоли выполните команду:

> ping <*адрес_шлюза*>

Результаты занесите в файл отчета.

2. Оформление отчета по результатам выполнения практической работы.

По результатам выполнения работы необходимо подготовить отчет требования, к которому изложены в Приложении 1.

Контрольные вопросы:

1. Имеется сеть с IP = 192.168.55.0 и требуется разбить ее на ряд подсетей. Необходимо, чтобы в каждой подсети можно было использовать по 25 хостов. Какую маску необходимо применить в таком случае, чтобы обеспечить максимально возможное число таких подсетей?

A 255.255.255.192; B. 255.255.255.224; C. 255.255.255.240;

D 255.255.255.248.

2. У вас имеется маска 255.255.255.252. Какое значение имеет префикс? A. /16; B. /24;

C. /30, D. /32

3. Если имеется IP– адрес 172.16.10.5/25, то какой широковещательный адрес должен использовать этот хост?

A. 255.255.255.255; B. 172.16.10.127; C. 172.16.10.255;

D. 172.16.10.128.

4. Сколько машин позволяет иметь в подсети маска 255.255.255.252?

A. 16384; B. 2; C. 4094; D. 6.

5. Каков диапазон допустимых адресов машин для подсети 172.16.10.5/26?

A. с 172.16,10.1 по 172.16.10.30; B. с l72.16.10.1 по l72.16.10.31;

C. с 172.16.10.1 по 172.16.10.62; D. с 172.16.10.1 по 172.16.10.63.

6. Если вы хотите объединить в подсеть машины с адресами с 192.168.10.64 по 192.168.10.127, то какими будут адрес и маска подсети?

A. 192.168.10.64 255.255.255.192; B. 192.168.10.0 255.255.255.192;

C. 192.168.10.64 255.255.255.224; D. 192.168.10.0 255.255.255.224.

7. Назовите основное назначение и возможности технологии применения масок переменной длины (VLSM).

8. Назовите основное назначение и возможности технологии бесклассовой междоменной маршрутизации (CIDR).

9. Объясните основные функции, выполняемые шлюзом в коммуникационной схеме протокола IP.

Каким образом, машины, работающие в IP сети, определяют, когда пакет необходимо доставить шлюзу, а в каком случае доставка выполняется непосредственно с помощью протоколов канального

Практическая работа № 11-12

Тема: Расчет времени двойного оборота. Расчет сокращения межкадрового интервала.

Цель работы: Научиться рассчитывать время двойного оборота

Теоретические сведения

Модель, применяемая для оценки конфигурации Ethernet, основана на подсчете временных характеристик данной конфигурации. В ней применяется две системы расчетов: одна предполагает вычисление двойного (кругового) времени прохождения сигнала по сети, а другая – проверку допустимости получаемого (межкадрового) временного интервала. При этом расчеты в обеих системах расчетов ведутся для наихудшего случая.

При первой системе расчетов используются такие понятия, как “начальный сегмент”, “промежуточный сегмент” и “конечный сегмент”. Отметим, что промежуточных сегментов может быть несколько, а начальный и конечный сегменты при разных расчетах могут меняться местами. Для расчетов используются величины задержек, представленные в Таблице 1.

Таблица 1

Тип сегмента Ethernet	Макс. длина, м	Начальный сегмент	Промежуточный сегмент	Конечный сегмент	Задержка на метр длины		
t0	tm	t0	tm	t0	tm	t1	
10BASE5		11,8	55,0	46,5	89,8	169,5 212,8	0,0866
10BASE2		11,8	30,8	46,5	65,5	169,5 188,5	0,1026
10BASE-T		15,3	26,6	42,0	53,3	165,0 176,3	0,1130
10BASE-FL		12,3	212,3	33,5	233,5	156,5 356,5	0,1000
FOIRL		7,8	107,8	29,0	129,0	152,0 252,0	0,1000
AUI (> 2 м)	2+48=50		5,1		5,1	5,1	0,1026

Примечание. Задержки даны в битовых интервалах.

Расчет сводится к следующему:

1. В сети выделяется путь наибольшей длины;

2. Если длина сегмента не максимальна, то рассчитывается двойное (круговое) время прохождения в каждом сегменте выделенного пути по формуле: $ts=L \cdot t1+t0$, где L – длина сегмента в метрах (при этом надо учитывать тип сегмента: начальный, промежуточный или конечный);

3. Если длина сегмента максимальна, то из таблицы для него берется величина задержки tm;

4. Суммарная величина задержек всех сегментов выделенного пути не должна превышать 575 битовых интервалов;

5. Затем необходимо проделать те же действия для обратного направления выбранного пути (то есть, считая конечный сегмент начальным, и наоборот);

6. Если задержки в обоих случаях не превышают 575 битовых интервалов, то сеть работоспособна.

Если в выбранной вами конфигурации сети путь наибольшей длины не столь очевиден, то подобные расчеты необходимо произвести для всех путей, претендующих на наибольшую

задержку сигнала. В любом случае двойное время прохождения в соответствии со стандартом недостаточно, чтобы сделать окончательный вывод о работоспособности сети.

2.6.2. Расчет сокращения межкадрового интервала (PVV – path variability value)

Чтобы признать конфигурацию сети корректной, нужно рассчитать также уменьшение межкадрового интервала репитерами (репитерными концентраторами).

Эта величина не должна быть меньше, чем 49 битовых интервалов. Для вычислений здесь также используются понятия начального сегмента и промежуточного сегмента (конечный сегмент не вносит вклада в сокращение межкадрового интервала, так как пакет доходит по нему до принимающего компьютера без прохождения репитеров и репитерных концентраторов).

Для расчета сокращения межкадрового интервала можно воспользоваться значениями максимальных величин уменьшения межкадрового интервала при прохождении репитеров (репитерных концентраторов) различных физических сред приведенными в Таблице 2.

Таблица 2

Тип сегмента	Начальный сегмент	Промежуточный сегмент
10BASE5		
10BASE2		
10BASE-T	10,5	
10BASE-FL	10,5	

Вычисления здесь очень простые. Суммируя величины сокращений межкадрового интервала для наибольшего пути в выбранной конфигурации и сравнивая сумму с предельной величиной в 49 битовых интервалов, мы можем сделать вывод о работоспособности сети.

Такие же вычисления проводятся и для обратного направления по этому же пути.

3 Порядок выполнения работы

1. Ознакомиться с теоретической частью к лабораторной работе.

2. В соответствии с заданным вариантом (приложение 1) спроектируйте локальную вычислительную сеть организации, проведите расчеты .

3. Подготовьте спецификацию на оборудование и материалы спроектированной локальной вычислительной сети организации .

4. Подготовьте отчет. Пример приведен в приложении 2.

4 Требования к отчету

Отчет по лабораторной работе должен содержать:

а) титульный лист;

б) задание;

в) конфигурацию спроектированной сети;

г) расчеты, подтверждающие работоспособность сети;

д) спецификацию на оборудование и материалы.

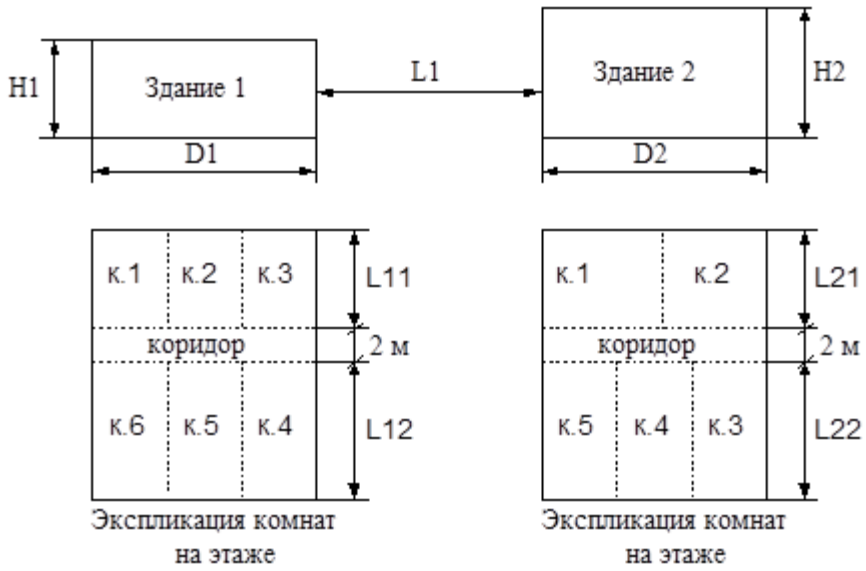
Контрольные вопросы:

1. Среды передачи для сети Ethernet.
2. Аппаратура 10BASE5.
3. Аппаратура 10BASE2.
4. Аппаратура 10BASE-T.
5. Аппаратура 10BASE-FL.

6. Порядок выбора конфигурации Ethernet?

7. Что означает число 575, как оно формируется?

ПРИЛОЖЕНИЕ 1



Вариант	L1, м	H1, м	D1, м	L11, м	L12, м	H2, м	D2, м	L21, м	L22, м	Этажность здания 1	Этажность здания 2
1.											
2.											
3.											
4.											

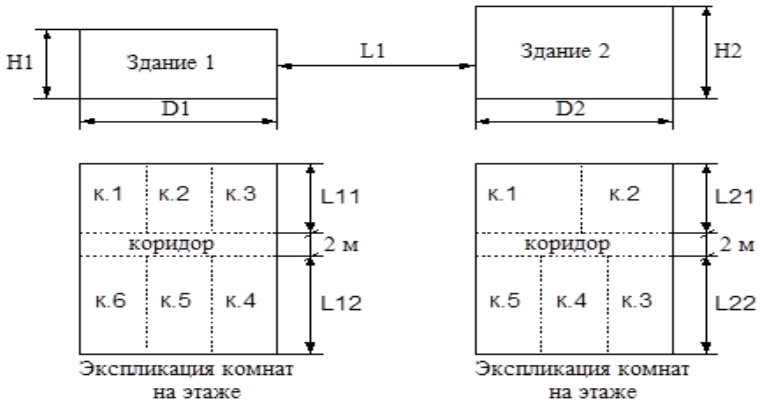
Вариант	Здание	Этаж	Количество компьютеров в комнате					
к.1	к.2	к.3	к.4	к.5	к.6			
1.								
						-		

Вариант	Здание	Этаж	Тип среды передачи	Тип среды передачи между зданиями
1.			10BASE5	10BASE5
	10BASE2			
	10BASE-T			
		10BASE-FL		
	10BASE5			
2.			10BASE2	10BASE2
	10BASE-T			

		10BASE-FL		
	10BASE5			
	10BASE2			
3.			10BASE-T	10BASE-T
	10BASE-FL			
	10BASE5			
		10BASE2		
	10BASE-T			
4.			10BASE-FL	10BASE-FL
	10BASE5			
		10BASE2		
	10BASE-T			
	10BASE-FL			

ПРИЛОЖЕНИЕ 2

Пример содержания отчета



Тип сегмента Ethernet	Макс. длина, м	Начальный сегмент	Промежуточный сегмент	Конечный сегмент	Задержка на метр длины			
t0	tm	t0	tm	t0	tm	t1		
10BASE5		11,8	55,0	46,5	89,8	169,5	212,8	0,0866
10BASE2		11,8	30,8	46,5	65,5	169,5	188,5	0,1026
10BASE-T		15,3	26,6	42,0	53,3	165,0	176,3	0,1130
10BASE-FL		12,3	212,3	33,5	233,5	156,5	356,5	0,1000
FOIRL		7,8	107,8	29,0	129,0	152,0	252,0	0,1000
AUI (> 2 м)	2+48=50		5,1		5,1		5,1	0,1026

Формула расчета: $t_s = L \cdot t_1 + t_0$

В выбранной конфигурации сети наибольший путь составляет 1214 м.

10BASE5 à10BASE2 $t_1 = 99 \cdot 0{,}0866 + 11{,}8 = 20{,}3734$ $t_2 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$ $t_3 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$ $t_4 + t_5 = 311 \cdot 0{,}1026 + 169{,}5 = 201{,}4$ $t_1 + t_2 + t_3 + t_4 + t_5 = 396{,}182 < 575$	10BASE5 ß 10BASE2 $t_4 + t_5 = 311 \cdot 0{,}1026 + 15{,}3 = 47{,}2086$ $t_3 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$ $t_2 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$ $t_1 = 99 \cdot 0{,}0866 + 169{,}5 = 20{,}3734$ $t_1 + t_2 + t_3 + t_4 + t_5 = 399{,}682 < 575$

Задержки в обоих случаях не превышают 575 битовых интервалов. Сеть работоспособна.

Таблица 2

Тип сегмента Начальный сегмент Промежуточный сегмент

10BASE5

10BASE2

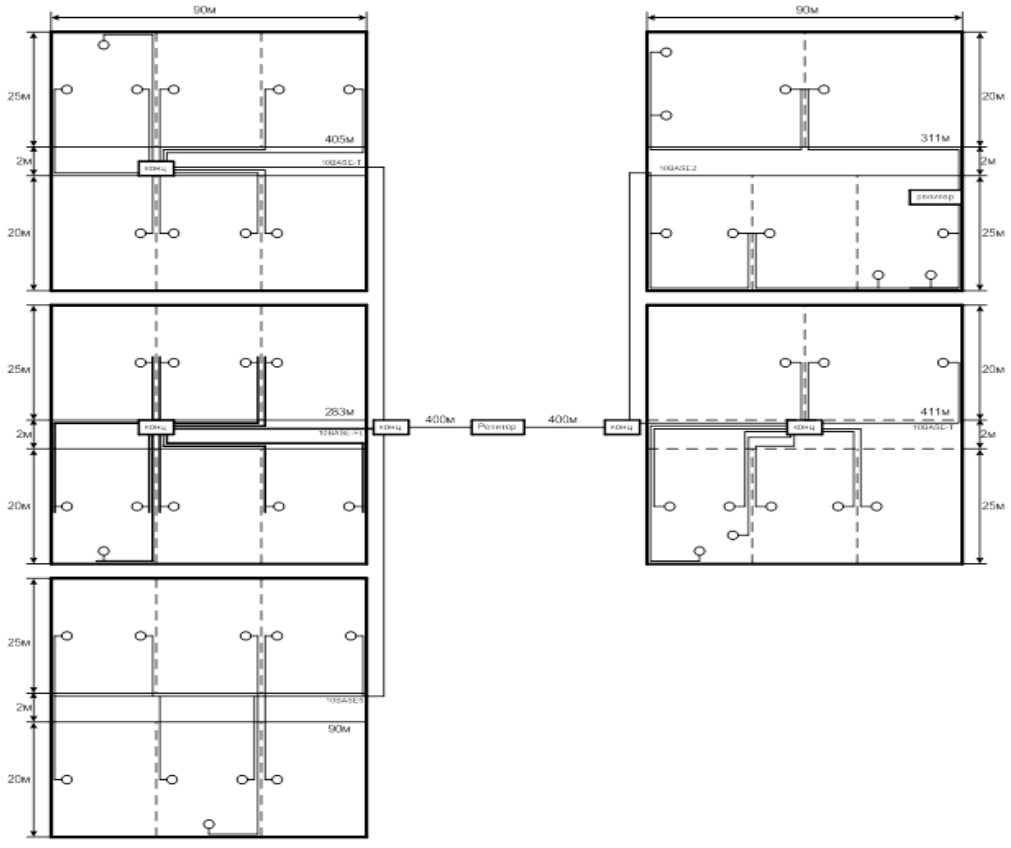
10BASE-T 10,5

10BASE-FL 10,5

16+8+8=32

Суммы величин сокращений межкадрового интервала для всех путей в выбранной конфигурации меньше предельной величины в 49 битовых интервалов. Сеть работоспособна.

Схема спроектированной сети



4) Спецификация:

№№	Наименование	Единица измерения	Количество
Оборудование			
1.	Репитер	шт.	
2.	Репитерный концентратор на 4 порта	шт.	
3.			
4.	Концентратор на 16 портов	шт.	
5.	Сетевой адаптер	шт.	
Материалы			
6.	“Толстый” кабель с разъемами N-типа на концах	м	
7.	Трансиверные кабели с 15-контактными разъемами на концах	шт.	
8.	Трансиверы	шт.	
9.	Оптоволоконные трансиверы (FOMAU)	шт.	
10.	Barrel-коннектор N-типа для присоединения терминаторов на концах кабеля	шт.	
11.	N-терминатор	шт.	
12.	N-терминатор с заземлением	шт.	
13.	Отрезки «тонкого» кабеля с BNC-разъемами на двух концах	шт.	
14.	BNC Т-коннекторы	шт.	
15.	BNC терминатор без заземления	шт.	
16.	BNC терминатор с заземлением	шт.	
17.	Отрезки кабеля с разъемами RJ-45 на концах	шт.	
18.	Оптический кабель		

Таблица 2

Тип сегмента Начальный сегмент Промежуточный сегмент

10BASE5

10BASE2

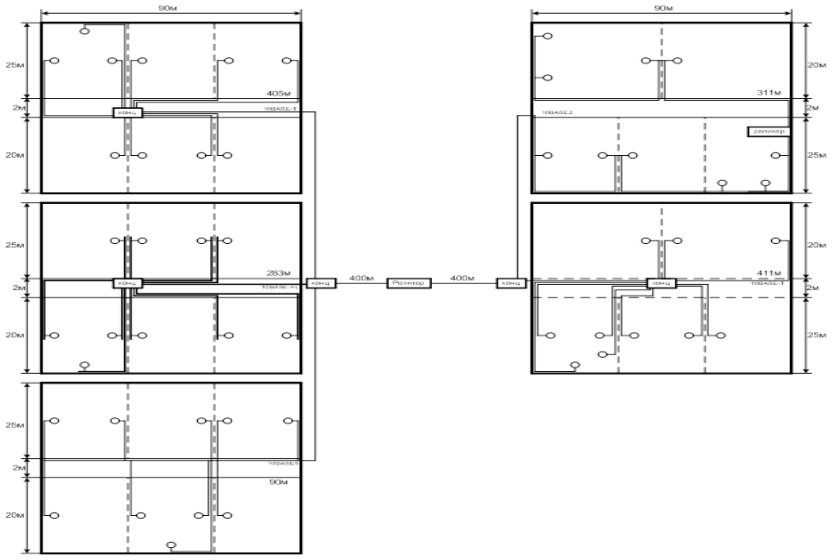
10BASE-T 10,5

10BASE-FL 10,5

16+8+8=32

Суммы величин сокращений межкадрового интервала для всех путей в выбранной конфигурации меньше предельной величины в 49 битовых интервалов. Сеть работоспособна.

Схема спроектированной сети



4) Спецификация:

№№	Наименование	Единица измерения	Количество
Оборудование			
1.	Репитер	шт.	
2.	Репитерный концентратор на 4 порта	шт.	
3.			
4.	Концентратор на 16 портов	шт.	
5.	Сетевой адаптер	шт.	
Материалы			
6.	“Толстый” кабель с разъемами N-типа на концах	м	
7.	Трансиверные кабели с 15-контактными разъемами на концах	шт.	
8.	Трансиверы	шт.	
9.	Оптоволоконные трансиверы (FOMAU)	шт.	
10.	Barrel-коннектор N-типа для присоединения терминаторов на концах кабеля	шт.	
11.	N-терминатор	шт.	
12.	N-терминатор с заземлением	шт.	
13.	Отрезки «тонкого» кабеля с BNC-разъемами на двух концах	шт.	
14.	BNC Т-коннекторы	шт.	
15.	BNC терминатор без заземления	шт.	
16.	BNC терминатор с заземлением	шт.	
17.	Отрезки кабеля с разъемами RJ-45 на концах	шт.	
18.	Оптический кабель		

Практическая работа № 13

Тема: Создание простейшей локальной сети

Цель: ознакомление с основными принципами работы, чтобы понять как работать в программе Cisco Packet Tracer на примере создание простой локальной вычислительной сети, путем описания пошаговых инструкции по настройке.

Теоретические сведения

Характеристика Cisco Packet Tracer

Cisco Packet Tracer разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования, а также для проведения уроков по лабораторным работам в высших заведениях.

Основные возможности Packet Tracer:

Дружественный графический интерфейс (GUI), что способствует к лучшему пониманию организации сети, принципов работы устройства;

Возможность смоделировать логическую топологию: рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;

моделирование в режиме real-time (реального времени);

режим симуляции;

Многоязычность интерфейса программы: что позволяет изучать программу на своем родном языке.

усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;

наличие Activity Wizard позволяет сетевым инженерам, студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

проектирование физической топологии: доступное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д.;

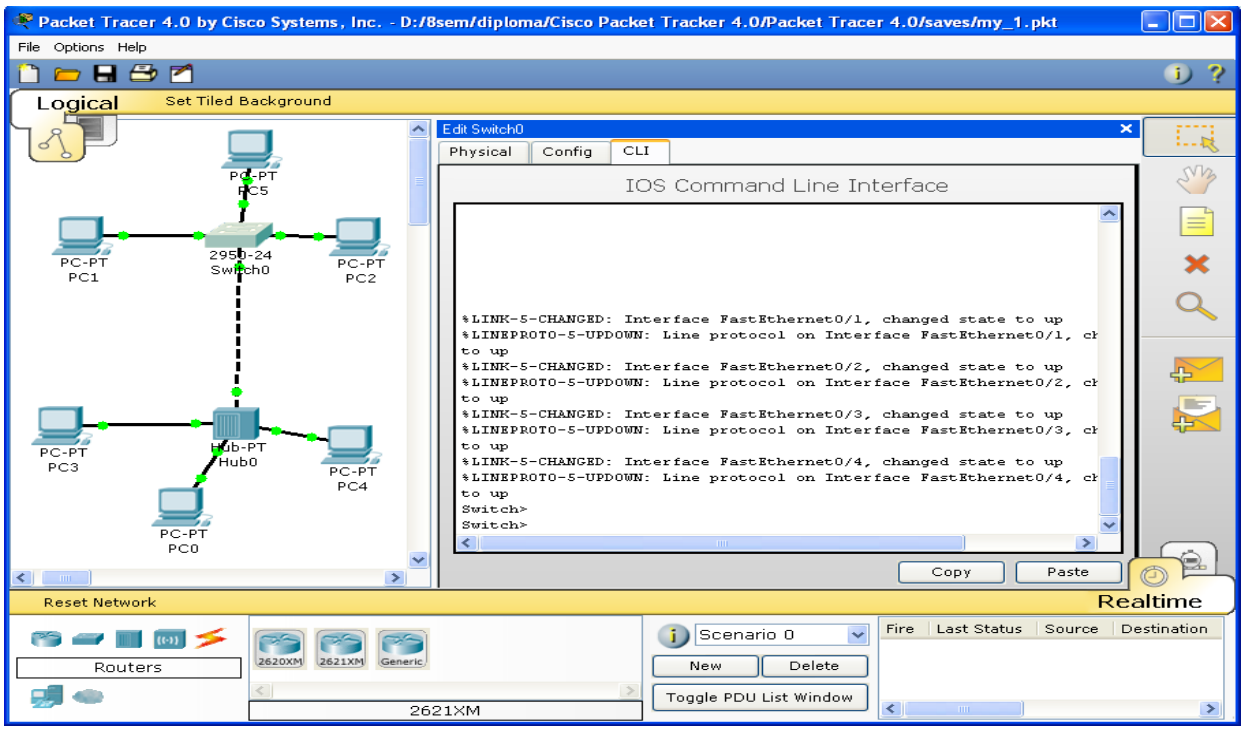


Рисунок 1 - Cisco Packet Tracer

Одной из самых важных особенностей данного симулятора является наличие в нем «Режима симуляции» (рисунок 2). В данном режиме все пакеты, пересылаемые внутри сети, отображаются в графическом виде. Эта возможность позволяет сетевым специалистам наглядно продемонстрировать, по какому интерфейсу в данные момент перемещается пакет, какой протокол используется и т.д.

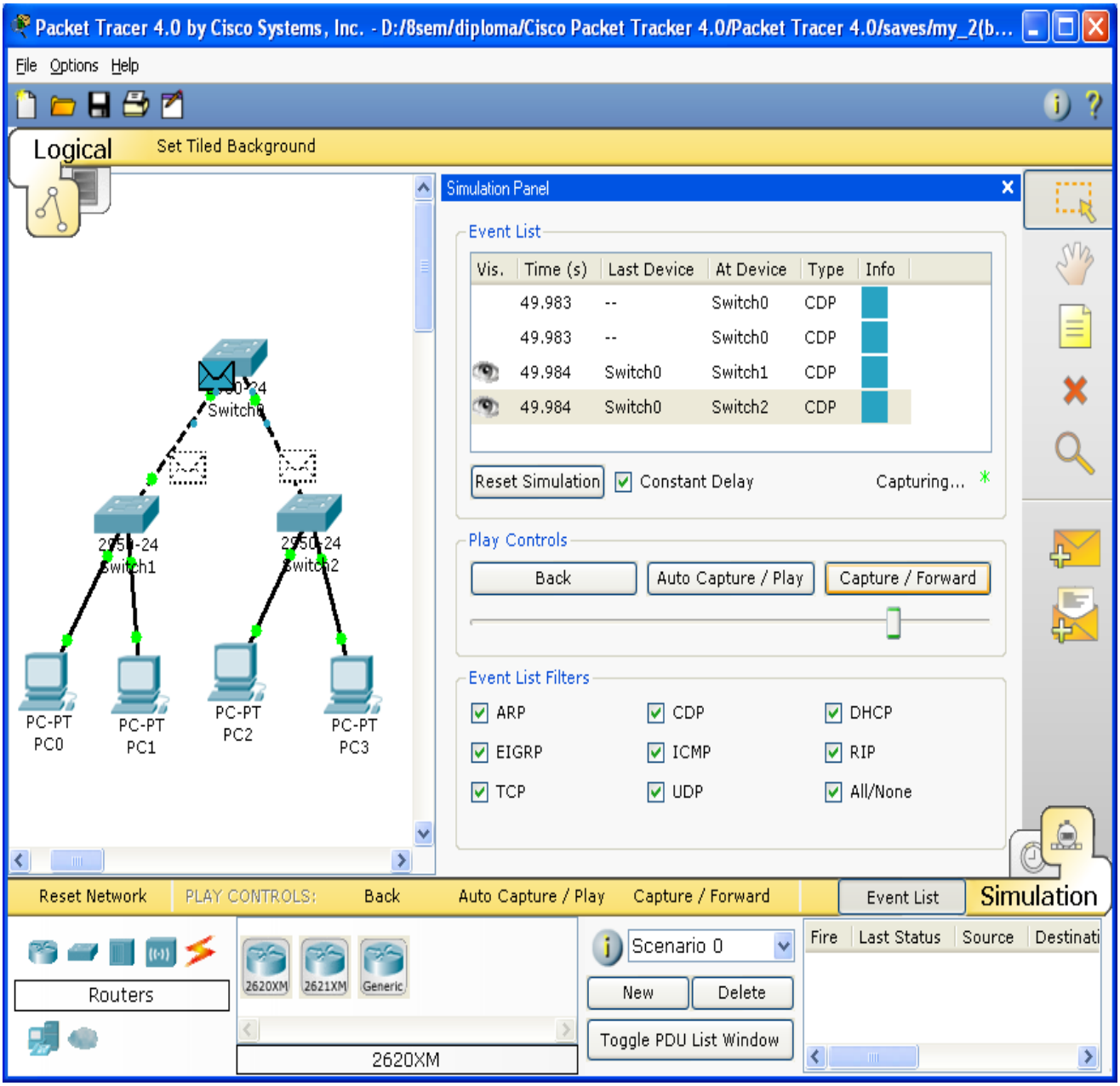


Рисунок 2 - Режим «Симуляции» в Cisco Packet Tracer

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» сетевые инженеры могут не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (рисунок 3).

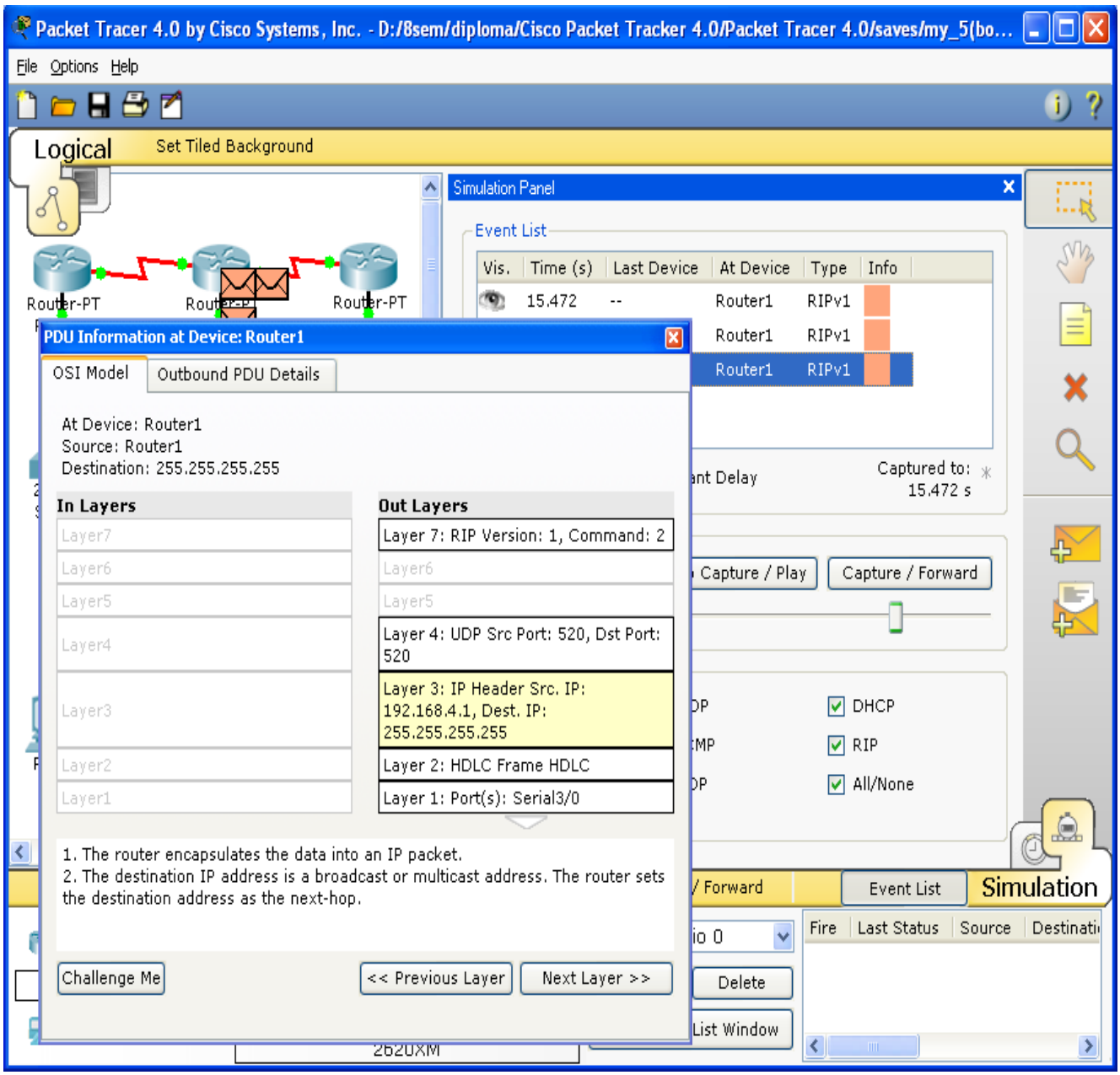


Рисунок 3 - Анализ семиуровневой модели OSI в Cisco Packet Tracer

Такая кажущаяся на первый взгляд простота и наглядность делает практические занятия чрезвычайно полезными, совмещая в них как получение, так и закрепление полученного материала.

Packet Tracer способен моделировать большое количество устройств различного назначения, а так же немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности.

Моделируемые устройства:

коммутаторы третьего уровня:

Router 2620 XM;

Router 2621 XM;

Router-PT.

Коммутаторы второго уровня:

Switch 2950-24;

Switch 2950T;

Switch-PT;

соединение типа «мост» Bridge-PT.
Сетевые концентраторы:
Hub-PT;
повторитель Repeater-PT.
Оконечные устройства:
рабочая станция PC-PT;
сервер Server-PT;
принтер Printer-PT.
Беспроводные устройства:
точка доступа AccessPoint-PT.
Глобальная сеть WAN.
Типы связей:
консоль;
медный кабель без перекрещивания (прямой кабель);
медный кабель с перекрещиванием (кросс-кабель);
волоконно-оптический кабель;
телефонная линия;
Serial DCE;
Serial DTE.
Так же целесообразно привести те протоколы, которые студент может отслеживать:
ARP;
CDP;
DHCP;
EIGRP;
ICMP;
RIP;
TCP;
UDP.
Интерфейс Cisco Packet Tracer
Интерфейс программы Cisco Packet Tracer представлен на рисунке 4.

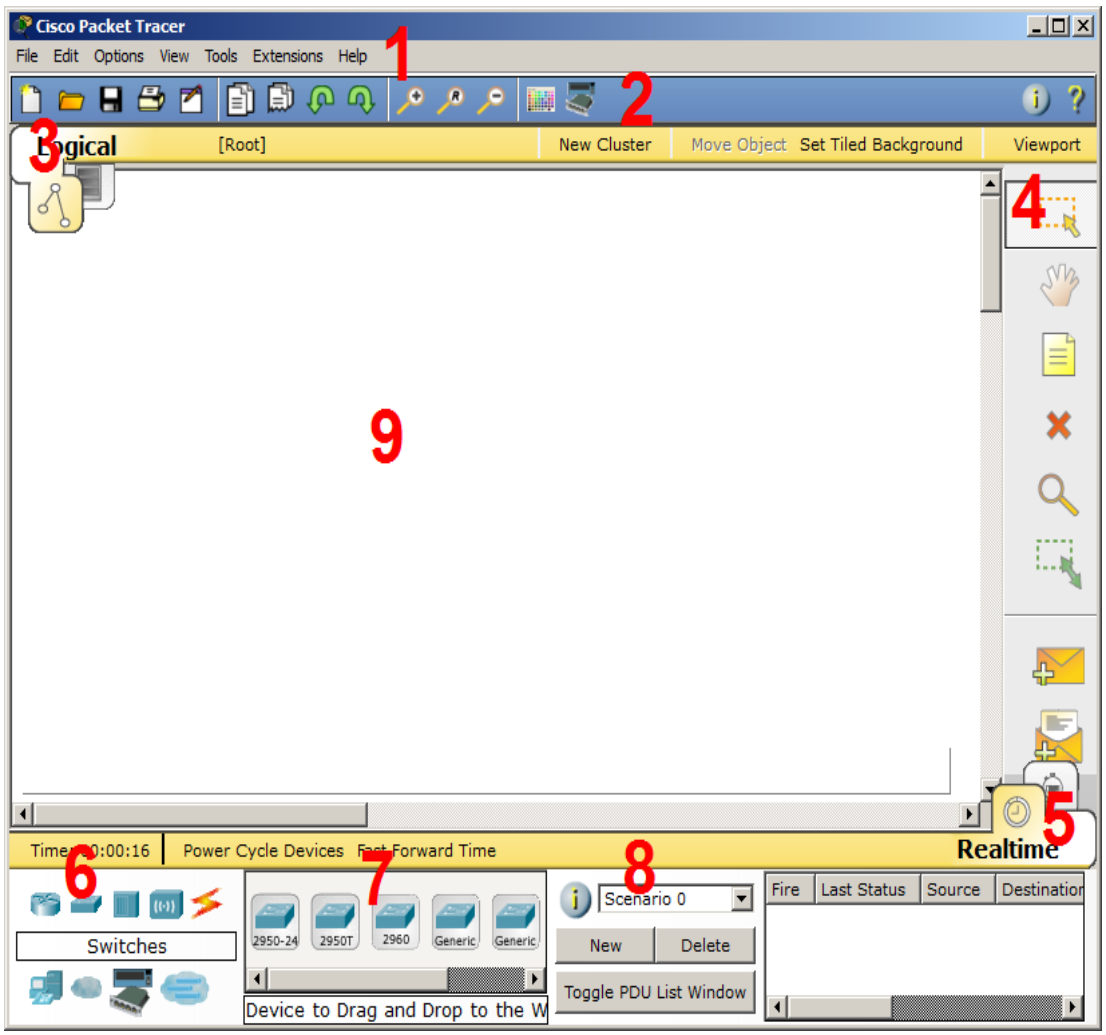


Рисунок 4 – Интерфейс программы Cisco Packet Tracer

Главное меню программы;

Панель инструментов – дублирует некоторые пункты меню;

Переключатель между логической и физической организацией;

Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а так же формирование произвольных пакетов;

Переключатель между реальным режимом (Real-Time) и режимом симуляции;

Панель с группами конечных устройств и линий связи;

Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники.

Панель создания пользовательских сценариев;

Рабочее пространство;

Большую часть данного окна занимает рабочая область, в которой можно размещать различные сетевые устройства, соединять их различными способами и как следствие получать самые разные сетевые топологии.

Сверху, над рабочей областью, расположена главная панель программы и ее меню. Меню позволяет выполнять сохранение, загрузку сетевых топологий, настройку симуляции, а также много других интересных функций. Главная панель содержит на себе наиболее часто используемые функции меню.

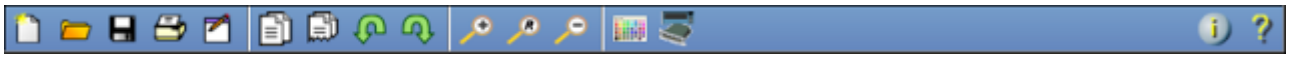


Рисунок 5 - Главное меню Packet Tracer

Справа от рабочей области, расположена боковая панель, содержащая ряд кнопок отвечающих за перемещение полотна рабочей области, удаление объектов и т.д.

Снизу, под рабочей областью, расположена панель оборудования.

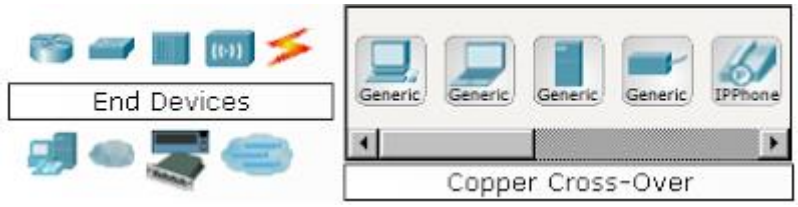


Рисунок 6 - Панель оборудования Packet Tracer

Данная панель содержит в своей левой части типы доступных устройств, а в правой части доступные модели. При выполнении различных лабораторных работ, эту панель придется использовать намного чаще, чем все остальные. Поэтому рассмотрим ее более подробно.

При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы устройств, наиболее часто используемые в лабораторных работах Packet Tracer, представлены на рисунке 7.

Рисунок 7 - Основные типы устройств

Рассматривать конкретные модели устройств каждого типа, не имеет большого смысла. Отдельного рассмотрения заслуживают типы соединений. Перечислим наиболее часто используемые из них (рассмотрение типов подключений идет слева направо, в соответствии с приведенным на рисунке 8).

Рисунок 8 - Типы соединений устройств в Packet Tracer

Автоматический тип – при данном типе соединения PacketTracer автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств

Консоль – консольные соединение

Медь Прямое – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке. Подойдет для следующих соединений: коммутатор – коммутатор, коммутатор – маршрутизатор, коммутатор – компьютер и др.

Медь кроссовер – соединение медным кабелем типа витая пара, концы кабеля обжаты как кроссовер. Подойдет для соединения двух компьютеров.

Оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств имеющих оптические интерфейсы.

Телефонный кабель – обыкновенный телефонный кабель, может понадобится для подключения телефонных аппаратов.

Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля.

Пример локальной вычислительной сети

Рассмотрим на примере создание локальной вычислительной сети в cisco packet tracer, сеть представлена на рисунке 9. Далее описывается пошаговая инструкция.

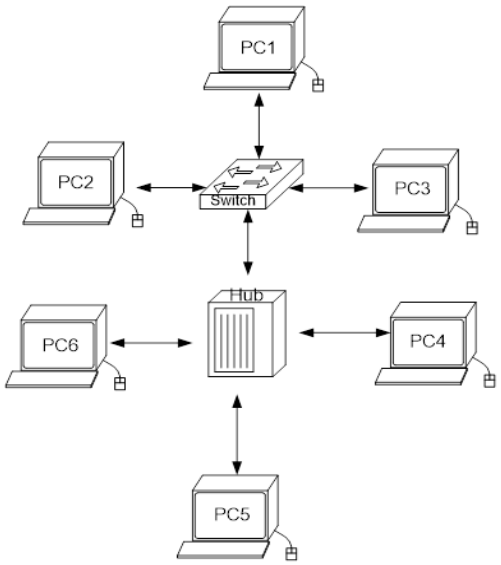


Рисунок 9 – Пример сети в cisco packet tracer.

Как известно, локальная вычислительная сеть – это компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий. В нашем случае это всего-навсего 6 рабочих станций, определенным образом связанных между собой. Для этого используются сетевые концентраторы (хабы) и коммутаторы (свичи).

Последовательность выполняемых действий:

1. В нижнем левом углу Packet Tracer выбираем устройства «Сетевые коммутаторы», и, в списке справа, выбираем коммутатор 2950-24,нажимая на него левой кнопкой мыши, вставляем его в рабочую область. Так же поступает с «Сетевым концентратором (Hub-PT)» и «Рабочими станциями (PC-PT)», в соответствии с рисунками 10, 11, 12, 13.

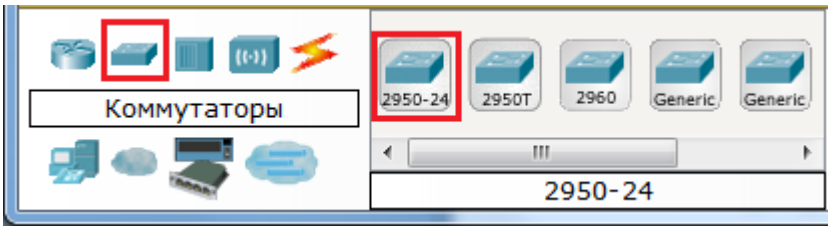


Рисунок 10 – Выбирается коммутатор 2950-24

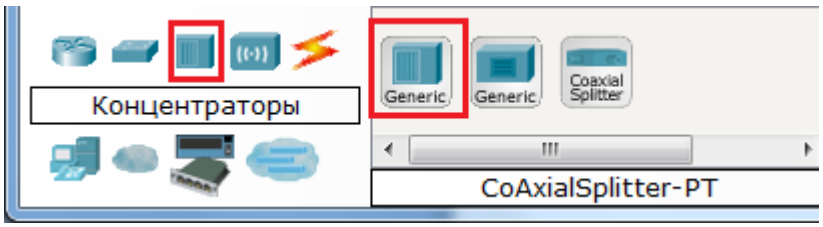


Рисунок 11 – Выбирается концентратор Hub-PT

Рисунок 12 – Выбирается персональный компьютер PC-PT

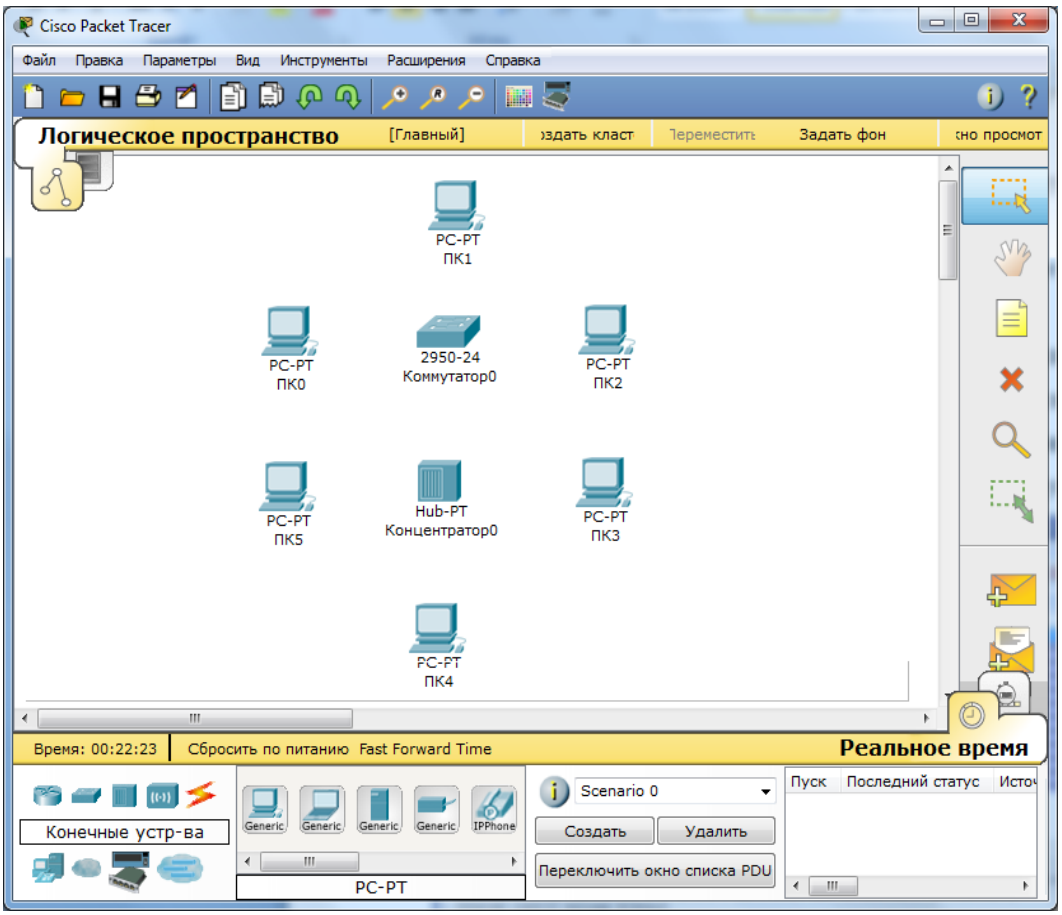


Рисунок 13 – Размещение компьютеров, коммутатора и концентратора на рабочей области

2. Далее необходимо соединить устройства, как показано на рисунке 8, используя соответствующий интерфейс. Для соединения компьютеров к коммутатору и концентратору используется кабель типа «медный прямой», в соответствии с рисунком 14.

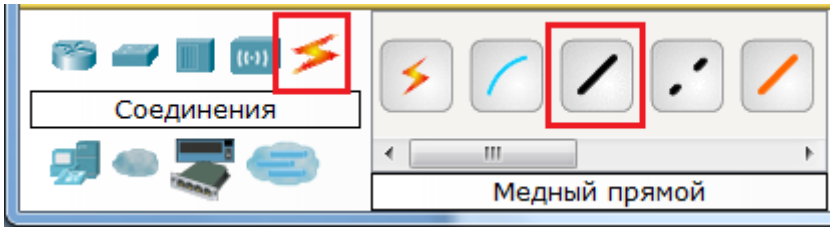


Рисунок 14 – Выбор типа кабеля «медный прямой»

А для соединения между собой коммутатора и концентратора используется медный кроссовер кабель, в соответствии с рисунком 15.

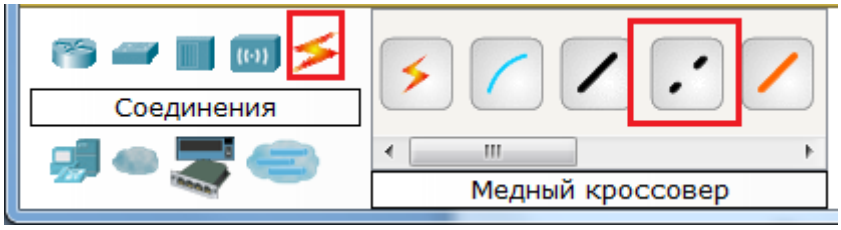


Рисунок 15 – Выбор типа кабеля «медный кроссовер»

Далее, для соединения двух устройств, необходимо выбрать соответствующий вид кабеля и нажать на одно устройство (выбрав произвольный свободный порт FastEthernet) и на другое устройство (также выбрав произвольный свободный порт FastEthernet), в соответствии с рисунками 16,17, 18.

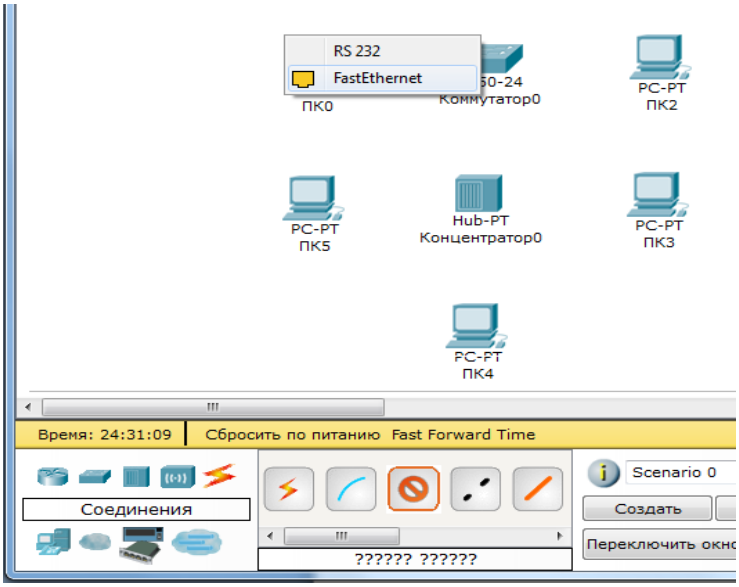


Рисунок 16 – Выбирается свободный порт на компьютере

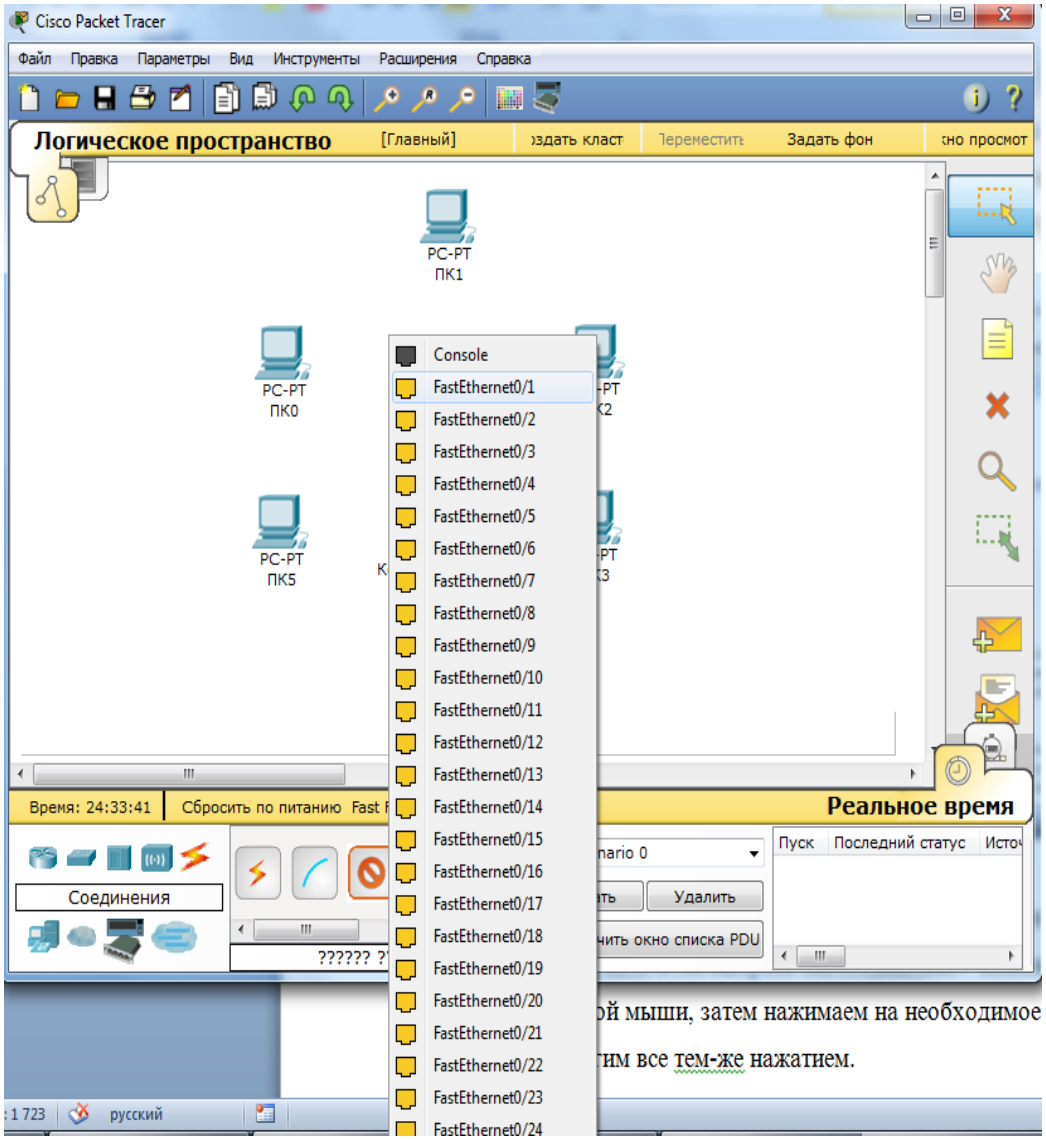


Рисунок 17 – Выбирается свободный порт на коммутаторе

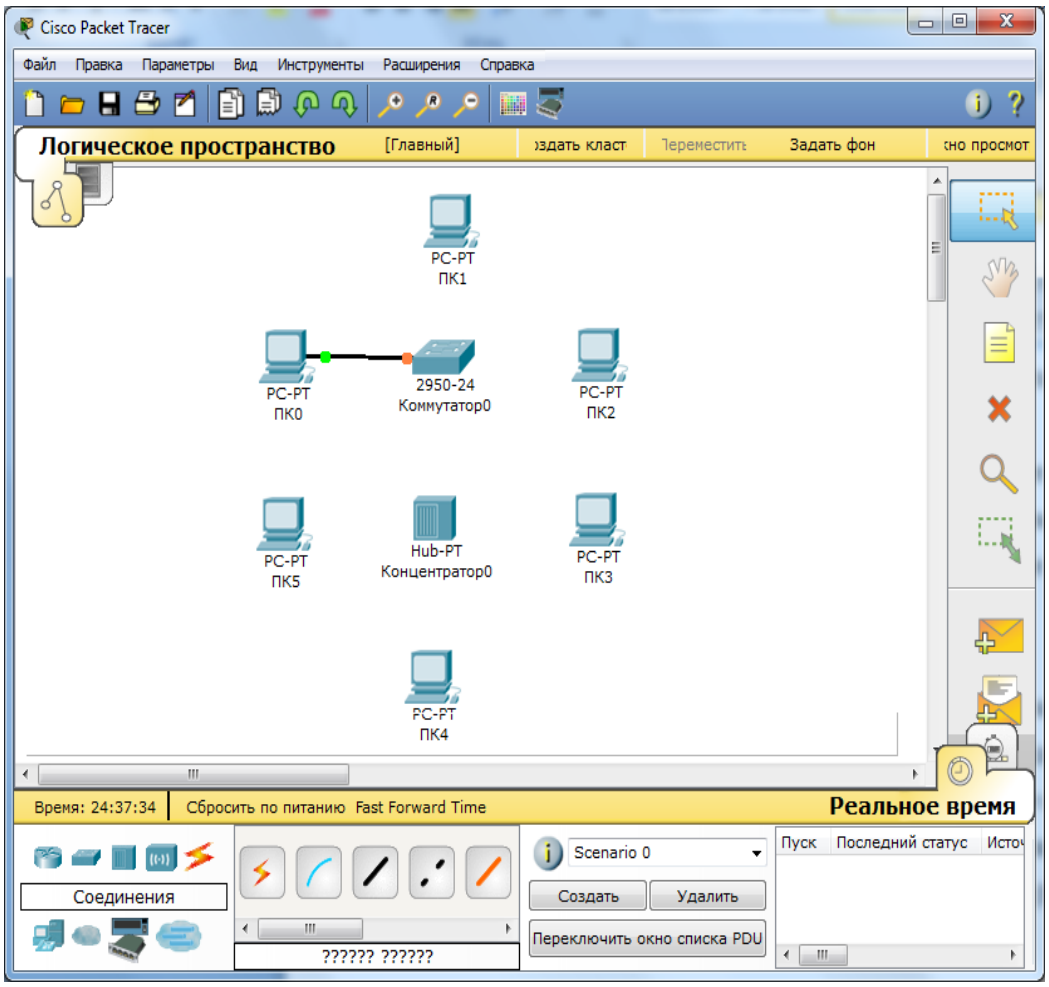


Рисунок 18 – Соединение медным прямым кабелем ПК 0 и коммутатор 0

Аналогично выполняется соединение для всех остальных устройств

Важно! Соединение между коммутатором и концентратором выполняется кроссовером.

Результат подключения устройств представлен на рисунке 19.

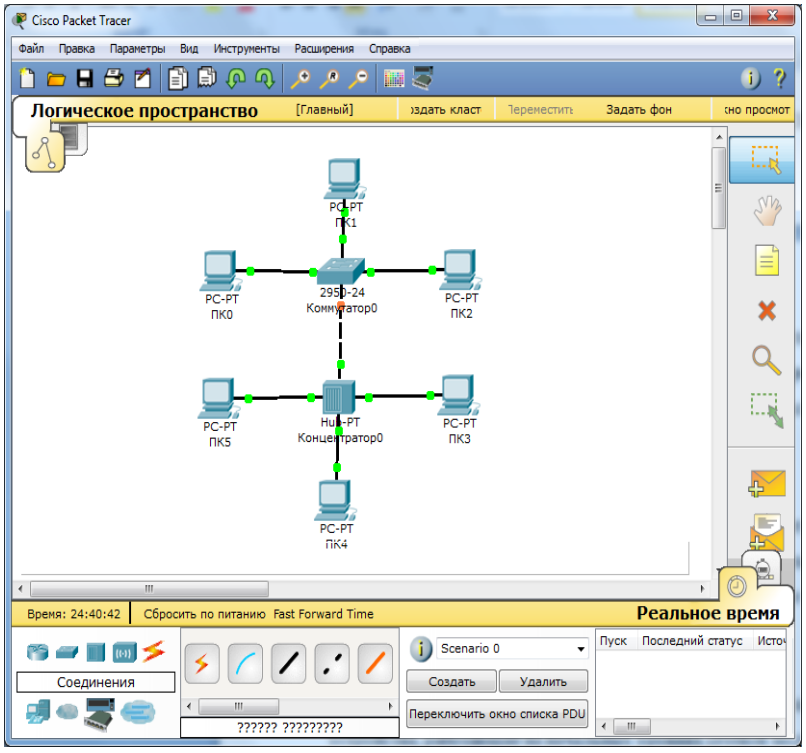


Рисунок 19 – Подключение устройств между собой.

3. Далее идет самый важный этап – настройка. Так как мы используем устройства, работающие на начальных уровнях сетевой модели OSI (коммутатор на 2ом, концентратор – на 1ом), то их настраивать не надо. Необходима лишь настройка рабочих станций, а именно: IP-адреса, маски подсети.

Ниже приведена настройка лишь одной станции (PC1) – остальные настраиваются аналогично.

Производим двойной щелчок по нужной рабочей станции, в соответствии с рисунком 20.

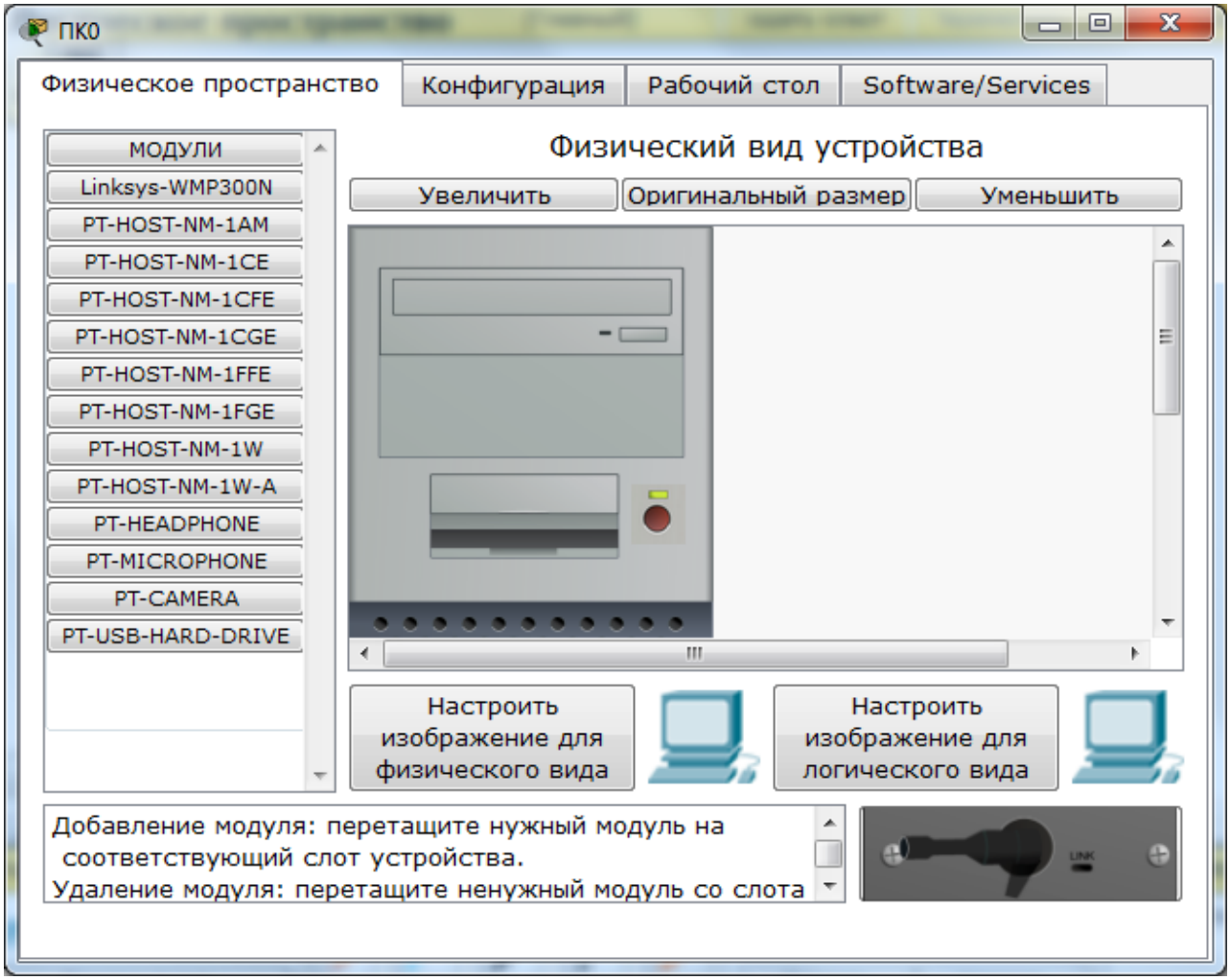


Рисунок 20 – Окно настройки компьютера PC0.

В открывшемся окне выбирается вкладку Рабочий стол, далее – «Настройка IP», в соответствии с рисунком 21.

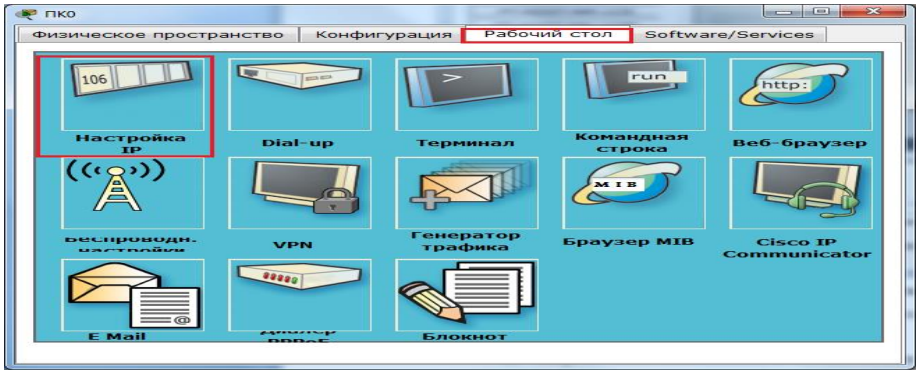


Рисунок 21 – Окно настройки компьютера PC0, вкладка «Рабочий стол».

Открывается окно, в соответствии с рисунком 22, где нужно ввести IP-адрес и маску.

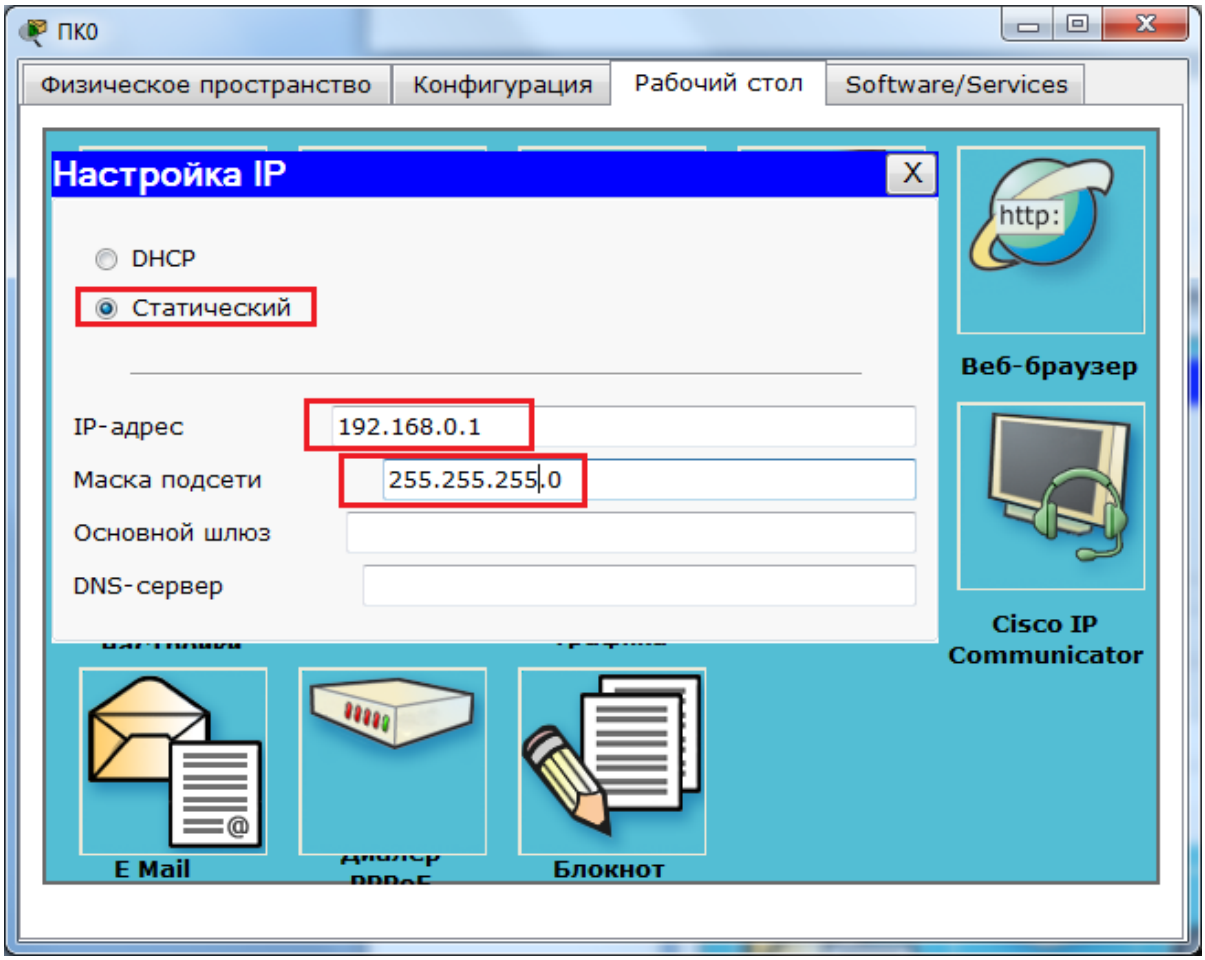


Рисунок 22 – Ввод статического IP-адреса и маски

Аналогично присваиваются IP-адреса всем остальным компьютерам.

Важно! IP-адреса всех рабочих станций должны находиться в одной и той-же подсети (то есть из одного диапазона), иначе процесс ping не выполнится.

Шлюз. Поле можно не заполнять.

DNS-сервер. Поле можно не заполнять.

4. Когда настройка завершена, выполняется ping-процесс. Например, запускается с PC5 и проверять наличие связи с PC1.

Важно! Можно произвольно выбирать, откуда запускать ping-процесс, главное, чтобы выполнялось условие: пакеты должны обязательно пересылаться через коммутатор и концентратор.

Для этого производим двойной щелчок по нужной рабочей станции, в открывшемся окне выбираем вкладку «Рабочий стол», далее – «Командная строка», в соответствии с рисунком 23.

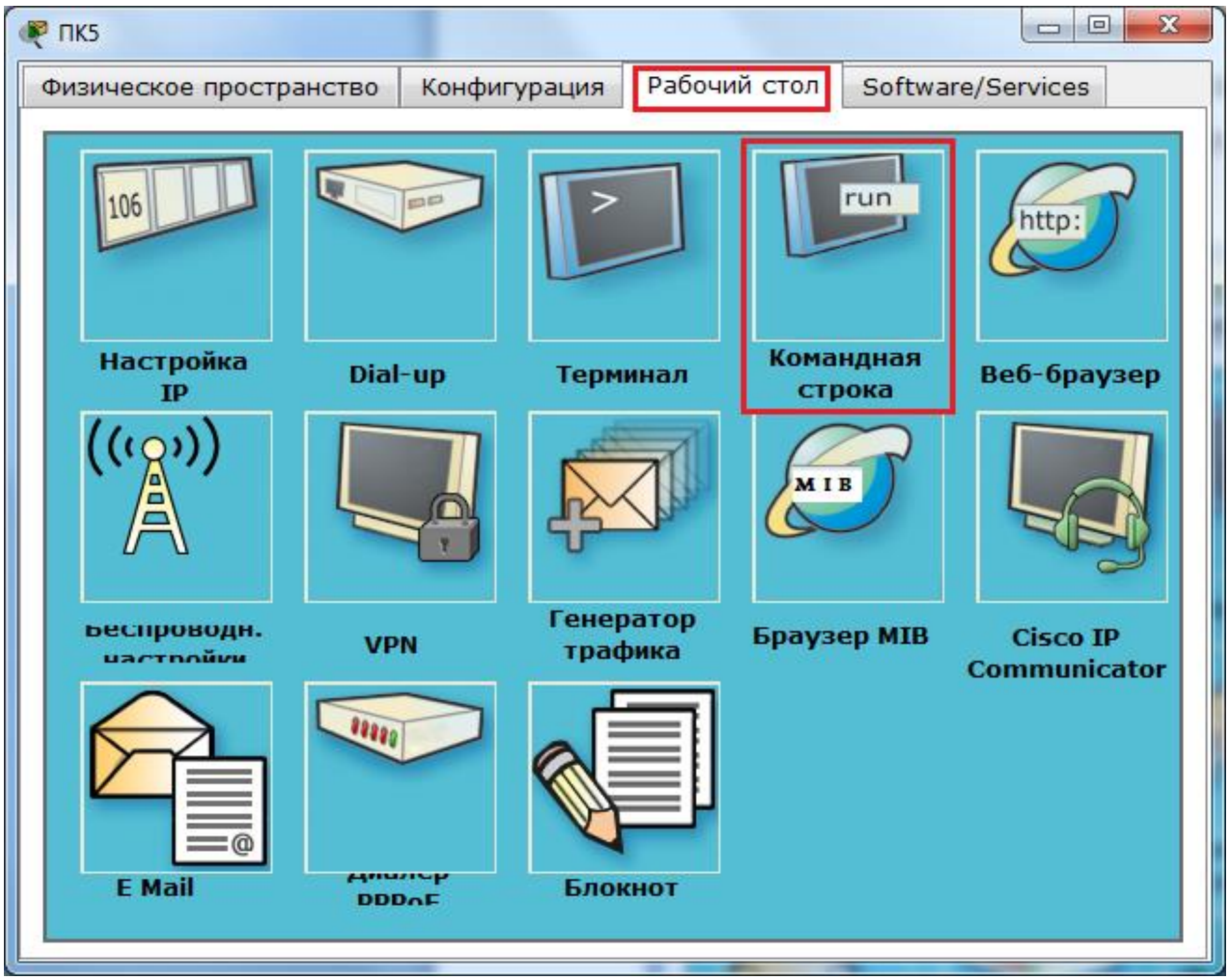


Рисунок 23 – Выбор режима «Командная строка»

Откроется окно командной строки, в соответствии с рисунком 24.

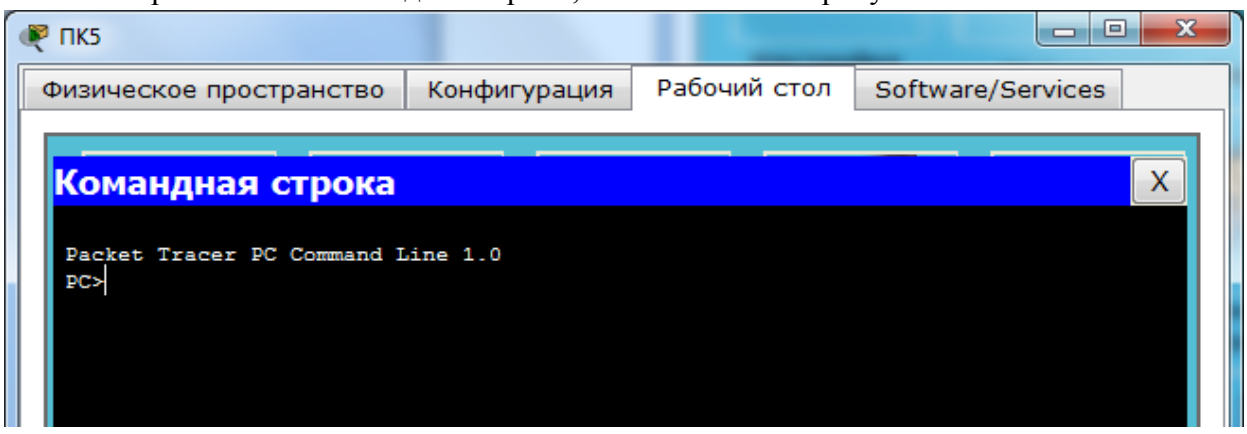


Рисунок 24 – Режим «Командная строка»

Нам предлагают ввести команду, что мы и делаем:

PC> ping 192.168.0.1

Нажимаем клавишу Enter. Если все настроено верно, то мы увидим следующую информацию, представленную на рисунке 25.

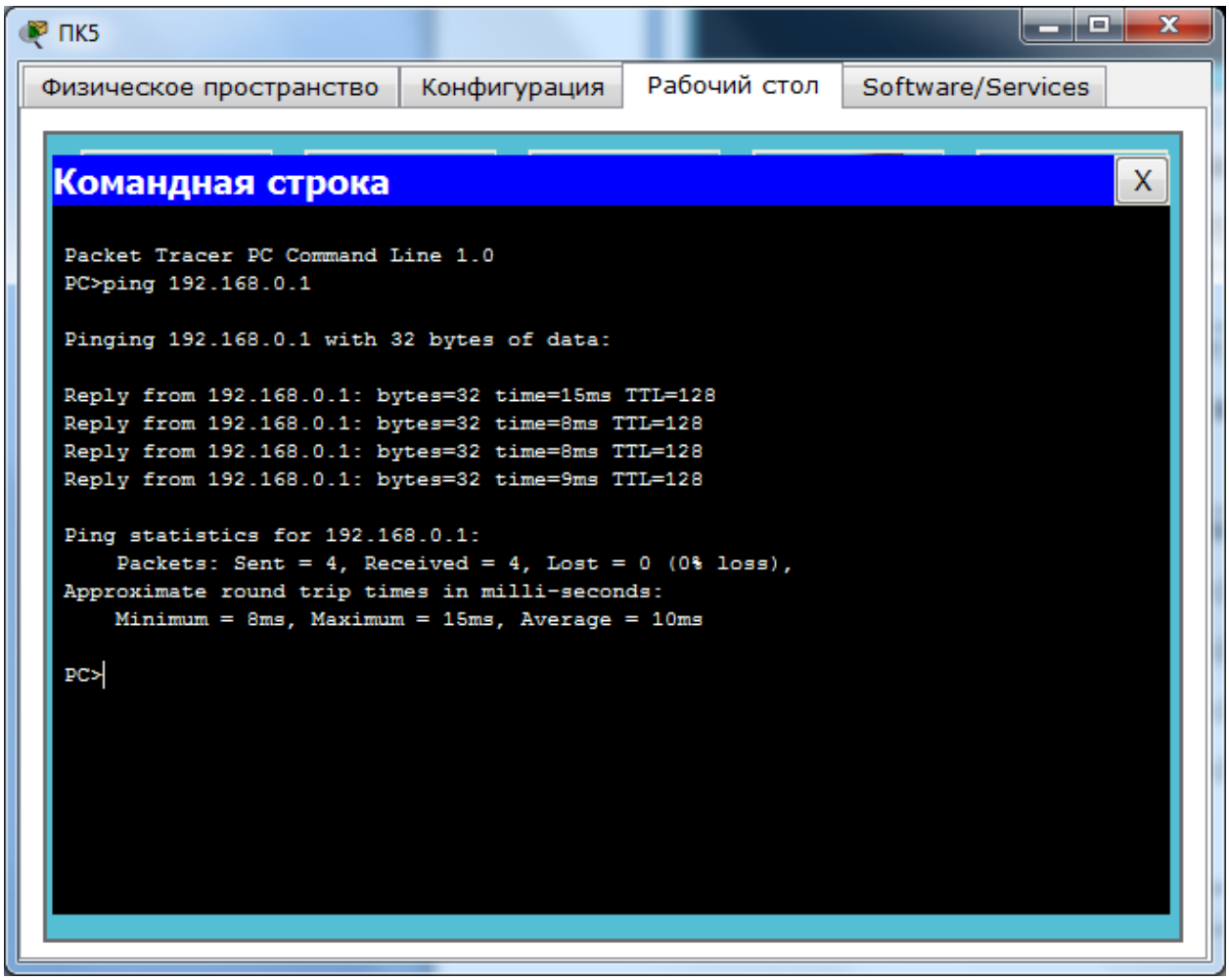


Рисунок 25 – Результат выполнение команды «ping»

Это означает, что связь установлена, и данный участок сети работает исправно.

Также Packet Tracer позволяет выполнять команду «ping» значительно быстрее и удобнее. Для этого, выбирается на боковой панели сообщение, в соответствии с рисунком 26.

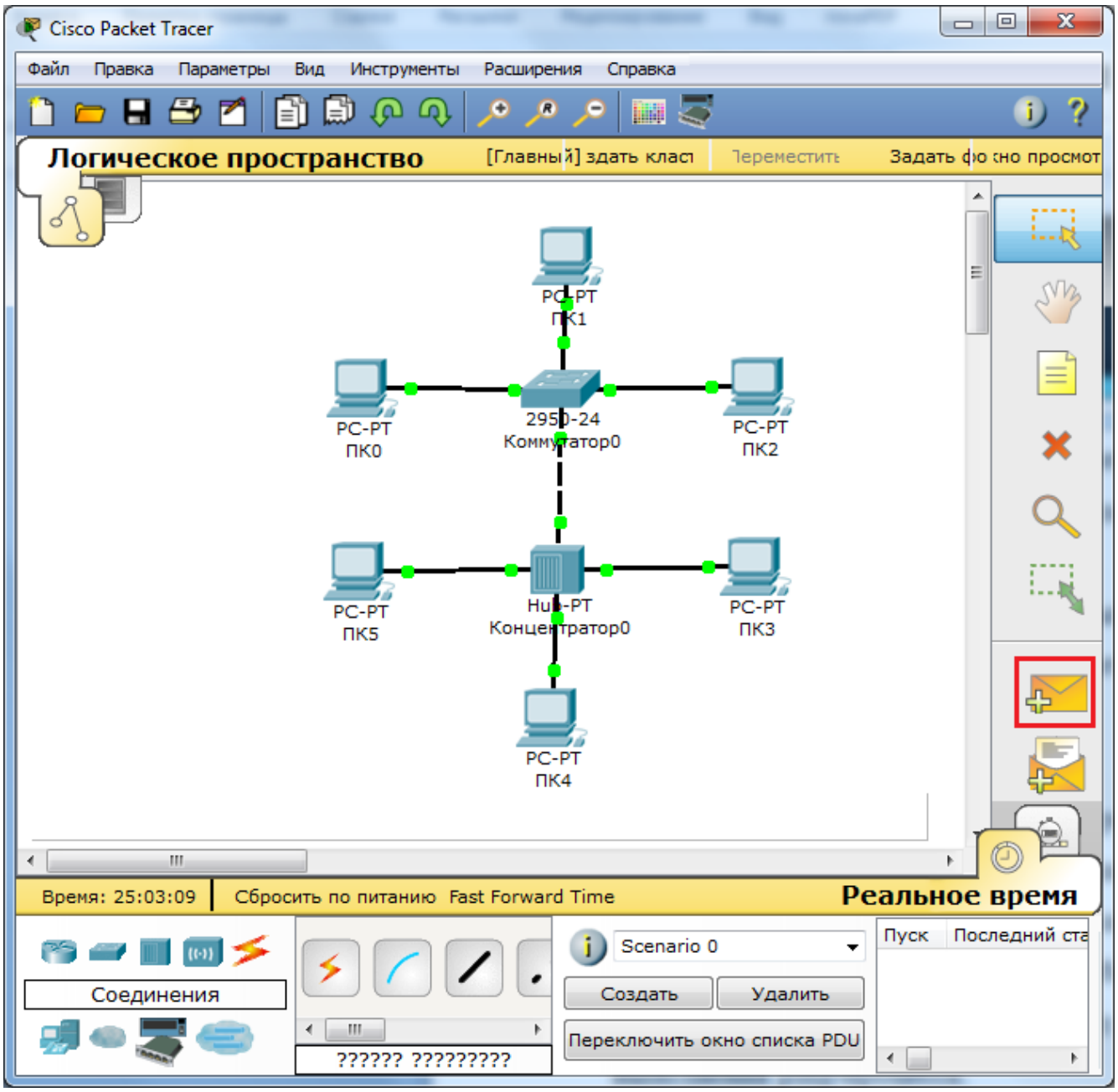


Рисунок 26 – Выбирается сообщение, для выполнение команды «ping»

Далее нужно кликнуть мышкой по компьютеру от кого будет передавать команда «ping» и еще раз щелкнуть по компьютеру, до которого будет выполнять команда «ping». В результате будет выполнена команда «ping», результат отобразиться в нижнем правом угле, в соответствии с рисунком 27.

Для более детального отображения результата выполнения команды выберите «Переключить окно списка PDU», в соответствии с рисунком 28.

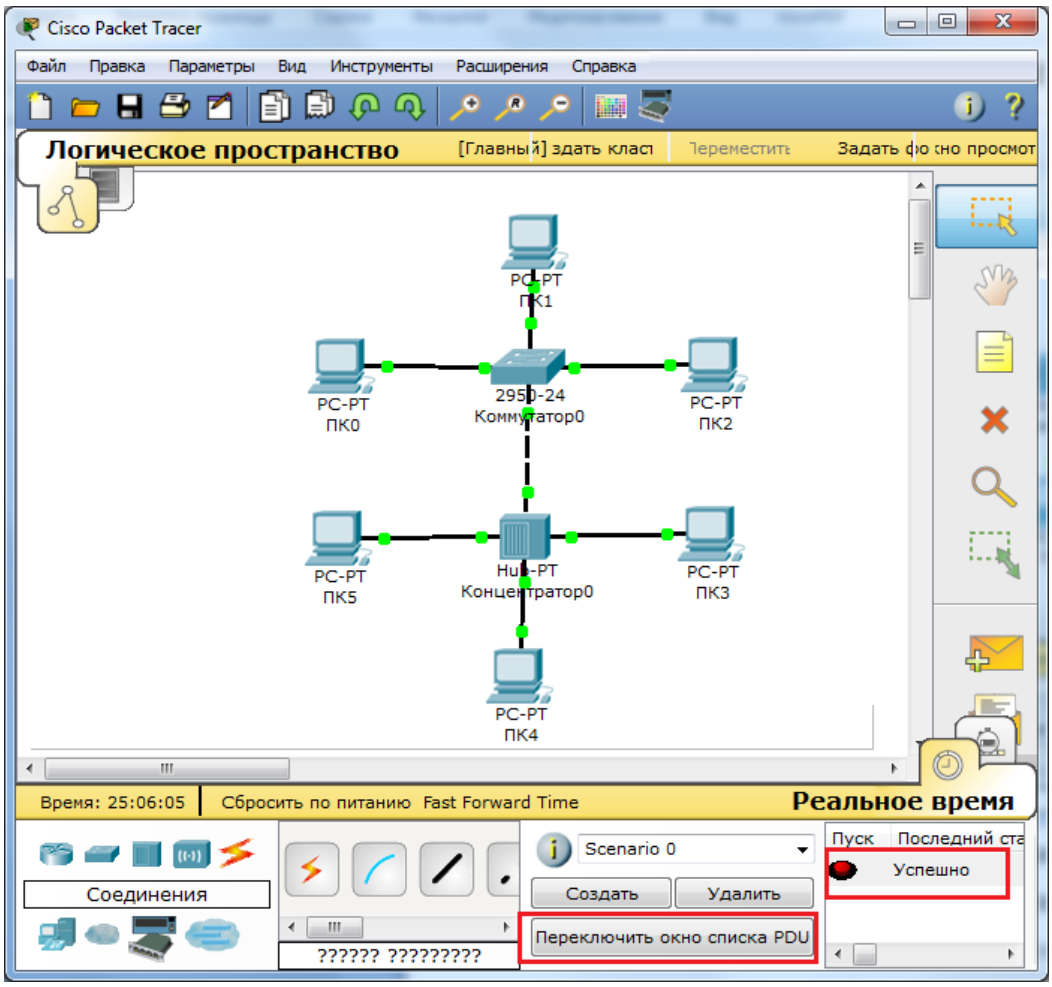


Рисунок 27 – Результат выполнения команды «ping»

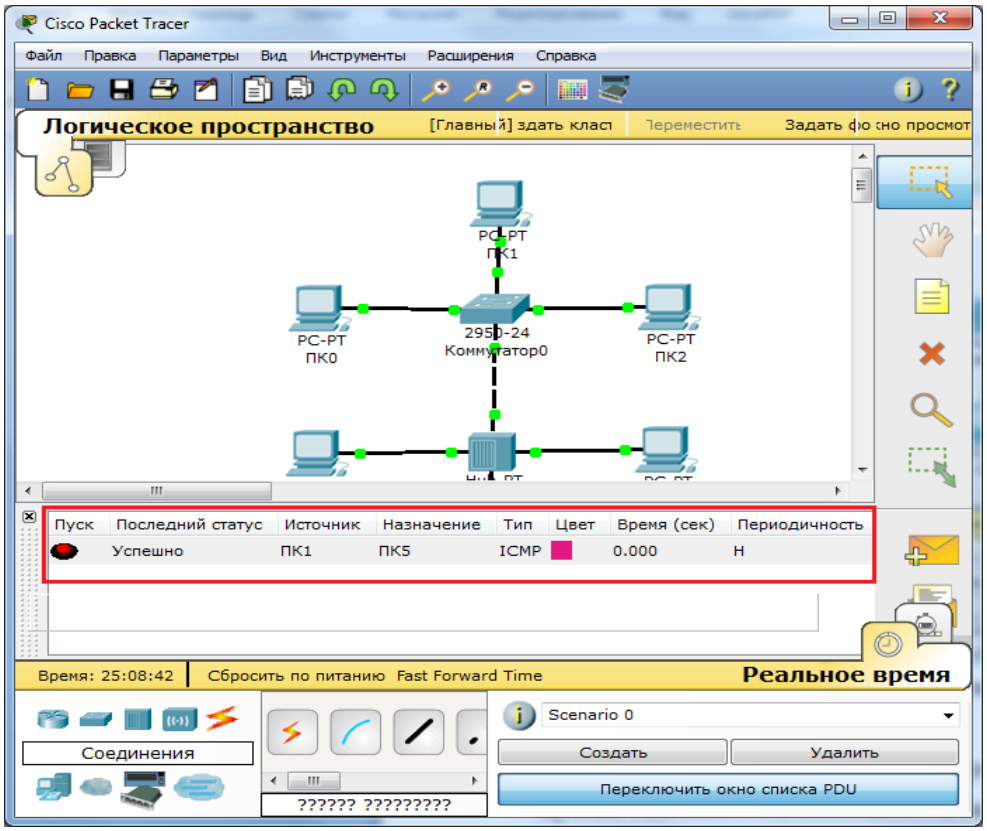


Рисунок 28 – Результат выполнения команды «ping»

5. В Packet Tracer предусмотрен режим моделирования, в котором подробно описывается и показывается, как работает утилита Ping. Поэтому необходимо перейти в «режим симуляции», нажав на одноименный значок в нижнем левом углу рабочей области, или по комбинации клавиш Shift+S. Откроется «Панель моделирования», в которой будут отображаться все события, связанные с выполнения ping-процесса, в соответствии с рисунком 29.

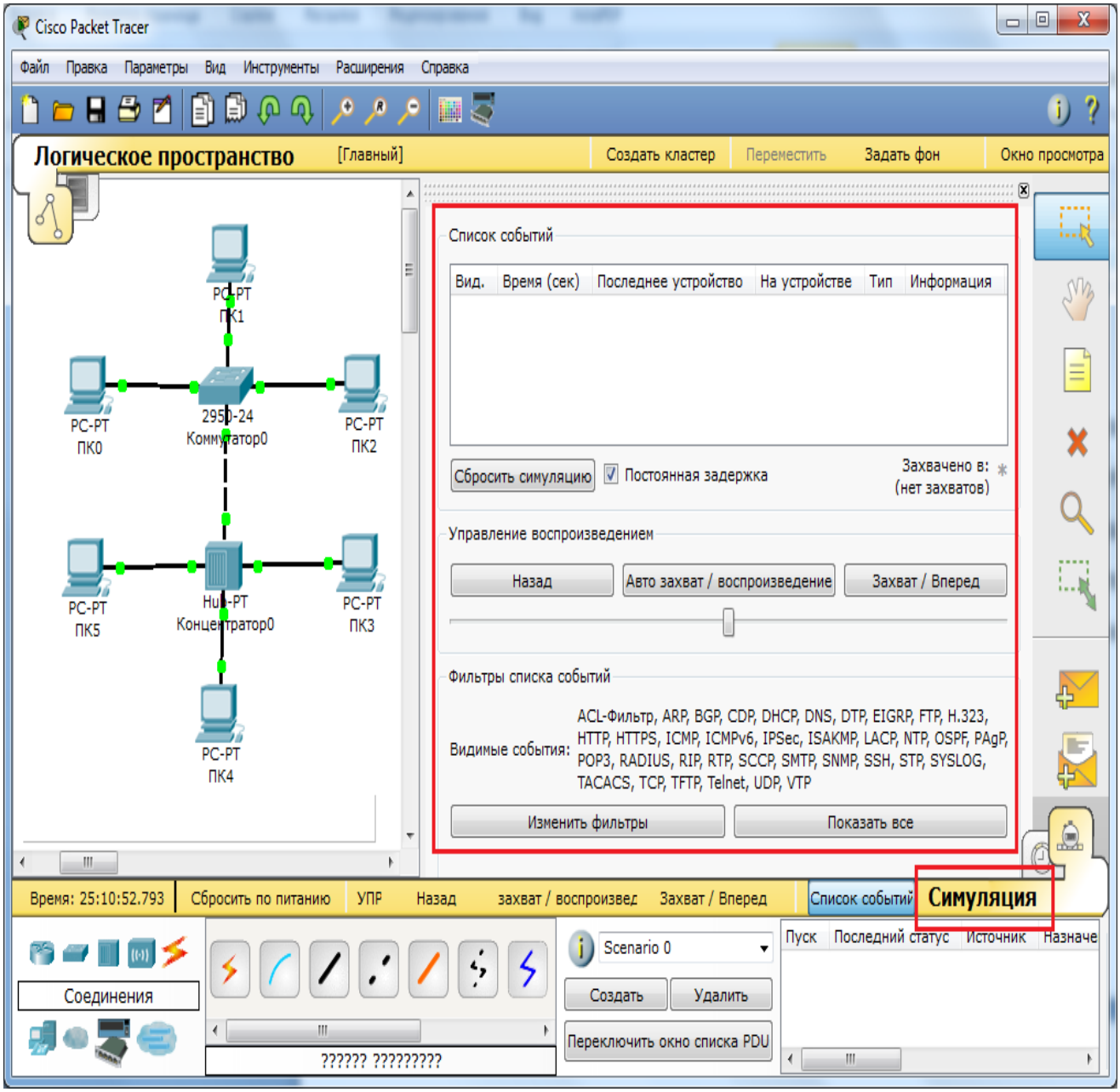


Рисунок 29 – Переход в «режим симуляции»

Перед выполнение симуляции необходимо задать фильтрацию пакетов. Для этого нужно нажать на кнопку «Изменить фильтры», откроется окно, в соответствии с рисунком 30, в котором нужно оставить только «ICMP» и «ARP».

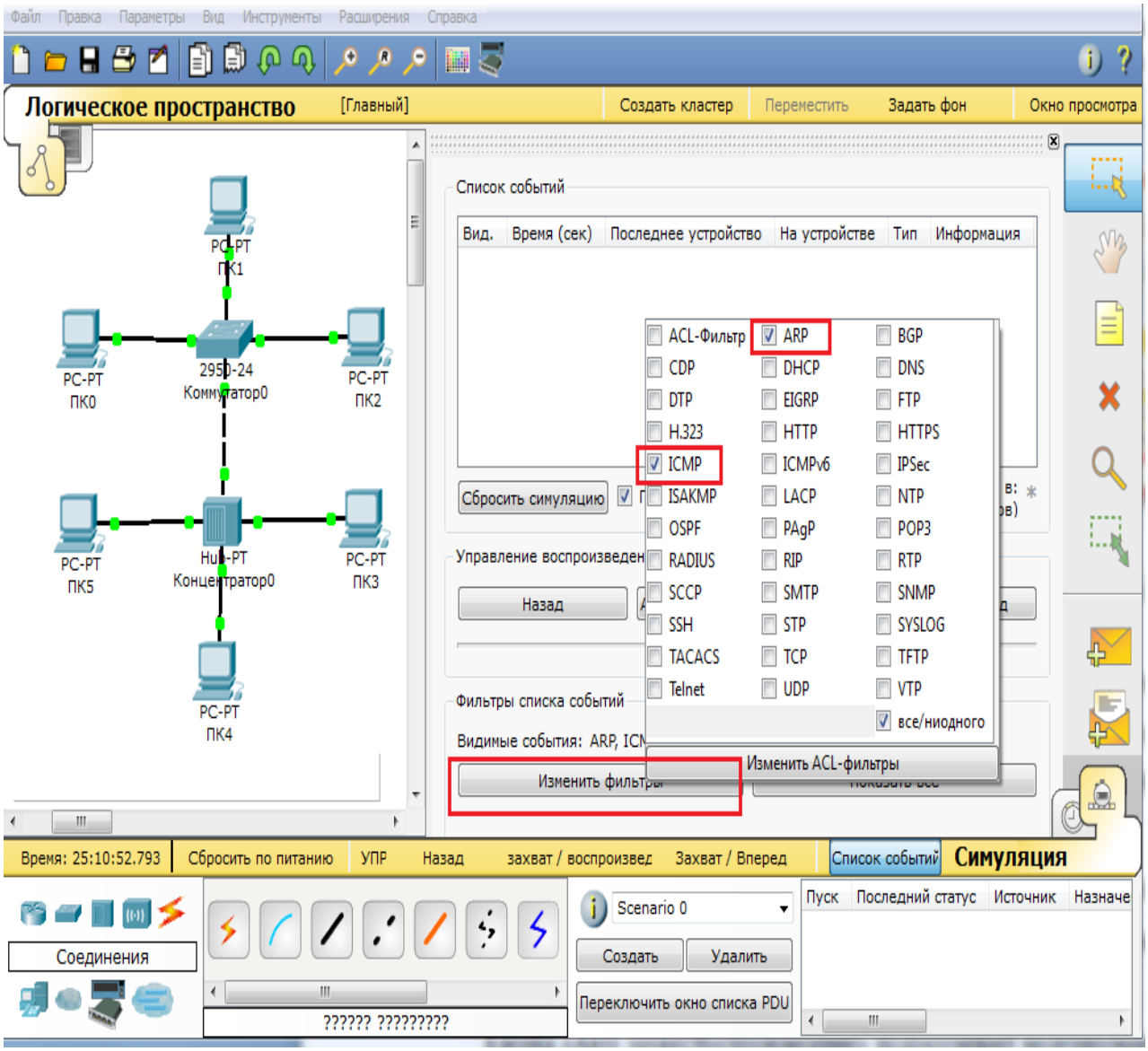


Рисунок 30 – Настройка фильтра

Теперь необходимо повторить запуск ping-процесса. После его запуска можно сдвинуть «Панель моделирования», чтобы на схеме спроектированной сети наблюдать за отправкой/приемкой пакетов.

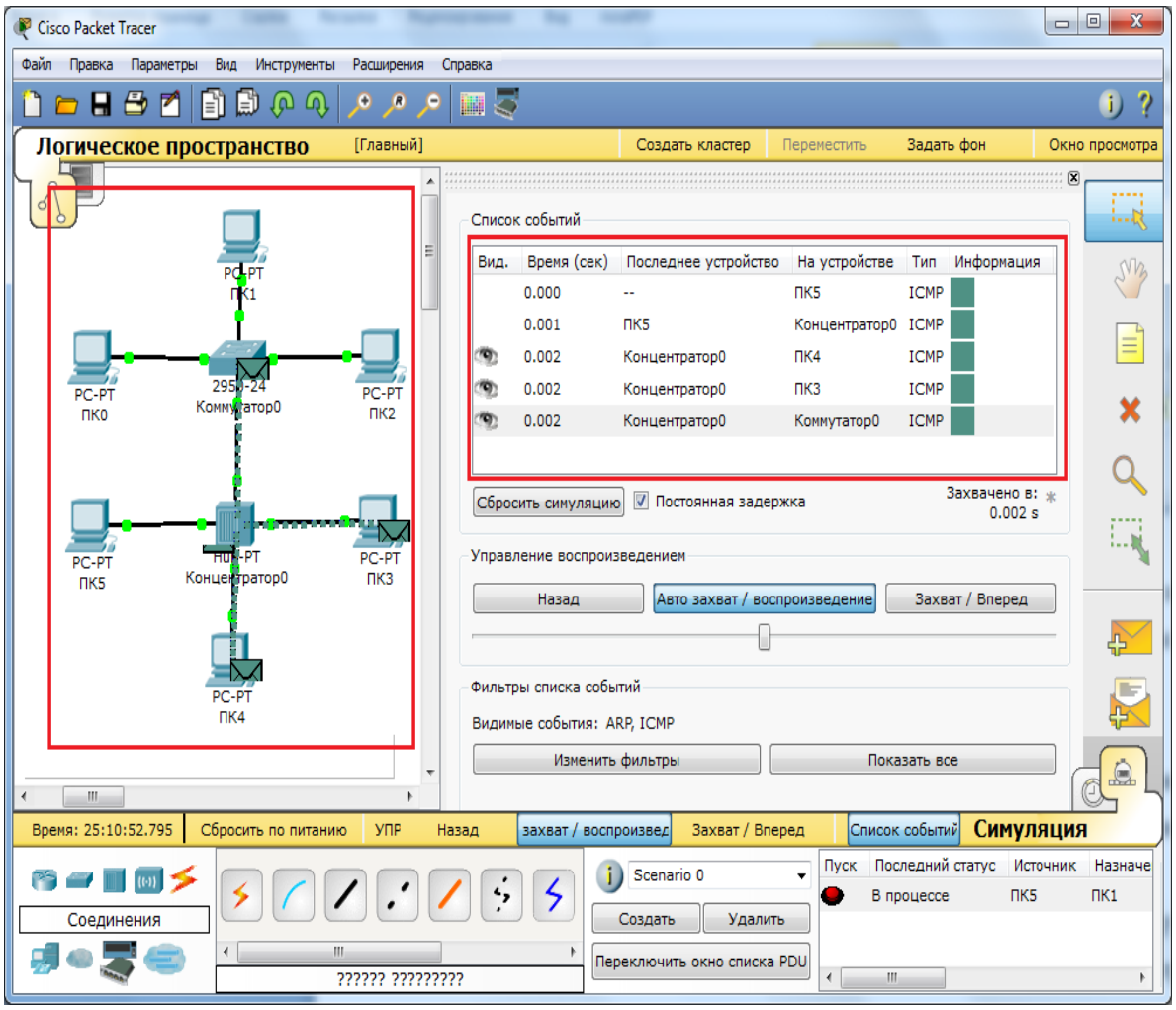


Рисунок 31 – Выполнение процесса симуляции

Кнопка «Авто захват/Воспроизведение» подразумевает моделирование всего ping-процесса в едином процессе, тогда как «Захват/Вперед» позволяет отображать его пошагово.

Чтобы узнать информацию, которую несет в себе пакет, его структуру, достаточно нажать правой кнопкой мыши на цветной квадрат в графе «Информация».

Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна «Редактирования» соответствующей рабочей станции.

Для удаления задания нажимается кнопка «Удалить» в нижней части экрана.

И так, мы научились основам работы с программой Cisco, рассмотрели основные возможности и принципы настройки, путем пошаговой инструкции по созданию локальной вычислительной сети.

Практическая работа № 14-15

Тема: «Объединение компьютеров в локальную вычислительную сеть»

Цель работы:

- Получить практические навыки в соединении компьютеров в локальную сеть;
- Выполнить диагностику и устранить неполадки, возникающие в процессе соединения.

Необходимое оборудование и материалы:

- Компьютеры.
- Кабель UTP категории 5.
- Разъемы RJ-45.
- Щипцы для обжима.
- LAN-Tester (Устройство для проверки правильности и качества обжима).
- Сетевые карты.
- Коммутатор или концентратор.

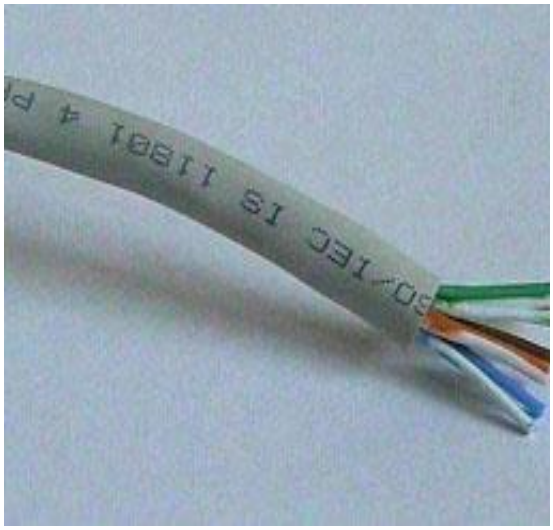
Теоретические сведения.

Разъемы RJ-45

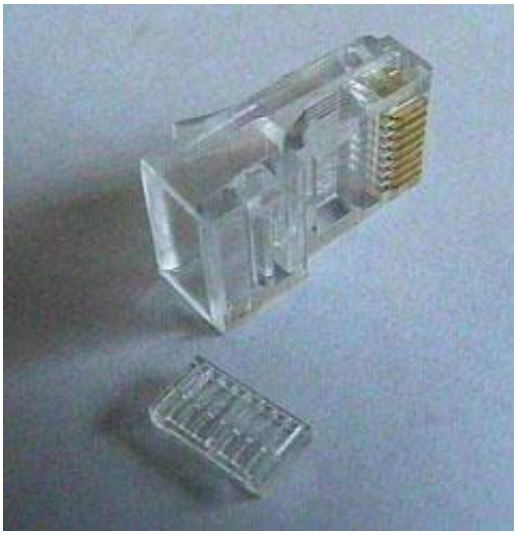
Для подключения витых пар используются разъемы стандарта RJ-45 , которые в зависимости от вида кабеля витой пары бывают:

- экранированными или неэкранированными;
- для одножильных или многожильных витых пар;
- конструктивно выполненными со вставками или без вставок. Вставки выполняют роль направляющих для проводников витой пары, упрощающих заправку проводников в корпус разъема.

Кабель из 4-х неэкранированных витых пар



Разъем RJ-45 для витой пары со вставкой



Корпуса разъемов выполнены из прозрачного пластика, поэтому внутренние части контактов разъема хорошо различимы. Нужно обратить внимание на конструктивное выполнение тех частей контактов, которые предназначены для соединения с проводниками витой пары. Контакты разъемов для многожильных проводников имеют вид двухзубой вилочки, внутренние

поверхности зубцов которой имеют заточку по типу ножа и при обжимке прорезают изоляцию проводника, раздвигая его жилы, таким образом создается контакт.

В разъемах для одножильных проводников зубцы вилочки слегка раздвинуты в стороны и при обжимке охватывают жилу с двух сторон, прорезая изоляцию и создавая контакт.

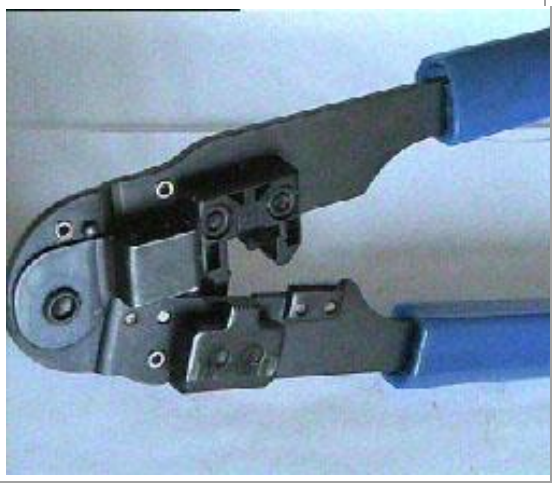
Для разделки витых пар используют специальное устройство (обжим), которое имеет три рабочие области и соответственно выполняет три функции.

Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников витой пары.

В центре находится гнездо для обжима разъема.

В верхней части устройства--область для зачистки наружной изоляции витой пары (внутренняя изоляция проводников не зачищается, а как уже было сказано прорезается контактами разъема).

Устройство для зачистки и обжима витых пар



2. Последовательность операций при разделке разъема витой пары

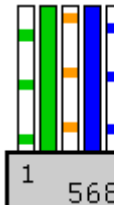
Вначале проводят зачистку наружной изоляции кабеля. При зачистке плоского кабеля его упирают в специальный выступ на устройстве, расположенный в области зачистки, чтобы получить глубину зачистки под стандартный разъем, зажимают кабель и рывком производят зачистку. Немного более сложным выглядит процесс зачистки круглых кабелей витых пар. Наружную изоляцию круглого кабеля лучше только слегка надрезать, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную.

Зачистка наружной изоляции круглого кабеля витой пары	Удаление наружной изоляции по кольцевому надрезу
	

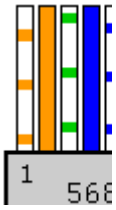
После зачистки разводят провода витой пары в одной плоскости в определенном порядке, выравнивают длину всех проводов и еще раз ровно подрезают. Порядок разводки проводов для разъемов RJ-45 определяется стандартом EIA/TIA568A или EIA/TIA568B.

Стандарт EIA/TIA568B более распространен, хотя принципиальной разницы между этими двумя стандартами нет. Для получения прямого кабеля для подключения к активному оборудованию нужно, чтобы порядок разводки с обоих концов кабеля был одинаковым. Для получения перекрестного (CROSSOVER) кабеля для соединения двух сетевых адаптеров напрямую необходимо с разных концов кабеля использовать разные стандарты.

	белый/зеленый
	зеленый
	белый/оранжевый
	синий
	белый/синий
	оранжевый
	белый/коричневый
	коричневый

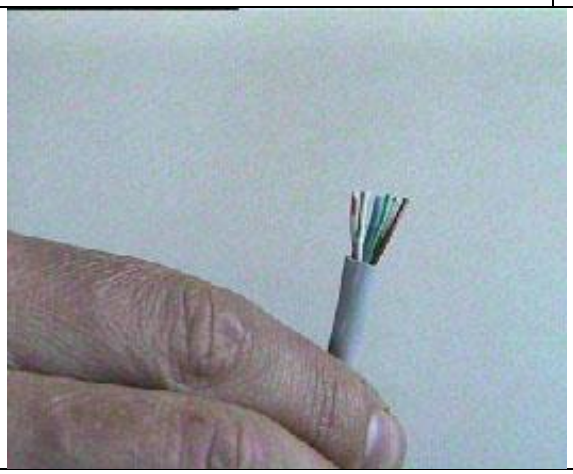
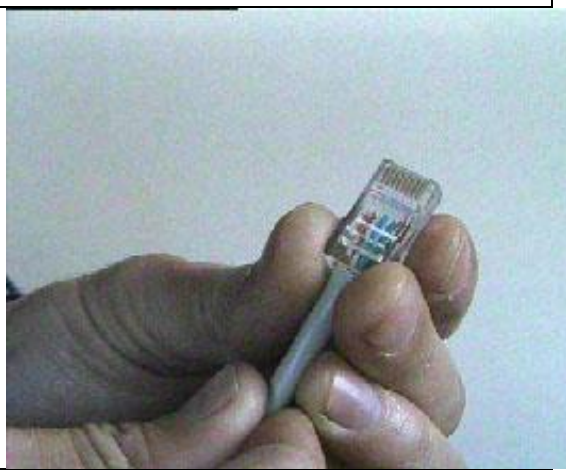


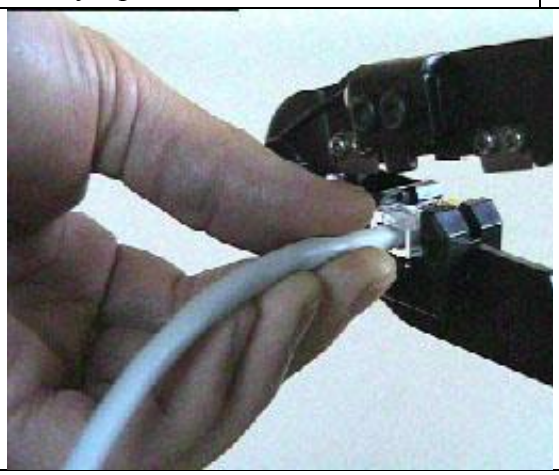
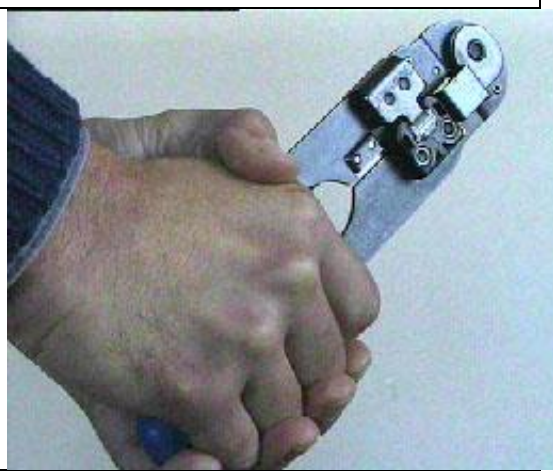
	белый/оранжевый
	оранжевый
	белый/зеленый
	синий
	белый/синий
	зеленый
	белый/коричневый
	коричневый



Затем производят заправку проводников в разъем и обжимку. Рекомендуется по возможности использовать разъемы без вставки, так как процесс заправки проводников в корпус такого разъема выполняется проще.

Если конструктивно разъем выполнен без вставки, то проводники аккуратно заправляются в его корпус до упора в торец разъема. Затем вставляют разъем в гнездо обжимного устройства и надавливают до тех пор, пока устройство полностью не закроется.

Кабель витой пары, подготовленный для заправки в разъем	Заправка проводников витой пары в разъем RG-45 без вставки
	

Установка разъема RJ-45 в гнездо обжимного устройства	Обжимка разъема
	

Если в конструкцию разъема входит вставка, то сначала на проводники витой пары надевается вставка. Вставка имеет форму крышки спичечного коробка, на одной из поверхностей которого имеются прорези по количеству проводников в витой паре. Вставку надевают на проводники таким образом: чтобы прорези были обращены к корпусу разъема. После насаживания вставки проводники витой пары еще раз подрезают и выравнивают срез с краем вставки. Для закрепления вставки в этом положении полезно у ее противоположного конца обжать проводники пальцами, чтобы вставка не смещалась. Затем вставку с проводниками вставляют в корпус разъема до тех пор, пока она не упрется в торец разъема, и обжимают разъем также как в случае разъема без вставки.

4. Порядок выполнения работы

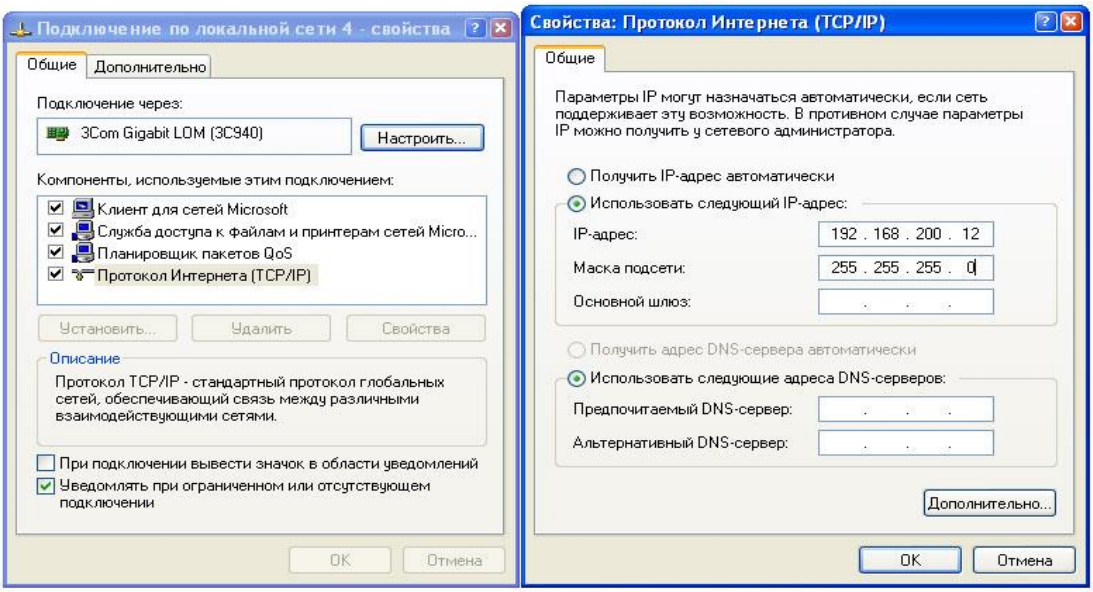
Задание 1. Соединить два компьютера между собой без использования активного сетевого оборудования типа коммутатора, концентратора.

1. Для выполнения работы подгруппа разделяется на несколько бригад. Каждой бригаде студентов предоставляются 2 компьютера, которые необходимо объединить в сеть.
2. Включить компьютеры и проверить их работоспособность.
3. Установить в компьютеры сетевые карты. Перед установкой сетевых карт необходимо ВЫКЛЮЧИТЬ питание. Обязательно закрепить карты при помощи винта.
4. Обжать кабель для соединения двух компьютеров. Обжим выполняется перекрестным способом. Убедиться в успешности обжимки при помощи тестера.
5. Соединить компьютеры обжатым кабелем.
6. Включить компьютеры.
7. Убедиться в исправности сетевых карт. Обычно на сетевых картах имеется индикатор «LINK». Он показывает наличие физического соединения по сетевому кабелю. Соответственно, при отключенном кабеле индикатор гореть не должен, а при правильно подключенном с обоих концов кабеле – должен. Если это так – сетевая карта скорее всего физически исправна.
8. Если индикатор не включен, проверить правильность обжима кабеля с помощью тестера и при необходимости повторить обжим кабеля.
9. Установить драйверы сетевых карт. Операционная система обнаруживает новое оборудование, если оно поддерживает стандарт Plug and Play. Далее, если драйвер устройства входит в дистрибутив системы – он устанавливается оттуда, если не входит – с носителя,

поставляемого вместе с устройством. Дистрибутив Windows находится на диске С в папке \win 98 SE. Драйверы устройств записаны на диске С в папке \ drivers\. Беспроблемное обнаружение устройства, установка драйверов и отображение сообщения «устройство работает нормально» в свойствах устройства в диспетчере устройств свидетельствуют об исправности сетевой карты. При неисправности сетевой карты заменить ее и повторить проверку.

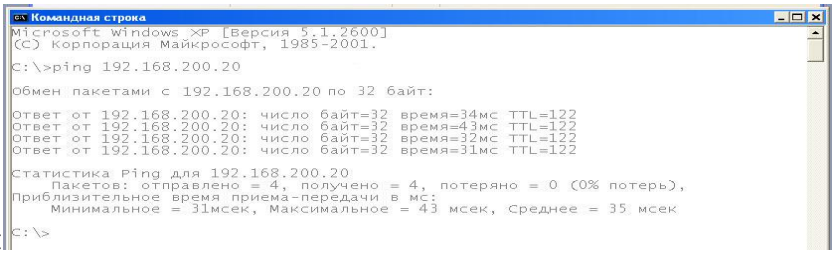
10. Произвести настройку протокола IP. Назначить компьютерам статические
11. IP-адреса (не одинаковые и принадлежащие одной подсети) и указать маску подсети.

Например:



Убедиться в наличии соединения между компьютерами. Проверку связи между компьютерами можно выполнить с помощью утилиты ping. Для этого в командной строке вводится ping и адрес проверяемого компьютера. Можно использовать IP-адрес, Net BIOS имя.

Например:



Если проверка проходит нормально, значит сеть полностью работоспособна.

Создать на диске временную папку, установить на нее общий доступ. Со второго компьютера попробовать скопировать в нее файлы. Нормальное копирование данных подтверждает работоспособность сети.

Задание 2. Соединить компьютеры между собой с использованием активного сетевого оборудования.

2. Задание 2 выполняется, после того, как все бригады выполнили задание №1.
3. Для соединения компьютеров с активным оборудованием необходимо обжать дополнительные кабели (по одному на каждый компьютер). Кабель должен быть прямым, а не перекрестным, то есть иметь одинаковый стандарт обжима с обоих концов. Хотя, в настоящее время часто встречается оборудование, автоматически определяющее тип подключенного кабеля, и способное работать как с тем, так и с другим.

4. Подключить все компьютеры к коммутатору или концентратору с помощью подготовленных кабелей.

5. Проверить, что все компьютеры находятся в одной подсети, и если это не так, изменить IP-адреса должным образом.

6. Проверить, есть ли доступ к общим ресурсам всех компьютеров. При отсутствии доступа проверить правильность обжима кабелей и исправность сетевых карт. Добиться работоспособности всей сети.

Возможные проблемы при соединении компьютеров:

– Неверно или некачественно обжат кабель. В этом случае процедуру обжимки придется повторить с самого начала.

– Разъем неплотно вставлен в гнездо сетевой карты. Вставлять разъем нужно до защелкивания собачки.

– Неисправна сетевая карта. В этом случае сетевую карту необходимо заменить.

– Неверно прописан IP адрес машины. Оба компьютера должны находиться в одной подсети. Это означает, что маски подсети у них одинаковы, номера подсетей совпадают, а номера хостов могут быть любыми допустимыми, но не одинаковыми.

5 Содержание отчета:

– Тема и цель работы

– Теоретические сведения о стандартах обжима витой пары (различие в использовании)

– Последовательность выполнения задания

– Анализ обнаруженных неисправностей и способы их устранения

– Вывод по лабораторной работе (рекомендации по устранению неполадок, порядок проверки неисправностей)

6 Контрольные вопросы:

1. Какое оборудование необходимо использовать при объединении двух компьютеров в сеть без активного сетевого оборудования ?

2. Как проверить правильность обжима сетевого кабеля?

3. Какой способ обжима кабеля используется при подключении компьютера к коммутатору?

4. Как определить исправность сетевой карты?

5/ Как проверить наличие связи между компьютерами?

6. В каком случае используются сетевые кабели с перекрестным обжимом?

7. Как должны быть назначены адреса компьютеров одной сети?

8. Как проверить возможность доступа к общим ресурсам сети?

9. Что может быть причиной нарушения связи между компьютерами сети?

10. В чем заключается настройка протокола IP при объединении компьютеров в сеть?

Практическая работа № 16-17

Тема: «Подключение и использование локальной сети. Диагностирование и настройка сетевых соединений.»

Цель работы: Приобретение практических знаний и навыков в настройке программного обеспечения ПЭВМ для обеспечения функционирования в составе локальной компьютерной сети.

Теоретические основы.

TCP/IP — набор сетевых протоколов, через которые компьютеры устанавливают связь друг с другом. Протокол определяет правила передачи данных по сети.

IP –адрес идентифицирует, определяет компьютер, подключенный к сети TCP/IP.

ICMP – протокол управляющих сообщений, используется, чтобы информировать о действиях и ошибках в сети. Например, маршрутизатор, не найдя соответствующего элемента для сети в таблице маршрутизации, отправляет сообщение ICMP.

DNS –сервер – содержит базу данных имен хостов и алиасных имен (имен –псевдонимов), ставящих в соответствие IP- адресам имена. Сервер DNS сначала проверяет собственную базу данных и кэш, и если ему не удается разрешить имя, он запрашивает корневой сервер DNS. По всему миру находятся несколько корневых серверов DNS. Для ускорения обработки следующих запросов серверы DNS сохраняют в кэше информацию, не найденную в их базе данных.

MAC – адрес – физический адрес определяется сетевой интерфейсной картой, обычно шести байтный. Уникальность адреса обеспечивается изготовителем.

Маршрутизатор (Роутер) – устройство, соединяющее несколько физических сетей. Маршрутизатор получает сообщение и направляет его адресату, используя известный ему наилучший путь к этому адресату. Он хранит таблицу маршрутов. Собирает информацию о путях между сетями: данные о потери пакетов и время передачи.

Основной шлюз – IP адрес маршрутизатора, соединение с которым будет происходить напрямую.

Пакет – блок информации в виде двоичных цифр, представляющих данные и служебную информацию. Внутри пакета эта информация расположена в соответствии с определенным форматом.

TTL- значение времени жизни, определяет число маршрутизаторов, через которые может пройти пакет. Оно инициализируется отправителем и уменьшается на единицу каждым маршрутизатором, обрабатывающим пакет.

Маска подсети используется для определения маршрутизатором номера сети и номера узла в конструкторе IP адреса.

Сетевой порт представляет собой число от 1 до 65535, указанное и известное обоим приложениям, между которыми устанавливается связь. Например, клиент, как правило, посылает незашифрованный запрос в сервер по целевому адресу на TCP-порт 80. Обычно компьютер посылает запрос DNS на DNS-сервер по целевому адресу на UDP-порт 53. Клиент и сервер имеют IP-адрес источника и назначения, а также сетевой порт источника и назначения, которые могут различаться. Исторически все номера портов ниже 1024 получили название «известных» или служебных номеров портов и зарегистрированы в организации IANA (Internet Assigned Numbers Authority). В некоторых операционных системах только системные процессы могут использовать порты этого диапазона. Кроме того, организации могут зарегистрировать в IANA порты с 1024 по 49151-й, чтобы связать порт со своим приложением. Такая регистрация обеспечивает структуру,

которая помогает избежать конфликтов между приложениями, стремящимися использовать порт с одним номером. Однако в целом ничто не мешает приложению запросить конкретный порт, если он не занят другой активной программой.

Порядок проведения работы.

Проверка работоспособности сетевого соединения с использованием стандартных утилит Windows.

Утилита ping

Утилита ping тестирует сетевое соединение путем посылки ICMP-пакетов типа 8 (*запрос эха*), на которые получатель отвечает ICMP-пакетом типа 0 (*эхо-ответ*). С помощью этой утилиты удобно проверять наличие пути до заданного узла и определять временные характеристики этого пути. Утилите ping достаточно указать IP-адрес или DNS-имя, однако имеется ряд параметров, позволяющих более тонко управлять ее работой. Утилита ping выводит результат каждого запроса/ответа на отдельной строке, а перед завершением работы выдает статистику: минимальное, максимальное и среднее время передачи пакета, количество и долю потерянных пакетов. Фактически ping является '*рабочей лошадкой*' при тестировании сетевых соединений.

Общий формат использования утилиты (как всегда, находящиеся в квадратных скобках параметры опциональны): ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]] [-w таймаут] конечноеИмя. Для получения такой подсказки достаточно запустить ping без параметров, для вывода подсказки в файл ping_test.txt следует использовать ping > ping_test.txt (то же относится и к большинству иных утилит).

Параметр '-t' включает постоянную проверку связи до нажатия Ctrl+C. При нажатии Ctrl+Break выводится статистически накопленная информация и работа продолжается (обычно этот параметр используют, чтобы как можно быстрее узнать о наличии связи с заданным узлом).

Параметр '-a' требует определение IP-адреса по имени узла (по умолчанию не выполняется).

Параметр '-n <число>' позволяет задать количество запросов (по умолчанию четыре запроса).

Параметр '-l <число>' дает возможность задать размер пакета (по умолчанию размер пакета 64 байта).

Параметр ‘-f’позволяет установить в запросах флаг ‘не фрагментировать’. Используется в сочетании с параметром ‘-l’для обнаружения сетей с малым размером кадра, для передачи через которые IP-пакеты приходится фрагментировать.

Параметр ‘-i <число>’ задает время жизни пакета (TTL), по умолчанию у ICMP-пакетов время жизни равно 255.

Параметр ‘-r <число>’ дает возможность получить маршрут, по которому передавались запрос и ответ (показать маршрутизацию). Числовой параметр может быть от 1 до 9 и определяет максимальное количество узлов, которые будут показаны в маршруте.

Параметр ‘-w <число>’ позволяет задать время ожидания каждого пакета (в миллисекундах), по умолчанию это 1’000 миллисекунд.

Утилита tracert

Утилита tracert дает возможность проследить маршрут пакетов до заданного узла и получить временные характеристики для каждого промежуточного маршрутизатора на этом пути. Эта утилита, как и ранее описанная ping, отправляет серию пакетов ICMP типа 8, но с разными значениям TTL: сначала отправляется три пакета с TTL=1 (на эти пакеты *ближайший маршрутизатор* ответит пакетами ICMP типа 11 (*истекло время передачи*), из которых будет извлечен его адрес), затем с TTL=2 (на эти пакеты ответит второй маршрутизатор) и так далее до тех пор, пока не будет достигнут заданный узел или значение TTL не превысит порог. Для каждого TTL утилита выводит по одной строке с адресом маршрутизатора (и, возможно, с его доменным именем - если удалось его разрешить) и тремя значениями времени, которое понадобилось для передачи пакета. Формальный синтаксис: tracert [-d] [-h максЧисло] [-j списокУзлов] [-w интервал] имя.

Параметр ‘-d’ позволяет (принудительно) не выполнять разрешение IP-адресов маршрутизаторов в доменные имена, это позволяет ускорить работу утилиты за счет отмены обращения к службе DNS.

Параметр ‘-h <число>’ дает возможность задать порог, до которого будет расти TTL (по умолчанию - 30).

Параметр ‘-w <число>’ позволяет задать время ожидания каждого пакета (в миллисекундах), по умолчанию 1’000 миллисекунд.

Утилита pathping

Утилита pathping фактически совмещает функциональность утилит ping и tracert и выполняется в две фазы: сначала, подобно tracert, собирается и выводится маршрут до заданного узла (только IP-адреса и имена) и затем, подобно ping, в течение некоторого времени (чем дольше выполнялась трассировка, тем больше будет это время) собирается статистика времен передачи пакетов, количеств и относительных долей потерянных пакетов для каждого из промежуточных маршрутизаторов (а не только для заданного узла, как ping).

Формальный синтаксис: pathping [-g Список] [-h Число_прыжков] [-i Адрес] [-n] [-p Пауза] [-q Число_запросов] [-w Таймаут] [-P] [-R] [-T] [-4] [-6] узел

Наиболее полезен результат работы второй фазы утилиты pathping - он наглядно показывает, на каком из маршрутизаторов имеются проблемы с передачей пакетов. Для Windows существует мощный визуальный (показывает движение пакетов на карте Планеты) трассировщик VisualRoute фирмы VisualWare (http://visualware.com).

Утилита arp

Утилита arp дает возможность просматривать и изменять ARP-таблицу, в которой хранятся пары 'MAC-адрес - IP-адрес' для тех узлов, с которыми в недавнем происходил обмен данными. Эта таблица формируется автоматически при работе сетевого узла, но администратор сети может вносить в нее записи вручную. Формальный синтаксис: arp –s inet_addr eth_addr [if_addr] или ARP –d inet_addr [if_affr] или ARP –a [inet_addr] [-N if_addr]. Здесь if_addr суть задает номер интерфейса.

Параметр '-a' позволяет вывести всю ARP-таблицу на экран.

Параметр '-a <IP-адрес>' запрашивает вывод записи об узле с заданным адресом на экран.

Параметр '-S <IP-адрес> <MAC-адрес>' позволяет добавить запись об узле с заданными адресами в ARP-таблицу.

Параметр '-d <IP-адрес>' служит для удаления записи об узле с заданным

адресом из ARP-таблицы.

Параметр ‘-d *’ очищает ARP-таблицу.

Утилита hostname

Утилита hostname всего-навсего выводит имя узла. Может быть использована в файлах сценариев для пакетной обработки.

Утилита ipconfig

Утилита ipconfig отображает и настраивает настройки протоколов TCP/IP. Без дополнительных параметров выводится IP-адрес, маска подсети и шлюз по умолчанию для всех сетевых интерфейсов. С параметром ‘/all’ кроме сказанного, выводятся MAC-адреса сетевых интерфейсов, имя узла, адреса серверов DNS и WINS и некоторая другая информация. Формальный синтаксис: ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] | /flushdns | displaydns /registerdns | /showclassid адаптер | /setclassid адаптер [устанавливаемый_код_ класса_dhcp]].

Параметр ‘/flushdns’ очищает кэш разрешенных имен DNS.

Параметр ‘/displaydns’ выводит кэш разрешенных имен DNS на экран.

Параметр ‘/release [адаптер]’ освобождает арендованный по DHCP (*Dynamic Host Configuration Protocol*) IP-адрес (если указан адаптер, то только для этого адаптера, иначе для всех адаптеров).

Утилита route

Утилита route отображает таблицу маршрутов и позволяет ее изменять. Формальный синтаксис: route [-f] [-p] [команда [узел]] [MASK маска] [шлюз] [METRIC метрика] [IF-интерфейс]. При использовании route параметр ‘метрика’ определяет качество данного маршрута (в *хопах* – количестве промежуточных маршрутизаторов, времени прохождения пакета по линиям связи, характеристикой надежности линии связи на данном маршруте и т.п.) в соответствие с заданным в сетевом пакете критерием (т.н. *классом сервиса*).

Команда ‘PRINT' выводит таблицу маршрутов: сетевой адрес; маска сети; адрес шлюза; интерфейс; метрика, команда ‘ADD’ позволяет добавить новый маршрут, ‘DELETE’ – удалить маршрут, ‘CHANGE’ – изменить (существующий) маршрут).

Утилита netstat

Утилита netstat отображает текущие соединения, порты, ожидающие соединения и статистические данные по протоколам TCP/IP. Без дополнительных параметров выводится список текущих соединений (протокол: TCP или UDP; локальный адрес и порт; внешний адрес и порт; состояние соединения). Формальный синтаксис: netstat [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]

Параметр ‘-a’ дополнительно отображает порты, ожидающие соединения; ожидающие TCP-порты обозначены состоянием ‘LISTENING’, а UDP-порты - внешним адресом ‘*:*’.

Параметр ‘-n’ требует выводить все адреса и номера портов в числовом формате, поскольку по умолчанию netstat пытается разрешить IP-адреса и имена и заменить номер порта на его имя.

Параметр ‘-r’ выводит таблицу маршрутов (сетевой адрес; маска сети; адрес шлюза; интерфейс; метрика). Подобную информацию можно получить с помощью утилиты route.

Параметр ‘-e’ позволяет получить статистику Ethernet.

Параметр ‘-s’ выводит статистику по протоколам TCP, UDP и IP.

Параметр ‘-e <протокол>’ применяется совместно с параметром ‘-s’ для ограничения выдаваемой статистики заданным протоколом (TCP, UDP или IP).

Утилита net view

Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере. Синтаксис утилиты net view:

net view [\\компьютер | /domain[:домен]]; net view /network:nw [\\компьютер] - используется в сетях Novell NetWare,

где \\компьютер - задает имя компьютера для просмотра общих ресурсов;

/domain[:домен] - задает домен (рабочую группу), для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети;

/network:nw - выводит все доступные серверы в сети Novell NetWare. Если указано имя компьютера, выводится список его ресурсов в сети NetWare. С помощью этого ключа могут быть просмотрены ресурсы и в других локальных сетях.

Вызванная без параметров, утилита выводит список компьютеров в текущем домене (рабочей группе).

Утилита net use

Подключает общие сетевые ресурсы или выводит информацию о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Синтаксис утилиты net use:

net use [устройство | *] [\\компьютер\ресурс[\том]] [пароль | *]] [/user:[домен\]имя пользователя] [[/delete] | [/persistent:{yes | no}]] net use устройство [/home[пароль | *]] [/delete: {yes | no}] net use [/persistent:{yes | no}],

где устройство - задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принтеры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключение к следующему доступному имени устройства;

\\компьютер\ ресурс - указывает имя сервера и общего ресурса. Если параметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" "). Имя компьютера может иметь длину от 1 до 15 символов; \том - задает имя тома системы Novell NetWare.

пароль - задает пароль, необходимый для подключения к общему ресурсу;

* - выводит приглашение для ввода пароля. При вводе с клавиатуры символы пароля не выводятся на экран;

/user - задает другое имя пользователя для подключения к общему ресурсу;

домен - задает имя другого домена. Если домен не указан, используется текущий домен;

имя пользователя - указывает имя пользователя для подключения; /delete - отменяет указанное сетевое подключение. Если подключение задано с символом звездочки, будут отменены все сетевые подключения; /home - подключает пользователя к его основному каталогу; /persistent - управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными;

yes - сохраняет все существующие соединения и восстанавливает их при следующем подключении;

по - не сохраняет выполняемые и последующие подключения. Существующие подключения восстанавливаются при следующем входе в систему. Для удаления постоянных подключений используется ключ /delete. Вызванная без параметров утилита net use извлекает список сетевых подключений.

Пример вызова команды net use:

C:\Documents and Settings\Администратор>net use

ВЫПОЛНИТЬ:

Сделать не менее двух скриншотов с результатами работы для каждой выше рассмотренной утилиты. Для каждой утилиты использовать минимум два параметра, например ‘–a’, ‘- n’.

Оформление отчета по лабораторной работе.

В первой части отчета указать параметры используемой сети (тип ПЭВМ, MAC- и IP-адреса сетевой карты, тип и число портов коммутатора, топология локальной сети).

При использовании утилит ping, tracert или pathping необходимо отметить время передачи пакетов (обычно среднее), число и долю потерянных пакетов (по ней сделать вывод о корректности работы каждого промежуточного маршрутизатора).

Просмотреть список всех сетевых портов на вашем компьютере и сосчитать количество открытых (прослушиваемых);

Определить маршрут до сайта по вариантам, с максимальным числом прыжков.

При использовании утилиты netstat необходимо зафиксировать назначение TCP- и UDP-портов имени ПЭВМ, локальному адресу и их состояние (параметр ‘-a’). Общую статистику обменов можно получить при использовании параметра ‘-e’, с использованием параметра ‘-s’ следует зафиксировать и проанализировать статистику по всем протоколам стека TCP/IP (включая ICMP, UDP).

При использовании утилиты route (с параметром PRINT для вывода на экран) просматривается как список интерфейсов, так и список активных маршрутов.

Контрольные вопросы:

1. Из каких соображений назначаются IP-адреса сетевым платам, если для входящих в локальную сеть компьютеров не предполагается доступ к InterNet? Если работа в InterNet предполагается?
2. Какие этапы предполагает настройка стека протоколов TCP/IP?
3. С какой целью применяется ‘маска подсети’? Что такое ‘основной шлюз’?
4. Какой формат имени сетевого ресурса используется при обращении к нему?
5. Каким путем утилиты ping, tracert и pathping осуществляют прослеживание маршрутов пакетов к заданному узлу?
6. В каких случаях и с какой целью используется утилита route? Что такое ‘метрика’ в списке параметров этой утилиты?
7. Какой протокол необходим для работы с утилитой ping? Найти описание и характеристики протокола.
8. Можно ли утилитой tracert задать максимальное число ретрансляций?
9. Какой результат выдаст утилита netstat с параметрами -a -s -r? Поясните полученный результат.
10. Что такое DNS –сервер, какую информацию он хранит, его назначение?
11. В чем отличие IP –адреса от MAC – адреса?
12. Назначение устройств роутеров, маршрутизаторов?