МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
КАСПИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И ИНЖИНИРИНГА ИМ.Ш.ЕСЕНОВА

ИНСТИТУТ МОРСКИХ ТЕХНОЛОГИИ

Кафедра «Вычислительная техника и программное обеспечение»

Шахимова Ы.А., Бобыр Ю.С.

КОМПЬЮТЕРНЫЕ СЕТИ

**Методические указания по выполнению лабораторных работ
для студентов специальностей
«Информационные системы»
«Вычислительная техника и программное обеспечение»**

Актау 2011г.

УДК 681.327(076)

Составители: Шахимова Ы.А., Бобыр Ю.С. – Компьютерные сети. Методические указания по выполнению лабораторных работ для студентов специальностей: «Информационные системы» «Вычислительная техника и программное обеспечение» - Актау: КГУТиИ, 2011г., -48 стр.

Рецензент: к.т.н. Кабылбекова В.В.

В методических указаниях представлены краткие теоретические материалы по прокладке и настройке локальных сетей, работе в локальных и глобальных сетях; приводятся примеры, задания и контрольные вопросы к каждой работе по основным разделам курса дисциплины. В данной разработке широко освещены вопросы построения компьютерных сетей; приведены виды топологии, используемые для физического соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных.

Методические указания по выполнению лабораторных работ предназначены для студентов специальностей: «Информационные системы» и «Вычислительная техника и программное обеспечение».

Печатается по решению учебно–методического совета Каспийского государственного университета технологий и инжиниринга им.Ш.Е. Есенова

Введение

Компьютерная сеть позволяет работать с многопользовательскими программами, обеспечивающими одновременный доступ всех пользователей к общим базам данных с блокировкой файлов и записей, обеспечивающей целостность данных. Любые программы, разработанные для стандартных ЛВС, можно использовать в других сетях.
Совместное использование ресурсов обеспечит существенную экономию средств и времени. Например, можно коллективно использовать один лазерный принтер вместо покупки принтера каждому сотруднику или беготни с дискетами к единственному принтеру при отсутствии сети.
Организация электронной почты. Можно использовать *ЛВС* как почтовую службу и рассылать служебные записки, доклады и сообщения другим пользователям.

Методические указания для выполнения лабораторных работ по дисциплине «Компьютерные сети» представляют собой введение в сетевую тематику и дают базовые знания по организации и функционированию сетей. Даны общие понятия компьютерных сетей, их структуры, сетевых компонентов в простой и доступной форме. Здесь приведены виды топологии, используемые для физического соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных. Передача данных в сети рассматривается на базе эталонной базовой модели, разработанной Международной организацией по стандартам взаимодействия открытых сетей. Описываются правила и процедуры передачи данных между информационными системами. Приводятся типы сетевого оборудования, их назначение и принципы работы. Описывается сетевое программное обеспечение, используемое для организации сетей. Рассматриваются принципы межсетевого взаимодействия. Приводятся основные понятия из области сетевой безопасности.

Лабораторная работа №1

Тема: Сетевые возможности ОС Windows

Цель работы: Изучение способов поддержки сети, технологии обмена данными в сети; организация доступа к файлам и папкам, создание сетевых дисков, формулировка правил поведения в сети.

Теоретические сведения:

Поддержка сети в windows

windows 2000

Windows 2000 представляет собой полнофункциональную сетевую операционную систему на базе технологии windows NT. Компьютер, оснащенный операционной системой windows 2000 может выступать не только в роли клиента, но и сервера сети, т.е. являться поставщиком сетевых услуг. windows 2000 объединяет и расширяет возможности windows 9x и windows NT.

Компоненты сети на базе Windows

Рабочая группа - совокупность компьютеров, имеющих схожие права доступа или другие отличительные признаки. Рабочие группы используются для построения более четкой организации сети.

Права (уровни) доступа - совокупность правил, определяющая возможности клиента сети при использовании ресурсов сети.

Сетевой ресурс представляет собой некоторое устройство, подключенное к сети (компьютер, принтер), либо данные.

Каждый компьютер подключенный к сети на базе Windows должен иметь сетевое имя, уникальное в пределах сети и должен входить в некоторую рабочую группу.

Папка "Сетевое окружение"

Папка "Сетевое окружение" предназначена для организации работы в сети. Обычно на рабочем столе Windows находится значок "Сетевое окружение", позволяющий открыть папку "Сетевое окружение"

По умолчанию папка "Сетевое окружение " отображает информацию о "своей" рабочей группе. Ярлык "Вся сеть" предназначен для доступа к другим рабочим группам.

Свойства папки "Сетевое окружение" позволяют настроить компьютер для работы в сети. Окно свойств имеет три страницы.

Страница "Конфигурация" содержит сведения об установленных сетевых адаптерах, протоколах и типе сети (Клиент для сетей Microsoft).

Для установки нового сетевого протокола или клиента нажмите кнопку "Добавить". Для управления доступом к файлам и принтерам нажмите кнопку "Доступ к файлам и принтерам". Для определения способа входа в сеть используйте переключатель "Способ входа в сеть".

Страница "Идентификация" содержит сведения о сетевом имени компьютера, рабочей группе и необязательный параметр "Описание компьютера".

Страница "Управление доступом" позволяет определить как пользователи сети могут использовать ресурсы данного компьютера.

Модель доступа "На уровне ресурсов" позволяет устанавливать доступ к файлам и папкам всем пользователям сети.

Модель доступа "На уровне пользователей" позволяет устанавливать доступ к файлам и папкам определенным пользователям сети.

Обмен данными в сети. Доступ к файлам и папкам

Работа с файлами в сети для пользователя практически не отличается от работы с файлами на локальном компьютере. Основное отличие состоит в том, что доступ к данным сетевого компьютера определяется пользователем этого компьютера, который назначает возможность доступа к отдельным файлам и папкам.

Ресурс, к которому определен доступ называется **общим.**

Если вызвать контекстное меню (правый щелчок мыши) для любой папки, то среди пунктов меню будет присутствовать пункт "Доступ", с помощью которого можно управлять разрешением сетевого доступа к этой папке.

Общий вид окна доступа:
Переключатель "*Локальный ресурс*" - запрещает сетевой доступ к папке.
Переключатель "*Общий ресурс*" позволяет назначить параметры доступа к папке.
Поле *"Сетевое имя"* определяет сетевое имя папки.
Поле "*Заметки*" - определяет описание папки.
Группа переключателей "*Тип доступа*" определяет как будет осуществляется сетевой доступ к папке.
Только чтение - возможно только чтение данных.
Полный доступ - возможно чтение и изменение данных.
Определяется паролем - для каждого из типов доступа определяется отдельный пароль.
Область "*Пароли*" позволяет назначить пароль для получения сетевого доступа.

Создание сетевых дисков

Операционная система Windows предоставляет возможность пользователю работать с некоторой сетевой папкой, к которой назначен доступ, как с дисковым устройством. Логический диск, полученный в результате такого подключения, называют *сетевым диском*.

Сетевой диск может быть назначен для любой папки.

Для создания сетевого диска вызовите контекстное меню папки "Сетевое окружение" и выберите пункт "Подключить сетевой диск", появится диалоговое окно "Подключение сетевого диска".

Поле "*Диск*" позволяет назначить букву для сетевого диска.

Поле "*Путь*" позволяет указать имя сетевого ресурса для подключения в качестве сетевого диска. Если переключатель "*Автоматически подключать при входе в систему*" выключен, то диск будет подключаться по команде пользователя, если же он включен, то диск будет подключаться автоматически.

После того как вы установили необходимые параметры для подключения сетевого диска, подтвердите свое решение нажатием кнопки "ОК".
Если не возникло проблем при подключении к сетевому ресурсу, то откроется окно той сетевой папки, для которой назначался сетевой диск.

Для просмотра содержимого сетевого диска можно использовать окно "Мой компьютер" и работать с ним как с обычным дисковым устройством.

Чтобы отключить сетевой диск откройте его контекстное меню и выберите пункт "Отключить".

Задания

1. Назначьте сетевой доступ к своей рабочей папке.
2. Найдите на компьютере 308-01, рабочей группы VTiPO папку Public и скопируйте в свою рабочую папку файл example.doc
3. Создайте в любом текстовом редакторе файл, описывающий правила поведения в сети и перешлите его соседу.
4. Подключите сетевой диск для любой общей папки в вашей рабочей группе.
5. Отключите этот сетевой диск.

Контрольные вопросы:

1. Для чего используются рабочие группы? Напишите определение термина.
2. Что такое «Права доступа»? Кто их устанавливает?
3. Что представляют собой сетевые ресурсы?
4. Где находится папка Сетевое окружение и для чего она используется?
5. Как можно получить сведения о б установленных сетевых адаптерах, протоколах и типе сети?
6. Как можно узнать сетевое имя компьютера?
7. Что означает модель доступа «на уровне ресурсов»? Какая модель существует еще и в чем разница между ними?
8. Как организовать доступ других машин к своим файлам и папкам?
9. Способ создания сетевого диска.

10. Основные правила поведения в сети.

Литература:

Осн. 1[248-270], 2[158-163]
Доп.3[69-90]

Лабораторная работа № 2.
Тема: Структуры и характеристики локальной сети

Цель работы: Исследование структуры и характеристик локальной сети

Теоретические сведения:

Протоколы, клиенты и серверы.

Протокол — это соглашение о порядке взаимодействия двух или более сторон. Обычно различают два типа взаимодействующих сторон: клиенты и серверы.

Можно считать, что сервер протокола — это постоянно работающая программа, ожидающая подключения клиентов и обрабатывающая их запросы. Клиент протокола — это программа, которая на основе пользовательского ввода формирует и отправляет на сервер запрос, а затем информирует пользователя о его результатах. Часто клиентом и сервером называют и сами компьютеры, на которых работают эти программы. Протокол должен определять формат сообщений, передаваемых по сети в каждом направлении, и последовательность появления этих сообщений. Конечный пользователь для своих целей обычно использует клиенты прикладных протоколов. Например, для отправки почты можно применять специальные почтовые программы, реализующие протокол SMTP (Simple Mail Transport Protocol), а для посещения веб-сайтов — браузеры, реализующие протокол HTTP (Hyper Text Transfer Protocol).

Подключение к удаленному серверу по протоколу SSH.

Важным примером протокола является протокол SSH (Secure SHell). Он предназначен для организации удаленного доступа пользователей к серверу (специальному компьютеру, на котором эти пользователи зарегистрированы).

Удаленный доступ позволяет выполнять команды операционной системы и запускать программы. При таком подключении команды, вводимые пользователем, передаются на удаленный сервер, выполняются там, а их результаты возвращаются пользователю. Это взаимодействие обычно происходит в консольном режиме, т.е. и команды, и их результаты - это текстовые строки, передающиеся по сети. Для подключения к серверу по протоколу SSH пользователь может воспользоваться любой программой, реализующей клиентскую часть протокола SSH, например, программой Putty (/IVTHOST/netlogon/pub/soft/putty), которую необходимо скопировать на локальный компьютер. При ее запуске следует указать имя сервера (Host Name), к которому необходимо подключиться, и выбрать протокол доступа (SSH), после чего нажать кнопку "Open". В этот момент клиент попытается подключиться к серверу, и если все пройдет успешно, то будет предложено ввести имя пользователя (логин) и пароль.

Подготовка компьютера к выполнению работы

1. На рабочем столе щелкнуть "Мое сетевое окружение", далее в одноименном окне активизировать строку "Сеть и удаленный доступ к сети".
2. В открывшемся окне Сеть и удаленный доступ к сети вызвать контекстное меню "Подключение по локальной сети" и выбрать пункт меню "Свойства". В окне "Подключение по локальной сети - свойства" убедиться в наличии следующих компонентов:
   - Драйвер сетевого адаптера.
   - Клиент для сетей Microsoft.
   - Протокол TCP/IP
   - Служба доступа к файлам и принтерам сети Microsoft.
3. Для проверки состояния сетевого адаптера нажмите "Настроить" и в окне свойств адаптера убедитесь, что устройство работает нормально.

Задания

1. Просмотр и поиск ресурсов в одноранговой сети Microsoft.

a) На рабочем столе откройте значок *Мое сетевое окружение* и через значок *Вся сеть* наблюдайте рабочие группы, домены и отдельные компьютеры в них. В сетевом окружении значки-триады компьютеров отображают рабочую группу или домен сети Microsoft.

b) По указанию преподавателя найдите заданный компьютер сети. Для поиска компьютера в сети выполните *Пуск*|*Найти*|*Файлы и папки*|*Компьютеры* или на рабочем столе щелкните правой кнопкой мыши на значке *Сетевое окружение* и выберите пункт *Поиск компьютеров*. В поле *Имя компьютера* введите его имя (без слэшей) и щелкните по *Найти*.

c) Если компьютер найден, то откроется список в правой части окна, где в столбце Имя будет стоять имя компьютера, а в столбце Размещение будет указано имя домена или имя рабочей группы (для компьютера, включенного в рабочую группу).

d) Выделите запись с найденным компьютером и выполните *Файл*|*Открыть*. Возможность обозрения и доступа к сетевым папкам будет предоставлена:

- для рабочих станций под Windows NT/2000 - когда найденный компьютер содержит вашу локальную учетную запись или входит в домен, где у вас есть учетная запись. В противном случае потребуется ввод корректных имени пользователя и сетевого пароля.
- для рабочих станций под Windows 98/ME - когда найденный компьютер входит в рабочую группу и объявил доступ на уровне ресурсов.

e) Другая возможность подключения к компьютеру сети предлагается командой *Пуск*|*Выполнить*, где следует ввести имя компьютера в сети (со слэшами). Далее можно просмотреть доступные ресурсы сервера или, нажав BackSpace, перейти в просмотр рабочей группы (домена) сервера.

f) Проверьте возможность доступа к вашему компьютеру или к компьютерам партнеров через сетевое окружение. Почему ресурсы этих компьютеров могут недоступны?

2. Объявление и защита общих ресурсов рабочей станции в сети Microsoft

a) В окне Проводника откройте папку D:\PUBLIC, а в ней создайте папки с именами **READ**, **FULL**, **CHANGE**, **BAN**, **HIDE**, **DOCS** для предоставления им различного сетевого доступа.

b) Щелкните по папке **READ** правой кнопкой и в контекстном меню выберите команду *Доступ*. Установите переключатель *Открыть общий доступ к этой папке*, затем: *Предельное число пользователей: максимально возможное*. Нажмите кнопку *Разрешения*. В окне *Разрешения* для **READ** для группы *Все* установите в группе *Разрешить* только флажок *Чтение*. Нажмите ОК. Обратите внимание, что при объявлении ресурса разделяемым его значок будет представлен иначе - с рукой, удерживающей папку снизу.

c) Щелкните по папке **FULL** правой кнопкой и в контекстном меню выберите команду *Доступ*. Аналогично папке **READ** войдите в окно *Разрешения* для **FULL**. Для группы *Все* установите в группе *Разрешить* флажок *Полный доступ*. Нажмите ОК.

d) Щелкните по папке **CHANGE** правой кнопкой и в контекстном меню выберите команду *Доступ*. Аналогично папкам **READ** и **FULL** войдите в окно *Разрешения* для **CHANGE**. Для группы *Все* установите в группе *Разрешить* флажки *Изменение* и *Чтение*. Нажмите ОК.

e) Щелкните по папке **BAN** правой кнопкой и в контекстном меню выберите команду *Доступ*. Установите переключатель *Открыть общий доступ к этой папке*, затем введите сетевое имя *SECRET* для данной папки. Аналогично предыдущему войдите в окно *Разрешения* для **BAN**. Для группы *Все* снимите все флажки в столбце *Разрешить*. Нажмите ОК.

f) Щелкните по папке **HIDE** правой кнопкой и в контекстном меню выберите команду *Доступ*. Установите переключатель *Открыть общий доступ к этой папке*, затем введите сетевое имя **HIDE$** для данной папки. Аналогично предыдущему войдите в окно *Разрешения* для **HIDE**. В окне *Разрешения* для **HIDE** для группы *Все* установите в группе *Разрешить* только флажок *Чтение*. Нажмите ОК.

g) Создайте или скопируйте в папки с именами **READ**, **FULL**, **CHANGE**, **BAN** и **HIDE** по одному текстовому файлу, а в папку READ также файл C:\WINNT\system32\CALC.EXE.

h) Не объявляйте общий доступ к папкам PUBLIC и DOCS.

3. Доступ к защищенным ресурсам одноранговой сети

a) Откройте сетевое окружение и значок *Соседние компьютеры*. Убедитесь в возможности обзора компьютеров вашей рабочей группы.

b) Когда сосед по сети завершит для вас все необходимые назначения, попытайтесь открыть значок его компьютера. При каких условиях появится окно *Ввод сетевого пароля*?

c) При этом на соседнем компьютере вы должны увидеть ресурсы партнера, объявленные общими, то есть папки READ, CHANGE, FULL и SECRET.

d) Проверьте права доступа к общим папкам партнера. Для этого откройте папку READ двойным щелчком и проверьте операции, разрешенные правом READ:

- просмотреть оглавление (содержимое) папки;
- открыть файл для просмотра текста;
- стартовать исполняемый файл;
- скопировать файл на свой компьютер.

Проверьте операции, не разрешенные правом READ:

- удалить файл в папке;
- добавить файл в папку;
- изменить содержимое файла;
- переименовать файл или изменить его атрибуты.

e) Проверьте права доступа к общей папке CHANGE. Для этого откройте ее двойным щелчком и проверьте операции, разрешенные правом CHANGE. Выполняться должны все операции, перечисленные в п.3.d, в том числе не разрешенные READ.

f) Проверьте права доступа к общей папке FULL. Для этого откройте ее двойным щелчком и проверьте операции, разрешенные правом FULL. Выполняться должны все операции, перечисленные в п.3.d.

g) Проверьте права доступа к общей папке SECRET. Убедитесь в том, что для этой папки запрещен сетевой доступ.

h) Обратите внимание на то, что общая папка HIDE не видна на компьютере партнера. Почему?

i) Введите в адресной строке проводника путь для доступа к скрытой общей папке \\NNN\HIDE$ где NNN - компьютер партнера, и нажмите Enter. Проверьте права доступа к общей папке HIDE.

j) Закройте сетевые папки и окно сетевого окружения.

k) Сетевые подключения и сетевые диски. В справочной системе найдите информацию о создании и подключении сетевого диска. Опишите процесс создания сетевого диска.

l) Паспорт сети. Создайте паспорт компьютерного класса, содержащий:

- № компьютерного класса;
- вид топологии сети;
- связь с другими сегментами сети;
- размеры помещения;
- схема расположения компьютеров;
- схема сетевого подключения;
- расчет оптимальной длины сетевого кабеля и местоположения концентратора, для соединения компьютеров при данном расположении;
- выводы и рекомендации.

Контрольные вопросы:

1. Что такое архитектура сети?
2. Как назвать способ определения, какая из рабочих станций сможет следующей использовать канал связи?
3. Перечислить преимущества использования сетей.
4. Чем отличается одноранговая архитектура от клиент серверной архитектуры?

Литература:

Осн. 1[271-276], 2[164-172]

Лабораторная работа № 3.

Тема: Основные сетевые устройства и их параметры

Цель работы: Изучить основные сетевые устройства и их параметры.

Теоретические сведения

Физическая структуризация локальной сети

Различают топологию физических связей (физическую структуру сети) и топологию логических связей сети (логическую структуру сети).

Конфигурация **физических связей** определяется электрическими соединениями компьютеров и может быть представлена в виде графа, узлами которого являются компьютеры и коммуникационное оборудование, а ребра соответствуют отрезкам кабеля, связывающим пары узлов.

Логические связи представляют собой пути прохождения информационных потоков по сети; они образуются путем соответствующей настройки коммуникационного оборудования.

В некоторых случаях физическая и логическая топологии сети совпадают. Например, сеть, представленная на Рис.3.1, а, имеет физическую кольцевую топологию. Пусть компьютеры этой сети используют метод детерминированного доступа. Причем сигнал всегда передается последовательно от компьютера к компьютеру в том же порядке, в котором компьютеры образуют физическое кольцо: то есть компьютер А передает сигнал компьютеру В, компьютер В -- компьютеру С и т.д. В этом случае логическая топология сети также является кольцом.

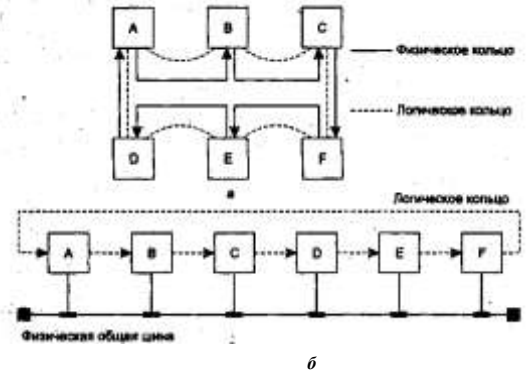


Рисунок 3.1. Логическая и физическая топологии сети

Сеть, показанная на Рис.3.1., б, являет собой пример несовпадения физической и логической топологий. Физически компьютеры соединены по топологии общая шина (звезда). Доступ же к шине происходит не по алгоритму случайного доступа, а путем передачи сигнала в кольцевом порядке: от компьютера А -- компьютеру В, от компьютера В -- компьютеру С и т. д. Здесь порядок передачи сигнала, уже не повторяет физические связи, а определяется логическим конфигурированием драйверов сетевых адаптеров. Ничто не мешает настроить сетевые адаптеры и их драйверы так, чтобы компьютеры образовали кольцо в другом порядке, например: В, А, С... При этом физическая структура сети никак не меняется.

Физическая структуризация единой разделяемой среды была первым шагом на пути построения более качественных локальных сетей. Цель физической структуризации -- обеспечить построение сети не из одного, а из нескольких физических отрезков кабеля. Причем эти различные в физическом отношении отрезки должны были по-прежнему работать как единая разделяемая среда.

Основными средствами физической структуризации локальных сетей являются **повторители** (repeater) и **концентраторы** (concentrator) или **хабы** (hub).

Повторитель

Простейшее из коммуникационных устройств -- повторитель -- используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. Повторитель повторяет сигналы, приходящие из ``одного сегмента сети в другие ее сегменты (Рис.3.2.), улучшая их физические характеристики -- мощность и форму сигналов, а также синхронность следования (исправляет неравномерность интервалов между импульсами). За счет этого повторитель позволяет преодолеть ограничения на длину линий

связи. Так как поток сигналов, передаваемых узлом в сеть, распространяется по всем отрезкам сети, такая сеть остается сетью с единой разделяемой средой.

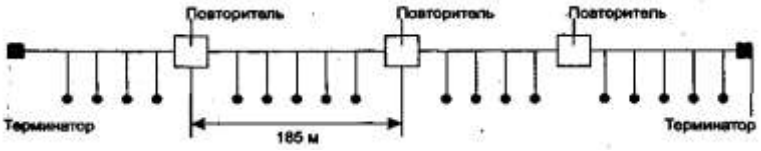


Рисунок 3.2. Повторители позволяют увеличить длину сети

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов, часто называют концентратором, или хабом. Эти названия отражают тот факт, что в данном устройстве сосредоточиваются все связи между сегментами сети.

Добавление в сеть повторителя всегда изменяет ее физическую топологию, но при этом оставляет без изменения логическую топологию.

Концентраторы

- являются необходимыми устройствами практически во всех базовых технологиях локальных сетей -- Ethernet, ArcNet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100 VG-Any LAN1. В работе концентраторов любых технологий много общего -- они повторяют сигналы, пришедшие с одного из своих портов, на других своих портах. Разница состоит в том, на каких именно портах повторяются входные сигналы. Так, концентратор Ethernet повторяет входной сигнал на всех своих портах, кроме того, с которого этот сигнал поступил (Рис 3.). А концентратор Token Ring (Рис. 3.3, б) повторяет входной сигнал только на одном, соседнем порту.

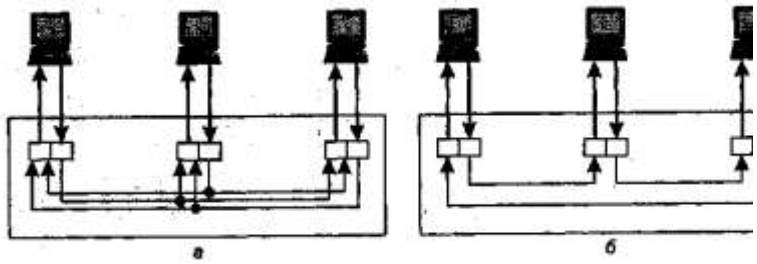


Рисунок 3.3. Концентраторы различных технологий

Логическая структуризация сети на разделяемой среде

Физическая структуризация сети не позволяет справиться с такими важными проблемами, как дефицит пропускной способности, невозможность использования в разных частях сети линий связи разной пропускной способности. В таком случае может помочь логическая структуризация сети.

Типовые физические топологии сети (шина, кольцо, звезда), которые ограничивают все сетевые устройства, предоставляя им для обмена данными только одну разделяемую среду, оказываются неадекватными структуре информационных потоков в большой сети. Например, в сети с общей шиной взаимодействие любой пары компьютеров занимает ее на все время обмена, поэтому при увеличении числа компьютеров в сети шина становится узким местом.

Распространение трафика, предназначенного для компьютеров некоторого сегмента сети, только в пределах этого сегмента называется **локализацией трафика. Логическая структуризация сети** - это процесс разбиения сети на сегменты с локализованным трафиком.

При правильно проведенной логической структуризации производительность сети может существенно повыситься, так как компьютеры одного отдела не будут простаивать в то время, когда обмениваются данными компьютеры других отделов. Кроме того, логическая структуризация позволяет дифференцировать доступную пропускную способность в разных частях сети.

Логическая структуризация сети проводится путем использования мостов, коммутаторов, маршрутизаторов и шлюзов.

Мост (bridge)

делит единую среду передачи на части (часто называемые **логическими сегментами**), передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если адрес компьютера назначения принадлежит другому сегменту (Рис. 3.3.). Тем самым мост изолирует трафик одного сегмента от трафика другого, повышая общую производительность сети. Локализация трафика не только экономит пропускную способность, но и снижает возможность несанкционированного доступа к данным, так как кадры не выходят за пределы своего сегмента и их сложнее перехватить злоумышленнику.

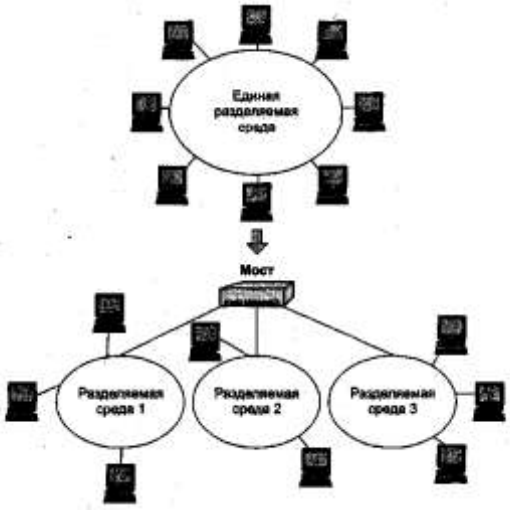


Рисунок 3.4. Мост делит единую среду передачи

Мосты используют для локализации трафика аппаратные адреса компьютеров. Все кадры, приходящие на определенный интерфейс моста, сгенерированы компьютерами, относящимися к сегменту, подключенному к этому интерфейсу. Мост извлекает из поступающих кадров адреса отправителей и помещает их в таблицу, где делает отметку о том, на какой его интерфейс поступил каждый из кадров. Так мост определяет, какие компьютеры подключены к каждому из его интерфейсов. В дальнейшем мост использует эту информацию для передачи кадра именно на тот интерфейс, через который идет путь к компьютеру назначения. Поскольку, точная топология связей между логическими сегментами мосту неизвестна, он может правильно работать только в тех сетях, в которых межсегментные связи не образуют замкнутых контуров (петель).

Коммутатор (switch)

Функционально подобен мосту и отличается от моста в основном более высокой производительностью. Каждый интерфейс коммутатора оснащен специализированным процессором, который обрабатывает кадры по алгоритму моста независимо от процессоров других портов. За счет этого общая производительность коммутатора обычно намного выше производительности традиционного моста, имеющего один процессорный блок. Можно сказать, что коммутаторы - это усовершенствованные мосты, которые обрабатывают кадры в параллельном режиме. Когда стало экономически оправданно использовать отдельные специализированные процессоры на каждом порту коммуникационного устройства, коммутаторы локальных сетей полностью вытеснили мосты.

Маршрутизатор

Ограничения, связанные с применением мостов и коммутаторов, - по топологии связей, а также ряд других, - привели к тому, что в перечне коммуникационных устройств появилось еще одно устройство - **маршрутизатор** (router). Маршрутизаторы более надежно и более эффективно, чем мосты, изолируют трафик отдельных частей сети друг от друга. Помимо локализации трафика маршрутизаторы выполняют еще много других полезных функций. Так, маршрутизаторы могут работать в сети с замкнутыми контурами, при этом они обеспечивают выбор наиболее рациональных маршрутов. Другой важной функцией маршрутизаторов

является их способность связывать в единую сеть сети, построенные на базе разных сетевых технологий, например Ethernet и ATM.

Помимо перечисленных устройств отдельные части сети может соединять шлюз (gateway). Шлюз позволяет объединять сети, построенные на существенно разных программных и аппаратных платформах. Например, шлюз может позволить пользователям, работающим в сети Unix, взаимодействовать с пользователями сети Windows. Традиционно в Интернете термины ``шлюз'' и ``маршрутизатор'' используются как синонимы.

Задания:

1. Изучите виды модемов и их основные характеристики.
2. Изучите сетевые карты и их основные характеристики.
3. Изучите сетевые кабели и их основные характеристики.
4. Определите параметры сетевой карты, установленной на рабочем ПК.
5. Выполните обжим сетевого кабеля, под руководством преподавателя, согласно цветовой раскладке.

Контрольные вопросы:

5. Что такое Маршрутизатор?
6. Для чего используется мост?
7. Перечислить преимущества коммутаторов.
8. Чем отличается концентраторы от повторителей?

Литература:

Осн. 1[248-270], 2[158-163]

Доп. 3[69-90]

Лабораторная работа № 4

Тема: Соединение компьютеров при помощи cross-over кабеля в сеть.

Цель работы: Приобретение знаний и практических навыков, необходимых для соединения компьютеров посредством cross-over кабеля в сеть на базе операционной системы MS Windows 2000/XP.

Ход работы:

При необходимости соединения пары компьютеров через сетевые интерфейсы понадобятся установленные и настроенные сетевые карты в обоих компьютерах, сетевой кабель UTP/FTP/STP/SFTP 4pair (рис. 4.1), из которого необходимо сделать кроссовер (cross-over) кабель, два коннектора RJ-45 (рис. 4.2) для оконцовки (обжимки) кабеля и обжимной инструмент (рис. 4.3).

Используется обычный кабель («витая пара») для локальных сетей UTP/FTP/STP/SFTP имеющий 4 пары. Необходимо определить, сколько кабеля требуется для соединения 2-х компьютеров, учитывая, что длина не может превышать 90м и быть не менее 1,5м.

Рисунок 4.1. Тип кабеля «витая пара»

Рисунок 4.2. Коннектор RJ-45

Рисунок. 4.3. Обжимной инструмент

Кабель обжимается с двух сторон разъемами RJ-45, по типу Cross-over. Cross-over ("нуль хабный") - используется для соединения двух компьютеров через сетевые карты напрямую, т.е. не используя активное сетевое оборудование (концентратор-hub, коммутатор-switch). Таким образом, возможно подключить только два компьютера одновременно. Для подключения трех и более компьютеров потребуется дополнительное сетевое оборудование.

При подключении трех и более компьютеров через концентратор или коммутатор используется кабель типа Straight-through (прямо проходящий). Название этого вида кабеля говорит само за себя - он передаёт сигнал напрямую из одного конца в другой, а именно с 1-го контакта на 1, 2-2, 3-3 и т.д. Используется для различных видов соединений (компьютер - концентратор, компьютер - ADSL/ISDN/кабельный модем, или соединения концентратор и коммутатор между собой).

При обжимке проводников воспользуемся стандартом TIA/EIA-568B, т.е. с одной стороны проводники должны быть расположены в следующем порядке (рис 4.4):

1 БЕЛО-ОРАНЖЕВЫЙ
2 ОРАНЖЕВЫЙ
3 БЕЛО-ЗЕЛЕНЫЙ
4 СИНИЙ
5 БЕЛО-СИНИЙ
6 ЗЕЛЕНЫЙ
7 БЕЛО-КОРИЧНЕВЫЙ
8 КОРИЧНЕВЫЙ

Рисунок 4.4. Порядок расположения проводников по стандарту TIA/EIA-568B

С другой стороны проводники должны быть расположены в другом порядке:

1 БЕЛО-ЗЕЛЕНЫЙ
2 ЗЕЛЕНЫЙ
3 БЕЛО-ОРАНЖЕВЫЙ
4 СИНИЙ
5 БЕЛО-СИНИЙ
6 ОРАНЖЕВЫЙ
7 БЕЛО-КОРИЧНЕВЫЙ
8 КОРИЧНЕВЫЙ

Включаем полученный кабель в сетевые карты компьютеров и приступаем к настройке операционной системы. В "Панель управления" выбираем ярлык "Сетевые подключения" и в появившемся окне находим ярлык "Подключение по локальной сети", запускаем его и устанавливаем следующие параметры:

На закладке "Общие" в списке "Отмеченные компоненты используются этим подключением" выбираем "Internet Protocol (TCP/IP)" и нажимаем кнопку "Свойства".

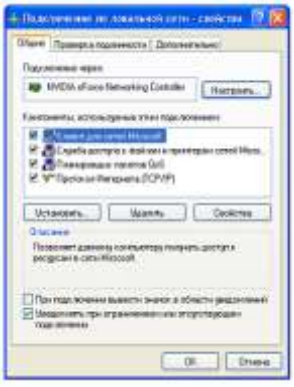


Рисунок 4.5. Закладка «Общие» закладки "Отмеченные компоненты используются этим подключением"

В появившемся окне свойств TCP/IP выбираем "Использовать следующий IP адрес"

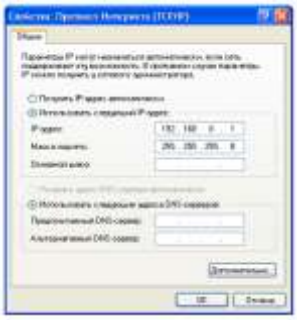


Рисунок 4.6. Закладка протоколы интернета

Для локальных сетей класса С отведен диапазон IP-адрессов 192.168.x.x (x=0-255). По этой причине рекомендуется использовать именно их. На одном компьютере указывается адрес 192.168.0.1, а на другом адрес 192.168.0.2 . Очень важно, что бы IP адреса отличались друг от друга последней цифрой. Маска подсети может быть указана 255.255.255.0, она устанавливается обязательно одинаковой на все компьютеры локальной сети. Теперь необходимо настроить рабочую группу, а также ввести имя компьютера для представления в сети. Для этого нажимаем правой кнопкой мыши на иконке "Мой компьютер" и выбираем пункт "Свойства". В появившемся окне переходим на закладку "Имя компьютера" и нажимаем кнопку "Изменить".В поле "Имя компьютера" вписываем имя, которым компьютер будет представляться в сети. Используйте английские буквы, цифры. Старайтесь не использовать другие символы, так как при этом возможны проблемы в работе сети.

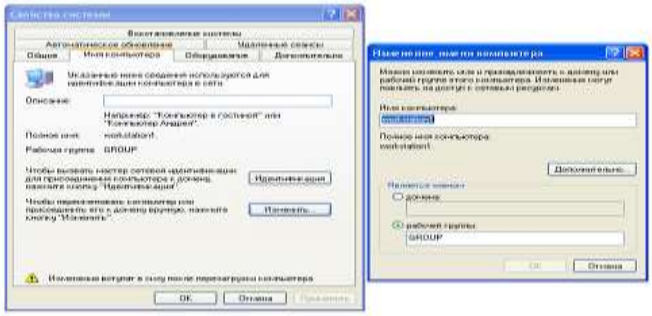


Рисунок 4.7. "Мой компьютер" пункт "Свойства".

Соединение уже настроено, теперь осталось сделать несколько открытых ресурсов ("расшарить" от английского слова "share"- делиться, разделять). Для этого выбираем папку, которую хотим открыть для доступа другому компьютеру, и нажимаем на ней правой кнопкой мыши. В появившемся меню выбираем пункт "Общий доступ и безопастность..." тем самым вы открываете окно свойств данной папки на закладке "Доступ". В появившемся окне поставьте галочку напротив "Открыть общий доступ к этой папке" и укажите имя общего ресурса, которое будет видно в сети для доступа. Имя, которое вы дадите папке для представления в сети, может быть любым и необязательно должно совпадать с именем папки.Если вы хотите что бы пользователи сети могли записывать или изменять файлы в вашей папке, установите так же галочку напротив "Разрешить изменение файлов по сети".

Задания

Попрактиковаться в получении практических навыков, необходимых для программно-аппаратного объединения компьютеров посредством cross-over кабеля в сеть.

Контрольные вопросы:

9. Что такое cross-over кабель?
10. Как осуществляется настройка операционной системы?
11. Порядок установки доступа к папке?
12. Какой кабель используется при подключении к концентратору?

Литература:

Осн. 1[273-287], 2[166-174]

Лабораторная работа № 5

Тема: Построение локальной вычислительной сети (ЛВС) по сетевой технологии Fast Ethernet (100 Base TX). Организация доступа к сети Internet по технологии Internet Connection Sharing (ICS).

Цель работы: Приобретение знаний и практические навыков, необходимых для соединения компьютеров по технологии Fast Ethernet (100 Base TX) в сеть на базе операционной системы MS Windows 2000/XP. А также организовать доступ к сети Internet.

Теоретические сведения:

Сетевая технология - это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств (например, сетевых адаптеров, драйверов, кабелей и разъемов), достаточный для построения вычислительной сети.

Протоколы, на основе которых строится сеть определенной технологии, специально разрабатывались для совместной работы, поэтому от разработчика сети не требуется дополнительных усилий по организации их взаимодействия.

При необходимости соединения N компьютеров (двух и более) нам понадобятся установленные и настроенные во всех компьютерах сетевые карты необходимой технологии, сетевой кабель UTP/FTP/STP/SFTP 5e 4pair, из которого необходимо сделать N прямо проходящих (Straight-through) кабелей, N*2 коннекторов RJ-45 для оконцовки (обжимки) кабеля и обжимной инструмент. В роли активного сетевого оборудования выступит концентратор или коммутатор, имеющей N портов. Технология Fast Ethernet предполагает объединение компьютеров в сеть посредством сетевого оборудования. В роли активного сетевого оборудования выступит концентратор или коммутатор, имеющей N портов (рис.5.1).

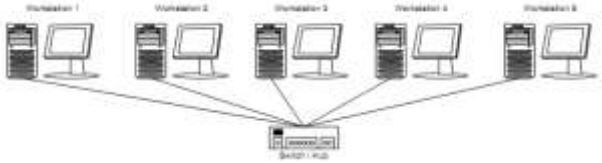


Рисунок 5.1. Объединение компьютеров в сеть посредством сетевого оборудования

При обжимке проводников воспользуемся стандартом TIA/EIA-568B.

Один конец полученного кабеля включаем в сетевые карты компьютеров, а другой в порт сетевого оборудования и приступаем к настройке операционной системы. В "Панель управления" выбираем ярлык "Сетевые подключения" и в появившемся окне находим ярлык "Подключение по локальной сети", запускаем его и устанавливаем следующие параметры:

На закладке "Общие" в списке "Отмеченные компоненты используются этим подключением:" выбираем "Internet Protocol (TCP/IP)" и нажимаем кнопку "Свойства".

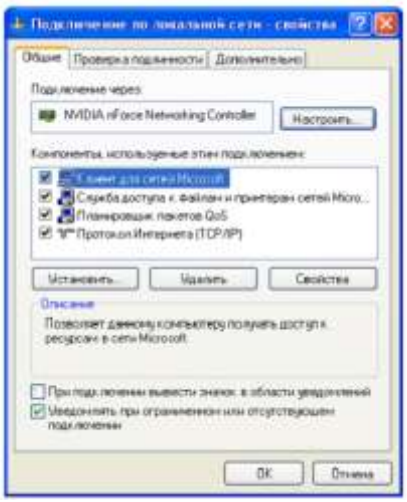


Рисунок 5.2. Закладка «Общие», "Сетевые подключения"

В появившемся окне свойств TCP/IP выбираем "Использовать следующий IP адрес"

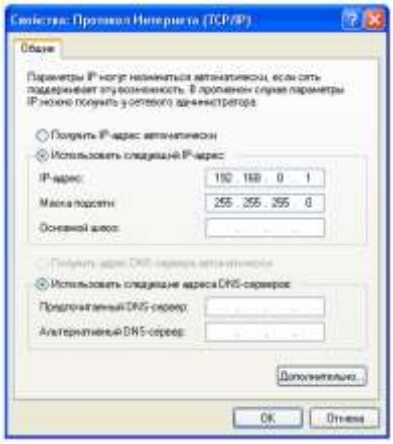


Рисунок 5.3 Свойства протокола TCP/IP

Зададим адреса в диапазоне от 192.168.0.1 до 192.168.0.N, а в качестве маски подсети укажем 255.255.255.0, она устанавливается обязательно одинаковой на все компьютеры локальной сети.

Теперь необходимо настроить рабочую группу, а также ввести имя компьютера для представления в сети. Для этого нажимаем правой кнопкой мыши на иконке "Мой компьютер" и выбираем пункт "Свойства". В появившемся окне переходим на закладку "Имя компьютера" и нажимаем кнопку "Изменить".

В поле "Имя компьютера" вписываем имя, которым компьютер будет представляться в сети. Используйте английские буквы, цифры. Старайтесь не использовать другие символы, так как при этом возможны проблемы в работе сети. Имена компьютеров должны отличаться друг от друга.

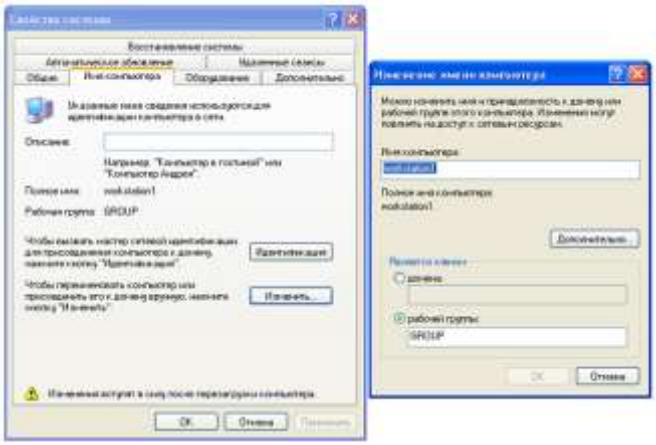


Рисунок 5.4. Свойства системы

Переходим, ко второй части лабораторной работы. На компьютере, через который планируется подключение сети к Internet необходимо наличие двух сетевых адаптеров.

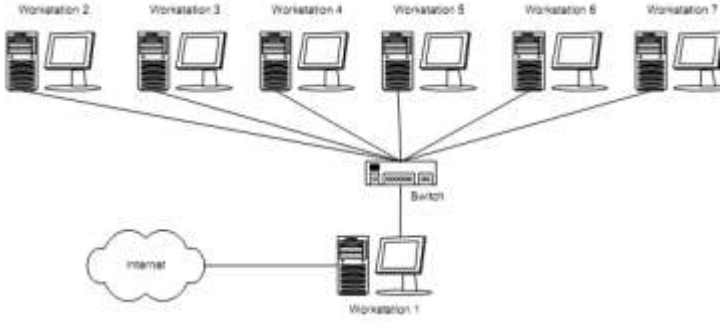


Рисунок 5.5. Схема подключения сети

На этом же компьютере, открываем Панель управления > Сеть и удаленный доступ к сети (Control Panel > Network Connections), выберите ваше подключение правой кнопкой и нажмите Свойства (Properties). В закладке Дополнительно (Advanced) отметьте флажок Общий доступ в моей сети для этого подключения (Allow Other Network Users To Connect Thought This Computer' s Internet Connection).

Рисунок 5.6. Вкладка «Сеть и удаленный доступ к компьютеру»

ICS жестко сконфигурирован и назначает компьютеру, обеспечивающему доступ, статический внутренний адрес 192.168.0.1. Все клиенты размещаются в одной физической подсети, получают адреса из диапазона 192.168.0.0/24 (/24 означает первые 24 единицы в маске сети, представленной в двоичной форме, т.е. это маска 255.255.255.0) и используют для разрешения имен только DNS-сервер, размещенный на этом же компьютере. На клиентских машинах устанавливаем Автоматическое получение IP-адреса.

Вывод. Теперь Вы сумеете построить сеть из нескольких компьютеров, с использованием сетевого оборудования, а также организовать доступ к сети Internet.

Контрольные вопросы:

1. Что такое cross-over кабель?
2. Как осуществляется настройка операционной системы?
3. Порядок установки доступа к папке?
4. Какой кабель используется при подключении к концентратору?

Литература:

Осн. 1[273-287], 2[166-174]
Доп.3[99-112]

Лабораторная работа № 6.
Тема: Утилиты для компьютерных сетей (Windows)

Цель работы: Изучить основные сетевые утилиты. (MS Windows)

Теоретические сведения

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации тестирования сетевого соединения. показан в Таб.6.1

Таблица 6.1.

arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.

netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Проверка правильности конфигурации TCP/IP.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Тестирование связи с использованием утилиты ping.

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда ping проверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение ``Request time out" (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа -w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем - неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран

звездочки (*), либо сообщения типа ``Destination net unreachable", ``Destination host unreachable", ``Request time out", ``Time Exeeded".

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP ``Time Exeeded" (Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Утилита ARP.

Основная задача протокола ARP - трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Утилита netstat.

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Задания

1. Получение справочной информации по командам

Выведите на экран справочную информацию по утилитам arp, ipconfig, nbstat, netstat, nslookup,route, ping, tracert, hostname. Для этого в командной строке введите имя утилиты без параметров или с /?. Изучите и запишите ключи, используемые при запуске утилит.

2. Получение имени хоста

Выведите на экран имя локального хоста с помощью команды hostname.

3. Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

4. Тестирование связи с помощью утилиты ping

Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.
С помощью команды ping проверьте перечисленные ниже адреса и для каждого из них отметьте время отклика. Попробуйте увеличить время отклика.

192.168.10.5
192.168.10.89
192.168.1.1
192.168.1.5
192.168.3.1
192.168.1.90

Задайте различную длину посылаемых пакетов. Определите доменное имя компьютера.

5. Определение пути IP-пакета

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их:

192.168.10.5
192.168.10.89
192.168.1.1
192.168.1.5
192.168.3.1
192.168.1.90

6. Просмотр ARP-кэша

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

7. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

8. Net view. Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда net view выводит список компьютеров в текущем домене.

Исследовать ресурсы домена tspu с помощью команды **net view**. Получить списки общих ресурсов компьютеров вашей аудитории.

Контрольные вопросы:

1. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
2. Каким образом каманда ping проверяет соединение с удаленным хостом?
3. Что такое хост?
4. Что такое петля обратной связи?
5. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?
6. Как работает утилита tracert?

Литература:

1. Осн. 1[288-294], 2[180-188]
2. Доп.3[115-122]

Лабораторная работа № 7.
Тема: Анализ задач ЛВС среднестатистического офиса.

Цель работы: Характеризация среднестатистической локальной сети, рассмотрение типичных задач ЛВС офиса, изучение приемов администрирования сети.

Теоретические сведения:

Характеристики типичной офисной сети: сервер, роутер, 15-20 рабочих станций. Сервер на Windows 2000 Server, с настроенным DNS, выполняет роль файлового сервера. На роутере, как обычно, proxy-server, mail-server. Интеренет- канал - выделенная линия на 33,6 Кбит/с.

Локальная сеть - Fast Ethernet 100 Мбит/с. Тип деятельности - торговая, посредническая или оказание информационных услуг.

Социальный фактор.

Как правило, в любой организации основную прослойку составляют менеджеры. Их небрежное отношение к технике, обусловленное низким образовательным уровнем, может представлять большую опасность для стабильности работы офисной сети, в виду внушительного эксплуатирования ресурсов последней.

Стандартная схема деятельности менеджера фирмы может заключаться в основном в:

- ✓ рассылке писем с предложением о сотрудничестве существующим и потенциальным клиентам, обычно с вложенным прайсом;
- ✓ получении таких же писем самими менеджерами;
- ✓ переписке по ICQ с клиентами и сотрудниками;
- ✓ постоянный поиск информации в Internet.

Многие проблемы являются типовыми и решить их можно путем элементарных мероприятий.

E-mail

Наличие почты в организации обязательно. Обычно компьютер с доступом в интеренет (роутер) один, поэтому требуется наличие почтового сервера для одновременного доступа к почте со всех имеющихся рабочих станций. Программ-серверов огромное множество, но рекомендуется остановить выбор на одном из самых популярных из них - MDaemon фирмы "Alt-N", http://www.mdaemon.com/. В MDaemon, как и во многих других почтовых серверах, есть функция создания листов рассылки. Заключается она в следующем: на специальный адрес провайдера, именуемый как "smart host", отсылается один вариант письма и список адресов, по которым его нужно разослать. Трафик не загружен и письма разосланы. Только необходимо проконсультироваться, поддерживает ли провайдер этот вид сервиса.

Также имеют место ограничения со стороны провайдера на количество рассылаемых писем в одной рассылке - обычно это число 40-50. Сделать в MDaemon это несложно. В верхнем меню "List" следует выбрать "New list". Появится окно настройки. Далее в закладке "Options" вводим имя рассылки, в закладке "Members" перечисляем все адреса, которые будут должны будут получать ваш список писем, в закладке "Routing" надо поставить переключатель на "Route a single copy…" и в открывшемся поле "Host Name" ввести адрес сервера, который нужно узнать у провайдера.

Теперь на адрес, который был введен в закладке "Options", отсылается скрытая копия письма, предназначенного для рассылки. Остальную работу сделает сервер провайдера.

При рассылке писем на любые адреса, попавшиеся на глаза, опасность заключается в том, что обычный пользователь может начать бороться со спамом, т.е. с вашей организацией. Методы борьбы бывают пассивные и активные.

Пассивные - это известные почтовые фильтры: блокировка входящих писем от спамерских адресов. При этом сисадмин может наблюдать процесс загрузки трафика при возврате блокированных писем. Предотвратить это легко - в настройках рассылочного листа в закладке "Members" внизу есть флажок "Automatically remove dead address …" При его установке несуществующие и заблокированные адреса будут автоматически удаляться из списка адресов рассылки.

Активные методы борьбы со спамом выражаются в том, что Интернет стабильно работает, почта приходит, но не уходит. Получатель спама отсылает письмо-жалобу вашему провайдеру о том, что с такого-то адреса ему рассылают нежелательную информацию. И довольно часто провайдер, не уведомив вас, блокирует порт исходящей почты. В целях профилактики данной проблемы системный администратор должен:

- ✓ Контролировать лично содержимое рассылок. По сетевому этикету, текст сообщения должен содержать информацию о том, как отказаться от рассылки, если получатель в ней не заинтересован.

✓ Обязательно создать дополнительный ящик abuse@ваш_домен. Этот адрес по умолчанию принят на всех почтовых серверах провайдеров, как своего рода книга жалоб.

✓ При любых проблемах с почтой сразу же звонить провайдеру.

Ограничения на размер входящих и исходящих писем можно установить в окне "Miscellaneous Options" меню «Setup», в закладке «Servers» внизу, под заголовком «Data transfer limit».

Большинство пользователей сходу читают вложения, не проверяя на вирусы. В этой ситуации системный администратор может установить антивирусные мониторы, типа антивируса Касперского. Хотя иногда как рабочая станция, так и сервер могут «зависать» из-за того, что антивирусные мониторы не поделили приоритет доступа с основной программой. Многие пользователи убирают антивирусный монитор из автозагрузки и системного трея, превышая таким образом свои полномочия и нарушая систему безопасности предприятия.

В подобных случаях при помощи почтового сервера можно довольно эффективно бороться с вирусами в почтовых вложениях. Для этого достаточно настроить фильтры (комбинация клавиш Ctrl+F5). И в закладке «Admins/Attachments» можно ввести названия файлов, расширения, которые будут удаляться из входящего письма. Поставьте разрешение только для *.rtf, тогда *.doc, *.pif, *.scr, *.bat, не говоря уже про *.exe, будут обрезаться. Таким образом, вы предотвратите на работе вирусную эпидемию. Только, настроив фильтр, следует предупредить пользователей, в каком формате можно получать вложения, иначе организация понесет убытки по вине сисадмина из-за нарушений связи

Internet

Прокси-серверов под Windows огромное множество. WinGate, WinRoute, WinProxy и т.д. В Windows 98, Me также есть подобие прокси, именуемое «общий доступ в Интернет».

Многие выбирают proxy-серверу фирмы «Alt-N» WinGate за его функциональность. Но рассмотрим более простой чешский продукт WinProxy, http://www.winproxy.cz, который также может использоваться, как простой mail-server. В принципе, не имеет значения, каким прокси-сервером пользоваться, главное – что с ним делать. Задача – облегчить трафик. В окне сетевого мониторинга и через статистику определите, какие посторонние сайты чаще всего посещают пользователи. Запрет на доступ к вышеуказанным ресурсам основательно разгрузит трафик.

Использование файрволлов не ограничивается защитой от хакеров. В первую очередь, это фильтр – пропуск нужной информации и отсеивание ненужной. Большинство сисадминов смогло по достоинству оценить возможности известного AtGuard (www.atguard.com). В принципе, возможности его велики – им даже можно некоторым разрешать, некоторым запрещать, к примеру, печатать на принтер.

Установив его на роутер, вы увидите вверху экрана полоску системных настроек. Далее нужно настроить фильтры и firewall в «AtGuard Settings». Интерфейс весьма интуитивен, настройка не вызывает затруднений. Кроме того, в РуНете есть множество документации на русском языке по настройке AtGuard. Программа имеет собственную базу адресов-источников баннеров, которую можно пополнять самостоятельно.

После дня-двух блокировки баннеров, фильтр сэкономит 40-100 Мбайт в месяц.

Организация выхода несколько компьютеров в Интернет на основе доступа только с одного из них.

Для создания коллективного доступа можно использовать простую в настройках и не требовательную к ресурсам программу – Kerio WinRoute. Она обеспечивает выход в Интернет компьютеров, входящих в локальную сеть, через одно внешнее соединение, неважно, каким устройством поддерживаемое – обычным модемом, модемом для выделенных линий, сетевую карту или SDSL. Достаточно, чтобы на компьютере, где будет установлена эта программа, было устройство для выхода в Интернет и сетевая плата для внутренней сети. Требования к этому компьютеру невелики – для вполне удовлетворительной работы может быть достаточно 486-го процессора, размер оперативной памяти зависит от числа подключений и желательно иметь хороший винчестер для кэширования. Если кроме обеспечения доступа к Сети иные возможности программы не требуются, достаточно установить четвертую версию программы.

Пятую версию лучше использовать, если планируете поставить почтовый сервер. Основные возможности программы:

- ✓ преобразование сетевых адресов (Network Address Translation, или NAT);
- ✓ распределение портов (Port mapping);
- ✓ фильтрация пакетов;
- ✓ поддержка DHCP, DNS и почтового серверов;
- ✓ поддержка кэширования http;
- ✓ протоколирование всех действий;
- ✓ удаленное администрирование.

Использование встроенного в программу DNS-модуля предназначено, в первую очередь, для снижения нагрузки по обращениям к внешним DNS-серверам. Имея собственный кэш запросов, программа будет обрабатывать обращения к внешним сервисам быстрее, просматривая кэш, и лишь при отсутствии в нем нужной информации будет обращаться к внешнему DNS-серверу. Для того чтобы использовать этот сервер DNS, нужно настроить протокол TCP/IP на клиентской машине. Для этого необходимо ввести адрес машины, на которой запущен WinRoute, как адрес DNS-сервера.

Использование прокси-сервера позволяет решать несколько задач. Во-первых - уменьшение внешнего трафика за счет использования сохраняемых в кэше просмотренных страниц. Кроме снижения трафика, увеличивается скорость доступа. Есть и минус - неудобно работать с часто обновляемыми страницами (новостные ресурсы, форумы). Во-вторых, использование прокси позволяет выполнить дополнительную настройку прав доступа к внешним ресурсам. Например, вы можете ограничить доступ определенным пользователям к определенным Web-сайтам. Запреты могут быть применены к отдельным пользователям, группам пользователей или отдельным URL'ам.

При настройке прокси-сервера назначаются:

- ✓ порт (лучше всего использовать порт по умолчанию - 3128);
- ✓ включение кэширования страниц;
- ✓ ведение лога посещенных страниц;
- ✓ размер кэша (устанавливается максимальный размер кэша в мегабайтах. Когда кэш превосходит этот лимит, происходит урезание наполнения кэша до 85% от лимита. Наиболее "старые" в кэше данные удаляются.);
- ✓ разрешение кэширования страницы при "досрочном" переходе пользователя к другой;
- ✓ разрешение на кэширование только структуры ftp-каталогов;
- ✓ срок, в течение которого данные будут храниться в кэше;
- ✓ максимальный размер хранимых объектов. Все, что больше - кэшироваться не будет.

Достоинства программы Winroute для использования в небольших сетях заключаются в простоте настройки, стабильности в работе и неприхотливости к используемому оборудованию.

Задания

1. Организуйте коллективный доступ в Интернет на основе программы Kerio Win Router.
2. Организуйте с помощью программы MDaemon прием вложений почтовых сообщений только с расширением *.rtf путем установке фильтра на указанном почтовом сервере.

Контрольные вопросы.

1.В чем заключаются достоинства программы Winroute для использования в небольших сетях?
2.Как называется одна из самых популярных программ, ставшая фактически стандартом почтовых серверов организаций? Кто является разработчиком программы? Как можно её найти?
3.Дайте определение понятия «спам».
4.В чем заключаются пассивные методы борьбы со спамом?
5.В чем заключаются активные методы борьбы со спамом?
6.Перечислите названия нескольких прокси-серверов.

7.Какая программа может обеспечить коллективный доступ в Интернет через одно внешнее соединение?

Литература:

1. Осн. 1[295-300], 2[189-194]
2. Доп.3[125-129]

Лабораторная работа № 8
Тема: Контроль за трафиком.

Цель работы: Изучение интерфейса и способов настройки для работы программы Tmeter с целью учета раздельного трафика – для интернета и внутренней локальной сети.

Теоретические сведения:

Для лабораторной работы мы будем использовать программу Tmeter. Для некоммерческого использования Tmeter позволяет задать только три счетчика трафика, но нам и этого хватит с лихвой. Отметим, что данное приложение несовместимо с некоторыми брандмауэрами. В частности, с NIS и Sygate он работать не будет, а вот с Outpost и Look'n'Stop проблем совместимости нет.

После скачивания программы Tmeter следует провести процедуру полной инсталляции. От значка на рабочем столе можно отказаться, так как программа и так всегда будет присутствовать в системном трее. После инсталляции нужно выполнить перезагрузку.

Щелкнув мышкой по значку в трее, запускаем управляющую программу. Заметьте, что в состав Tmeter входят два основных компонента: драйвер, считающий объем переданных данных, и консоль управления. Если у вас локальная сеть, то вы можете с одной консоли подключиться к драйверу на другом компьютере.

Далее следуем по древовидному меню в «Конфигурация -> Набор фильтров». Там уже есть три настроенных фильтра. Если у вас по сети доступ только в интернет, то можно оставить все как есть.

Но если вам нужно раздельно учитывать внешний и внутренний трафик, то удаляем фильтры «DNS» и «Весь трафик» и приступаем к заготовке новых. Нажимаем кнопку «Добавить» и выбираем «Правило» (признаки пакетов, которые необходимо подсчитывать) или «Фильтр» (группа правил). Последний используется для подсчета трафика, передающегося по разным портам, например, через почтовые POP3 и SMTP. Итак, добавляем фильтр.

Фильтру нужно дать какое-нибудь название, например «Внутренний трафик ЛВС». Затем в фильтр надо добавить правила.

По умолчанию тут ничего особо не изменяем. Кроме пункта «Назначение»: тут необходимо выбрать «IP-адреса моей локальной сети». «Описание правила» – это подсказка для самих себя, пишем что угодно. Нажимаем «OK». Готово. Отметим, что в окне «Редактор фильтра» можно задать цвет графика, показывающего загрузку канала. Для наглядности желательно, чтобы у разных фильтров были разные цвета. Вновь жмем «OK», и фильтр «Внутренний трафик ЛВС» готов.

Аналогично создаем еще один фильтр «Трафик интернет». Там тоже добавляем правило, при этом все оставляем по умолчанию, кроме пункта «Назначение» – в нем нужно выбрать «IP-адреса глоб. сети». Готово.

Теперь указываем программе Tmeter какой трафик считать локальным, а какой глобальным. Для этого следуем по дереву настроек в «Конфигурация -> Группы IP-адресов».

Здесь надо добавить диапазон IP-адресов вашей локальной сети. Скорее всего, это какой-то из этих четырех вариантов: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 или 169.254.0.0-169.254.255.255. Ничего не мешает добавить их все. Закончив все настройки, нажимаем кнопку «Применить», и настройки будут переданы драйверу.

Теперь можно пойти в меню «Статистика -> Счетчики фильтров», где и будет показываться то, что мы сейчас настраивали: график локального и интернетовского трафика, а также будет указано количество переданных и принятых байт.

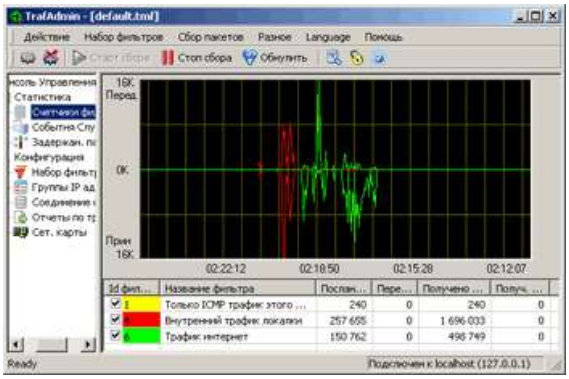


Рисунок 8.1. Окно программы TMeter

Задания

1. Установить программу TMeter с инсталляционного диска.
2. Создайте фильтры для раздельного учета внутреннего и внешнего трафика и добавьте правила (выберите разные цвета для разных графиков).

Контрольные вопросы:

1. В чем заключается цель использования программ для учета трафика?
2. Каковы возможности подобных программ?
3. Два основных компонента, входящих в состав программы TMeter.
4. Запишите алгоритм создания собственного фильтра в программе TMeter.
5. Как задается диапазон IP-адресов локальной сети?
6. Как указать IP-адрес глобальной сети при создании фильтра в программе TMeter?

Литература:

1. Осн. 1[301-312], 2[195-199]
2. Доп.3[133-138]

Лабораторная работа № 9
Тема: Изучение вопросов конфигурации сетей Ethernet

Цель работы: изучение вопросов конфигурации сетей Ethernet

Теоретические сведения

Наибольшее распространение среди локальных вычислительных сетей получила сеть Ethernet (стандарт IEEE 802.3). Стандарт определяет множественный доступ к моноканалу типа “шина” с обнаружением конфликтов и контролем передачи (по-русски МДКН/ОК - метод доступа с контролем несущей и обнаружением коллизий (столкновений), по-английски CSMA/CD – Carrier-Sense Multiple Access/Collision Detection). Основные характеристики стандарта IEEE 802.3 следующие: топология – “шина”, скорость передачи – 10 Мбит/с, метод доступа - CSMA/CD, передача узкополосная (моноканал). Передача идет пакетами переменной длины. Предусмотрена индивидуальная, групповая и широковещательная адресация.

Помимо стандартной топологии типа “шина” применяются также топологии типа “пассивная звезда” и “дерево”. При этом предполагается использование репитеров и пассивных (репитерных) концентраторов, соединяющих между собой различные части (сегменты) сети (рис. 9.1).

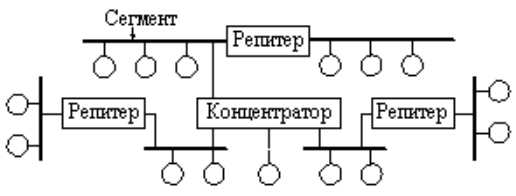


Рисунок 9.1. Пример соединения сети

В качестве сегмента может выступать единичный абонент. Главное – чтобы в полученной в результате топологии не было замкнутых путей (петель). Фактически получается, что абоненты соединены все в ту же “шину”, так как сигнал от каждого из них распространяется сразу во все стороны и не возвращается назад.

Для сети Ethernet стандарт определяет четыре основных типа среды передачи:

- 10BASE5 (“толстый” коаксиальный кабель);
- 10BASE2 (“тонкий” коаксиальный кабель);
- 10BASE-T (витая пара);
- 10BASE-F (оптоволоконный кабель).

Обозначение среды передачи включает в себя три элемента: цифра “10” означает скорость передачи 10 Мбит/с, слово BASE означает передачу в основной полосе частот (т.е. без модуляции высокочастотного сигнала), а последний элемент означает допустимую длину сегмента: “5” – 500 метров, “2” – 200 метров (точнее, 185 метров) или тип линии связи: “T” – витая пара (от английского “twisted-pair”, “F” – оптоволокно (от английского “fiber optic”).

Выбор конфигурации Ethernet

Соблюдение многочисленных ограничений, установленных для различных стандартов физического уровня сетей Ethernet, гарантирует корректную работу сети.

Правила “5-4-3” для коаксиальных сетей и “4-х хабов” для сетей на основе витой пары и оптоволокна не только дают гарантии работоспособности сети, но и оставляют большой “запас прочности” сети.

Для сетей, состоящих из смешанных кабельных систем, на которые правила о количестве повторителей не рассчитаны, необходимо проводить дополнительные расчеты.

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

- количество компьютеров в сети не более 1024;
- максимальная длина каждого физического сегмента не более величины, определенной в соответствующем стандарте физического уровня;
- время двойного оборота сигнала между двумя самыми удаленными друг от друга компьютерами сети не более 575 битовых интервала;
- сокращение межкадрового интервала при прохождении последовательности кадров через все повторители должно быть не больше, чем 49 битовых интервала.

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

Расчет времени двойного оборота сигнала

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 9.1.

Таблица 9.1.

Тип сегмента Ethernet	Макс. длина, м	Начальный сегмент		Промежуточный сегмент		Конечный сегмент		Задержка на метр длины
		t0	tm	t0	tm	t0	tm	t1
10BASE5	500	11,8	55,0	46,5	89,8	169,5	212,8	0,0866
10BASE2	185	11,8	30,8	46,5	65,5	169,5	188,5	0,1026

10BASE-T	100	15,3	26,6	42,0	53,3	165,0	176,3	0,1130
10BASE-FL	2000	12,3	212,3	33,5	233,5	156,5	356,5	0,1000
FOIRL	1000	7,8	107,8	29,0	129,0	152,0	252,0	0,1000
AUI (> 2 м)	2+48=50	0	5,1	0	5,1	0	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.

Расчет сокращения межкадрового интервала

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 9.2.

Таблица 9.2.

Тип сегмента	Начальный сегмент	Промежуточный сегмент
10BASE5	16	11
10BASE2	16	11
10BASE-T	10,5	8
10BASE-FL	10,5	8

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.

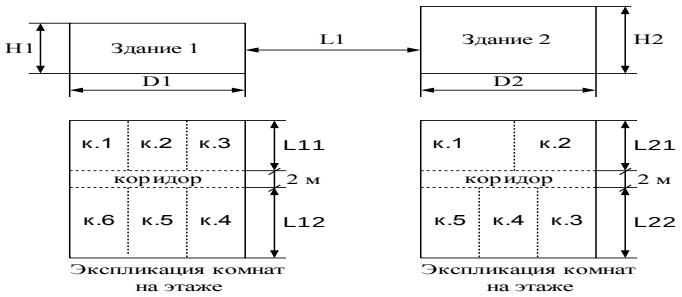
Порядок выполнения работы

1. Ознакомиться с теоретической частью к лабораторной работе.
2. В соответствии с заданным вариантом спроектируйте локальную вычислительную сеть организации (ПРИЛОЖЕНИЕ А).
3. Подготовьте спецификацию на оборудование и материалы спроектированной локальной вычислительной сети организации (ПРИЛОЖЕНИЕ Б).

Задания

1. Указать конфигурация спроектированной сети;
2. Создать программу расчетов, подтверждающих работоспособность сети (программа должна выполнять расчеты для любой конфигурации сети);

ПРИЛОЖЕНИЕ А



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.	*max*	*9*	*60*	*15*	*30*	*8*	*150*	*30*	*15*	*3*	*2*
2.	max	*6*	*75*	*20*	*25*	*12*	*120*	*25*	*20*	*2*	*3*
3.	max	*9*	*90*	*25*	*20*	*8*	*90*	*20*	*25*	*3*	*2*
4.	max	*6*	*120*	*30*	*15*	*12*	*60*	*15*	*30*	*2*	*3*

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

Вариант	***Здание***	***Этаж***	Тип среды передачи	Тип среды передачи между зданиями
1.	1	1	10BASE5	10BASE5
		2	10BASE2	
		3	10BASE-T	
	2	1	10BASE-FL	
		2	10BASE5	
2.	1	1	10BASE2	10BASE2
		2	10BASE-T	
	2	1	10BASE-FL	

		2	10BASE5	
		3	10BASE2	
3.	1	1	10BASE-T	10BASE-T
		2	10BASE-FL	
		3	10BASE5	
	2	1	10BASE2	
		2	10BASE-T	
4.	1	1	10BASE-FL	10BASE-FL
		2	10BASE5	
	2	1	10BASE2	
		2	10BASE-T	
		3	10BASE-FL	

Можно применять репитеры и репитерные концентраторы на 4, 8, 12 портов.

ПРИЛОЖЕНИЕ Б

№№	Наименование	Единица измерения	Количество
Оборудование			
1.	Репитер	шт.	
2.	Репитерный концентратор на 4 порта	шт.	
3.	Репитерный концентратор на 8 портов	шт.	
4.	Репитерный концентратор на 12 портов		
Материалы			
1.	“Толстый” коаксиальный кабель	м	
2.	“Тонкий” коаксиальный кабель	м	
3.	UTP-кабель категории 3	м	
4.	Оптический кабель	м	

Контрольные вопросы

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

Литература:

1. Осн. 1[320-321], 2[200-216]
2. Доп.3[140-143]

Лабораторная работа № 10

Тема: Изучение вопросов конфигурации сетей Fast Ethernet

Цель работы: изучение вопросов конфигурации сетей Fast Ethernet

Теоретические сведения: Сеть Fast Ethernet – это составная часть стандарта IEEE 802.3. Она представляет собой более быструю версию стандарта Ethernet, использующую метод доступа CSMA/CD (Carrier-Sense Multiple Access/Collision Detection) - метод доступа с контролем несущей и обнаружением коллизий (столкновений) и работающий на скорости передачи 100 Мбит/с. В Fast Ethernet сохранен формат кадра принятый в классической версии Ethernet.

Основная топология сети Fast Ethernet – “пассивная звезда”. Fast Ethernet требует обязательного применения концентраторов. Концентраторы могут объединяться между собой связными сегментами, что позволяет строить сложные конфигурации.

Стандарт определяет три типа среды передачи для Fast Ethernet:

- 100BASE-T4 (передача идет со скоростью 100 Мбит/с в основной полосе частот по четырем витым парам электрических проводов);

- 100BASE-TX (передача идет со скоростью 100 Мбит/с в основной полосе частот по двум витым парам электрических проводов);

- 100BASE-F4 (передача идет со скоростью 100 Мбит/с в основной полосе частот по двум оптоволоконным кабелям).

Для присоединения сетевого адаптера к сетевому кабелю в сети Fast Ethernet иногда используются специальные трансиверы, ориентированные на какой-то один тип кабеля. В этом случае применяемый сетевой адаптер не зависит от типа среды передачи, что повышает гибкость системы. Трансивер при этом подключается к адаптеру трансиверным кабелем длиной 0,5 м, оснащенным 40-контактным разъемом. Однако гораздо чаще сетевой адаптер ориентируется изготовителем на какой-то один неизменяемый тип передачи, и трансивер при этом уже не требуется, так как сетевой кабель подключается непосредственно к адаптеру. Адаптер в данном случае оснащен соответствующим кабелю разъемом.

Стандарт определяет два типа (класса) репитеров (концентраторов) для Fast Ethernet:

- репитеры Класса I характеризуются тем, что они преобразуют приходящие по сегментам сигналы в цифровую форму прежде чем передавать их во все другие сегменты. Поэтому к ним можно подсоединять сегменты разных типов: 100BASE-TX, 100BASE-T4 и 100BASE-FX. Но процесс преобразования требует временной задержки, поэтому можно использовать только один репитер Клас-са I в пределах одной зоны конфликта;

- репитеры Класса II непосредственно повторяют приходящие на них сигналы и передают их в другие сегменты без преобразования. Поэтому к ним можно подключаться только сегменты одного типа (например, 100BASE-TX) или сегменты, использующие одну систему сигналов (например, 100BASE-TX и 100BASE-FX). Задержка в репитерах Класса II меньше, чем в репитерах Класса I, поэтому можно применять два таких репитера в пределах одной зоны конфликта.

Аппаратура 100BASE-TX

Схема объединения компьютеров в сеть 100BASE-TX практически ничем не отличается от схемы 10BASE-T.

Для присоединения неэкранированных кабелей, содержащих две витые пары (волновое сопротивление 100 Ом) используются 8-контактные разъемы типа RJ-45 категории 5. Длина кабеля не может превышать 100 метров. Также используется топология типа “пассивная звезда” с концентратором в центре. Только сетевые адаптеры должны быть Fast Ethernet, концентратор рассчитан на подключение сегментов 100BASE-TX, и кабель должен быть категории 5. Между адаптерами и сетевыми кабелями могут включаться трансиверы.

Предельная длина 100 м в Fast Ethernet определяется заданными временными соотношениями обмена (ограничение на двойное время прохождения). Стандарт рекомендует ограничиваться длиной сегмента в 90 м, чтобы иметь 10% запас.

Из восьми контактов разъема используется только 4 контакта: два для передачи и два для приема. Стандарт предусматривает также возможность применения экранированного сетевого кабеля с двумя витыми парами (волновое сопротивление – 150 Ом). В этом случае применяется 9-контактный разъем D-типа.

Аппаратура 100BASE-T4

Основное отличие аппаратуры 100BASE-T4 от 100BASE-TX состоит в том, что в качестве соединительных кабелей в ней используются неэкранированные кабели, содержащие четыре витые пары (кабели категории 3, 4 или 5).

Схема объединения компьютеров в сеть ничем не отличается от 100BASE-TX. Длина кабелей не может превышать 100 м (стандарт рекомендует ограничиваться 90 м для 10 % запаса). Между адаптерами и кабелями в случае необходимости могут включаться трансиверы.

Для подключения сетевого кабеля к адаптеру (трансиверу) используются 8-контактные разъемы типа RJ-45, соответствующей категории.

Обмен данными идет по одной передающей витой паре, по одной приемной витой паре и по двум двунаправленным витым парам с использованием дифференциальных сигналов.

Аппаратура 100BASE-FX

Аппаратура 100BASE-FX очень близка к аппаратуре 10BASE-FL. Точно также здесь используется топология типа “пассивная звезда” с подключением компьютеров к концентратору с помощью двух разнонаправленных оптоволоконных кабелей. Между сетевыми адаптерами и кабелями возможно включение трансиверов. Оптоволоконные кабели подключаются к адаптеру (трансиверу) с помощью разъемов типа SC, ST.

Максимальная длина кабеля между компьютером и концентратором составляет 412 метров, причем это ограничение определяется временными соотношениями.

Выбор конфигурации Fast Ethernet

Для определения работоспособности сети Fast Ethernet стандарт IEEE 802.3 предлагает две модели, называемые Transmission System Model 1 и Transmission System Model 2. При этом первая модель основана на несложных правилах, а вторая использует систему расчетов.

В соответствии с первой моделью, при выборе конфигурации надо руководствоваться следующими принципами:

- сегменты, выполненные на электрических кабелях (витая пара), не должны быть длиннее 100 м;
- сегменты, выполненные на оптоволоконных кабелях, не должны быть длиннее 412 м;
- если используются трансиверы, то трансиверные кабели не должны быть длиннее 50 см.

При выполнении этих правил надо руководствоваться таблицей 10.1, определяющей максимальные размеры (в метрах) зоны конфликта (т.е. максимальное расстояние между абонентами сети, не разделенными коммутаторами). При этом в двух последних столбцах таблицы, относящихся к случаю использования смешанных сред передачи (как витых пар, так и оптоволоконных кабелей), предполагается, что длина витой пары составляет 100 м, применяется только один оптоволоконный кабель. Первая строка относится к соединению двух компьютеров без применения репитера. Нереализуемые ситуации отмечены в таблице прочерками.

Таблица 10.1.

Тип репитера (концентратора)	Витая пара	Оптоволоконный кабель	T4 и FX	TX и FX
Без репитера (два абонента)	100	412	-	-
Один репитер класса I	200	272	231	260,8
Один репитер класса II	200	320	-	308,8
Два репитера класса II	205	228	-	216,2

Вторая модель основана на вычислениях суммарного двойного времени прохождения сигнала по сети.

Для расчетов в соответствии со второй моделью сначала надо выделить в сети путь с максимальным двойным временем прохождения и максимальным числом репитеров (концентраторов) между компьютерами. Если таких путей несколько, то расчет должен производиться для каждого из них. Расчет в данном случае ведется на основании таб.10.2.

Таблица 10.2.

Тип сегмента	Задержка на метр (битовый интервал)	Максимальная задержка (битовый интервал)
Два абонента TX/FX	-	100
Два абонента T4	-	138
Один абонент T4 и один TX/FX	-	127
Сегмент на кабеле категории 3	1,14	114 (100 м)
Сегмент на кабеле категории 4	1,14	114 (100 м)
Сегмент на кабеле категории 5	1,112	111,2 (100 м)
Экранированная витая пара	1,112	111,2 (100 м)
Оптоволоконный кабель	1,0	412 (412 м)
Репитер (концентратор) класса I	-	140

Репитер (концентратор) класса II с портами TX/FX	-	92
Репитер (концентратор) класса II с портами T4	-	67

Для вычисления полного двойного (кругового) времени прохождения для сегмента сети необходимо умножить длину сегмента на величину задержки на метр, взятую из второго столбца таблицы 10.2. Если сегмент имеет максимально возможную длину, то можно взять величину максимальной задержки для данного сегмента из третьего столбца таблицы. Затем задержки сегментов, входящих в путь максимальной длины, надо просуммировать и прибавить к этой сумме величину задержки для двух абонентов (три верхние строчки таблицы) и величины задержек для всех репитеров (концентраторов), входящих в данный путь. Суммарная задержка должна быть меньше, чем 512 битовых интервалов.

Задержки в кабеле могут отличаться от тех, которые приведены в таблице 10.2.

Для более точного расчета следует использовать временные характеристики конкретного кабеля, применяемого в сети. Производители кабелей иногда указывают величину задержки на метр длины, а иногда – скорость распространения сигнала относительно скорости света (или NVP – Nominal Velocity of Propagation). Связанны эти две величины формулой: $t_з=1/(3\cdot10^{10}\cdot NVP)$, где $t_з$ - величина задержки на метр кабеля. Например, если NVP=0,4 (40%) от скорости света, то задержка $t_з$ будет равна 8,34 нс/м или 0,834 битовых интервала. Для вычисления двойного (кругового) времени прохождения нужно удвоенное значение $t_з$ умножить на длину кабеля.

В таблице 10.3 даны величины NVP для некоторых типов кабелей.

Таблица 10.3

Фирма	Марка	Категория	NVP
AT&T	1010	3	0,67
AT&T	1041	4	0,70
AT&T	1061	5	0,70
AT&T	2010	3	0,70
AT&T	2041	4	0,75
AT&T	2061	5	0,75
Belden	1229A	3	0,69
Belden	1455A	4	0,72
Belden	1583A	5	0,72
Belden	1245A2	3	0,69
Belden	1457A	4	0,75
Belden	1585A	5	0,75

Для некоторых репитеров и концентраторов изготовители указывают меньшие величины задержек, чем приведенные в таблице 2, что также надо учитывать при выборе конфигурации сети.

Порядок выполнения работы

1. Ознакомиться с теоретической частью к лабораторной работе.

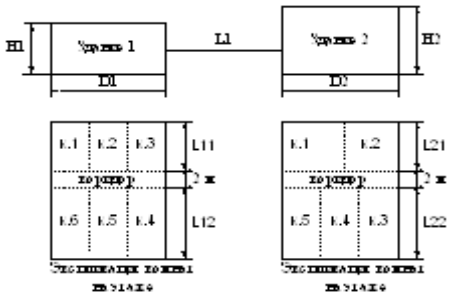
2. В соответствии с заданным вариантом спроектируйте локальную вычислительную сеть организации (ПРИЛОЖЕНИЕ А).

3. Подготовьте спецификацию на оборудование и материалы спроектированной локальной вычислительной сети организации (ПРИЛОЖЕНИЕ Б).

Задания

1. Указать конфигурация спроектированной сети;
2. Создать программу расчетов, подтверждающих работоспособность сети (программа должна выполнять расчеты для любой конфигурации сети);

ПРИЛОЖЕНИЕ А



Вариант	L1,м	H1,м	1,м	L11,м	L12,м	2,м	D2,м	L21, м	L22, м	Этажность здания 1	Этажность здания 2
1.	max	9	0	15	30		50	30	15	3	2
2.	max	6	5	20	25	2	20	25	20	2	3
3.	max	9	0	25	20		0	20	25	3	2
4.	max	6	20	30	15	2	0	15	30	2	3

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

Вариант	Здание	Этаж	Тип среды передачи	Тип среды передачи между зданиями
1.	1	1	100BASE-T4 (кабель AT&T 1010)	100BASE-FX
		2	100BASE-TX (кабель AT&T 1061)	
		3	100BASE-FX	
	2	1	100BASE-T4 (кабель AT&T 1041)	
		2	100BASE-TX (кабель AT&T 2061)	
2.	1	1	100BASE-TX (кабель Belden 1583A)	100BASE-T4 (кабель Belden 1229A)
		2	100BASE-FX	
	2	1	100BASE-TX (кабель Belden 1585A)	
		2	100BASE-FX	

		3	100BASE-T4 (кабель Belden 1455A)	
3.	1	1	100BASE-FX	100BASE-TX (кабель AT&T 2061)
		2	100BASE-T4 (кабель AT&T 2041)	
		3	100BASE-TX (кабель AT&T 1061)	
	2	1	100BASE-FX	
		2	100BASE-T4 (кабель AT&T 2061)	
4.	1	1	100BASE-T4 (кабель Belden 1455A)	100BASE-FX
		2	100BASE-TX (кабель Belden 1583A)	
	2	1	100BASE-FX	
		2	100BASE-TX (кабель Belden 1585A)	
		3	100BASE-FX	

ПРИЛОЖЕНИЕ Б

№№	Наименование	Единица измерения	Количество
Оборудование			
1.	Концентратор I класса на 8 портов	шт.	
2.	Концентратор I класса на 12 портов	шт.	
3.	Концентратор I класса на 16 портов	шт.	
4.	Концентратор I класса на 24 порта	шт.	
5.	Концентратор II класса на 8 портов	шт.	
6.	Концентратор II класса на 12 портов	шт.	
7.	Концентратор II класса на 16 портов	шт.	
8.	Концентратор II класса на 24 порта	шт.	
Материалы			
1.	UTP-кабель категории 3	м	
2.	UTP-кабель категории 4	м	
3.	UTP-кабель категории 5	м	
4.	STP-кабель категории 5	м	
5.	Оптический кабель	м	
6.	Вилка RJ-45	шт.	
7.	Розетка RJ-45	шт.	

Контрольные вопросы

1. Среды передачи для сети Fast Ethernet?
2. Аппаратура 100BASE-T4?
3. Аппаратура 100BASE-TX?
4. Аппаратура 100BASE-FX?
5. Выбор конфигурации Fast Ethernet (первая модель)?
6. Выбор конфигурации Fast Ethernet (вторая модель)?

Литература:

1. Осн. 1[320-321], 2[200-216]
2. Доп.3[140-143]

Лабораторная работа № 11

Тема: Основы работы с симулятором компьютерных сетей Packet tracer 5.0

Цель работы: Изучение основных функций симулятора компьютерных сетей Packet Tracer

Теоретические сведения:

На сегодняшний день на рынке IT существуют не так уж и много сетевых симуляторов. Широко известны такие симуляторы, как:

- BOSON NET SIM;
- CISCO Router eSim;
- Cisco Packet Tracker;
- Network Emulator;
- Dynamips;
- Cisco 7200 Simulator.

Из них наиболее распространенные в плане использования для обучения являются Boson NetSim, Cisco Packet Tracer и Network Emulator. Остановимся на них подробней.

Boson NetSim

Boson NetSim – программное обеспечение, которое моделирует работу сетевого оборудования Cisco, и разработано, чтобы помочь пользователю в изучении Cisco IOS.

Большинство других программных продуктов, «моделируя» поведение системы в заранее подготовленных лабораторных работах, фактически не могут отображать ситуаций, которые действительно могут случиться в сети. В отличие от них, NetSim использует технологии, специально разработанные компанией Boson, которые позволяют обойти этот недостаток и моделировать истинное поведение сети. Эти технологии позволят многим пользователям Boson NetSim выйти далеко за рамки выдуманных лабораторных работ, и лучше понять принципы функционирования Cisco IOS [5].

NetSim имеет очень развитую поддержку, обеспечивающую компанией Boson (это связано, конечно же, с бурными темпами развития телекоммуникационных сетей). В связи с этим, компания Cicso рекомендует использовать этот продукт для подготовки к сдачи экзаменов. Поэтому Boson выпускает различные версии NetSim'a, каждая из которых ориентирована на определенный экзамен и, соответственно, уровень знания пользователя.

Существует три версии NetSim'a для следующих экзаменов: NetSim для CCENT, NetSim для CCNA и NetSim для CCNP.

Cisco Packet Tracer

Данный программный продукт разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования.

Packet Tracer 4.0 включает следующие особенности:

- моделирование логической топологии: рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;
- моделирование в режиме реального времени;
- режим симуляции;
- моделирование физической топологии: более понятное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д.;
- улучшенный GUI, необходимый для более качественного понимания организации сети, принципов работы устройства;
- многоязыковая поддержка: возможность перевода данного программного продукта практически на любой язык, необходимый пользователю;
- усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;
- наличие Activity Wizard позволяет студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

С помощью данного программного продукта преподаватели и студенты могут придумывать, строить, конфигурировать сети и производить в них поиск неисправностей.

Packet Tracer дает возможность более подробно представлять новейшие технологии, тем самым делая учебный процесс чрезвычайно полезным с точки зрения усвоения полученного материала.

[**Network Emulator**

Программа Network Emulator была задумана в начале 1997 года. Проект превратился, по сути, в программу, обучающую ее пользователя всем тонкостям технологии на разных уровнях: от базовых понятий до особенностей обработки отдельных полей сетевых пакетов. Программа прошла путь от простейшего «роутера пакетов» до интеллектуального организатора виртуальных машин: на любом из компьютеров можно запустить несколько программ-аналогов настоящих приложений. Все они будут исполняться одновременно.

В дальнейшем появилось и другое «призвание» Network Emulator: обучение студентов принципу администрирования IP-сетей. Данное направление использования было с успехом реализовано в процессе проведения лабораторных работ по предмету "Сети ЭВМ" в Ульяновском Государственном Техническом Университете.

Данный симулятор включает в себя следующие возможности и технологии:

- маршрутизация, система моделирования каналов, IP-фильтрация;
- типы пакетов: ICMP, UDP, TCP, а так же низкоуровневые ARP-запросы;
- концепция интерфейсов и сокетов (простой, дейтаграммный и потоковый);
- эмуляция хостов, коммутаторов второго уровня и концентраторов;
- установка уровня помех на канале;
- связывание нескольких Network Emulator через реальную сеть TCP/IP [10].

В рамках курса лабораторные работы будут выполняться на Cisco Packet Tracer 4.0.

Cisco Packet Tracer 4.0 специально разработан для начала изучения современных телекоммуникационных систем, и больше других симуляторов соответствует данной задаче.

Cisco Packet Tracer

Данный симулятор позволяет студентам проектировать свои собственные сети, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Студенты могут изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней, рабочие станции, определять типы связей между ними и соединять их. После того, как сеть спроектирована, студенты могут приступать к конфигурированию выбранных устройств посредством терминального доступа и ли командной строки (см. рис.11.1).

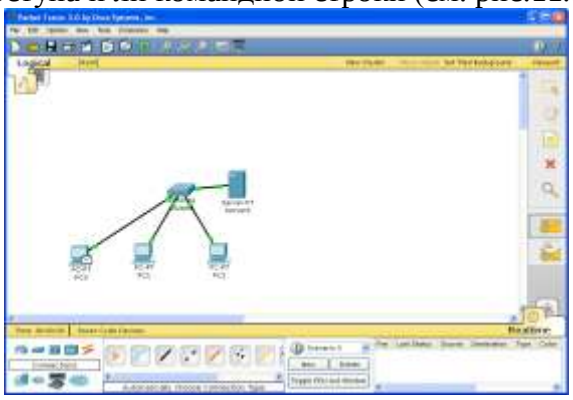


Рисунок 11.1 Cisco Packet Tracer 5.0

Отличительной особенностью данного симулятора является наличие в нем «Режима симуляции» (рис.11.2). В данном режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет студентам наглядно продемонстрировать, по какому интерфейсу в данные момент перемещается пакет, какой протокол используется и т.д.

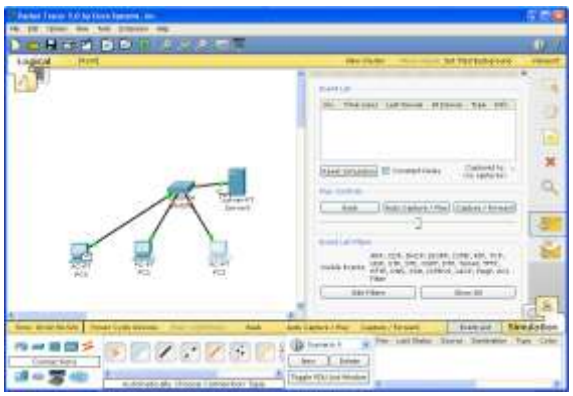


Рисунок 11.2. Режим «Симуляции» в Cisco Packet Tracer 5.0

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» студент может не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (см.рис.11.3).

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.

Практическая работа:

Построим простую локальную сеть с использованием статических IP адресов на основе HUB-а.

Для этого произведём следующие действия

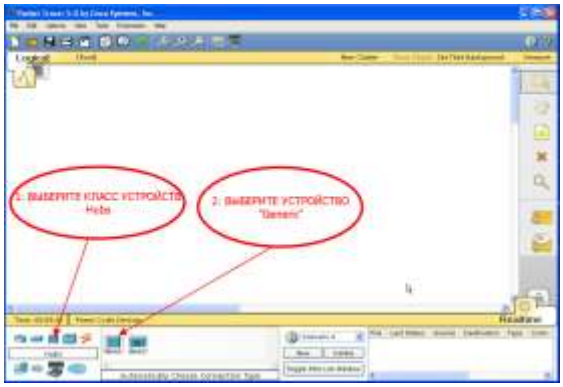


Рисунок 11.3 Добавление Hub

Рисунок 11.4 Добавление конечных устройств

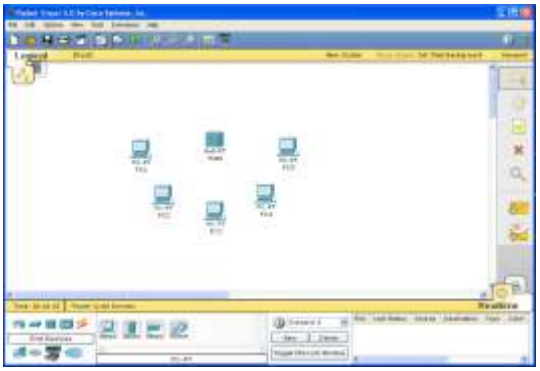


Рисунок 11.5 Результат добавления конечных устроств

Рисунок 11.6 Добавление физических соединений

7: Произведите подключение согласно таблице 11.1

Таблица 11.1: Параметры физических соединений

Устройство	Разъём	Конечное устройсво	Разъём конечного устройства
PC1	Fast Ethernet	Hub0	Port1
PC2	Fast Ethernet	Hub0	Port2
PC3	Fast Ethernet	Hub0	Port3
PC4	Fast Ethernet	Hub0	Port4
PC5	Fast Ethernet	Hub0	Port5

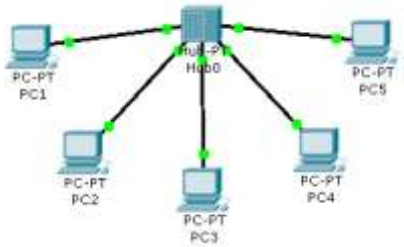


Рисунок 11.7 Результат добавления физических соединений

8: Двойным щелчком выберите устройство PC1, выберите вкладку «Desktop» и нажмите на значёк IP Configuration

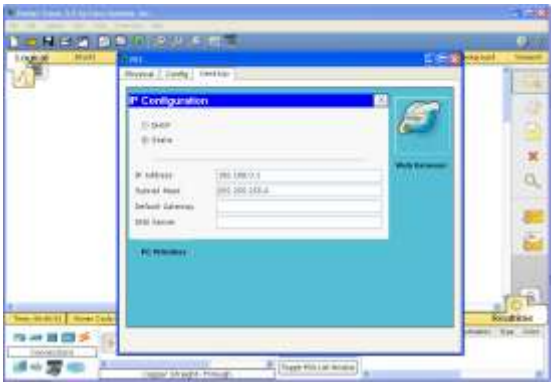


Рисунок 11.8 Логическая конфигурация конечных устройств

9: Произветите конфигурацию IP адреса соглано рисунку _

10: Произведите конфигурацию IP адресов остальных компьютеров согласно таблице 11.2

Таблица 11.2 Параметры логической конфигурации конечных устройств

Название устройства	IP адрес	Маска подсети	IP адрес шлюза	IP адрес DNS сервера
PC1	192.168.0.1	255.255.255.0		
PC2	192.168.0.2	255.255.255.0		
PC3	192.168.0.3	255.255.255.0		
PC4	192.168.0.4	255.255.255.0		
PC5	192.168.0.5	255.255.255.0		

После построения данной локальной вычислительной сети можно произвести анализ её поведения. Для этого существует 2 вида симуляции. Симуляция в реальном времени подойдёт для анализа работы приближённой к реальности. В разделе “Desktop” конечный устройств есть командная строка в которой имитируется работа ранее изученных нами команд для ОС семейства Windows.

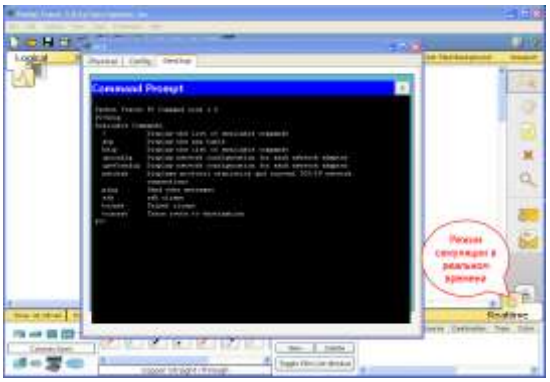


Рисунок 11.9 Симуляция командная строки в режиме реального времени

Откройте вкладку “Desktop” и выберите “Command prompt” произведите пинг компьютера в вашей сети. Например: 192.168.0.5Если сеть настроена правильно вы соответственно увидите информацию об ответных пакетах, примерно такую же как и в реальной сети.

Второй способ симуляции заключается в визуальном отображении пути пакетов передающихся по сети. Данный вид симуляции имеет несколько режимов, но все они основаны на пошаговом отображении процесса передачи пакета.

Для перехода в данный режим в правом нижнем углу выберите вкладку «Simulation Mode”

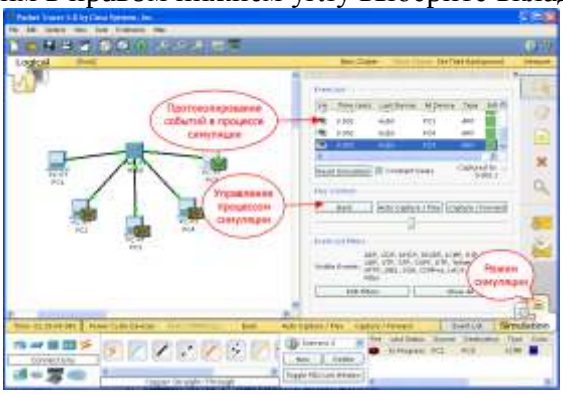


Рисунок 11.10 Режим пошаговой симуляции с визуальным отображением поведения передачи пакетов в сети

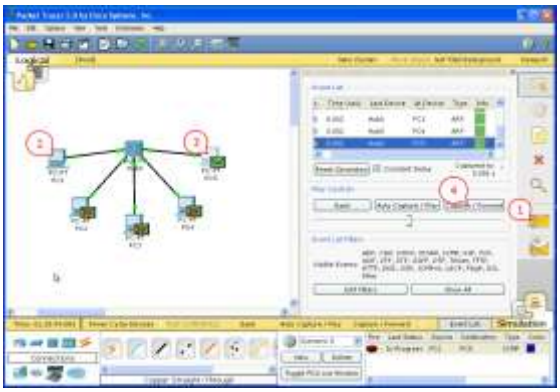


Рисунок 11.11 Пошаговая инструкция добавления тестового пакета

Для просмотра поведения передачи пакета из комьпютера A в компьютер B нужно выполнуить следующие действия согласно порядку указанному на рисунке _

1: Выбрать функцию добавления отправки пакета

2: Указать компьютер, который будет посылать пакет

3: Указать компьютер, примнимающий пакет
4: Произвдить пошаговую симуляцию передачи данных

Задания

Создать локальную вычислительную сеть тополгии «звезда» на основе коммутатора

1. Путём симуляции «реального времени» произвести проверку работоспособности сети
2. Путём пошаговой симуляции: произвести сравнительный анализ поведения сети в основе которой коммутатор (switch) по сравнению с ЛВС на основе концентратора (hub)

Контрольные вопросы:

1. Дать определение IP адрес
2. Дать определение MAC адрес
3. В чём функциональные различия между концентратором и коммутатором?
4. Максимальное количество компьютеров, подключаемых путём адресции TCP/IP V4 с маской подсети 255.255.255.0?
5. Какие существуют методы проверки работоспособности и поведения сети в Packet Tracer 5.0?

Литература:

Осн. 5[32-37]

Лабораторная работа № 12

Тема: Организация локальной вычислительной сети с использованием нескольких коммутаторов

Цель работы: Изучение особенности организации и поведения сети на основе нескольких коммутаторов образующих топологию сети «Дерево»

Теоретические сведения

Компьютерная вычислительная сеть с 24 битовой маской подсети может адресовать до 255 устройств. Для офиса и фирмы средних размеров обычно этого достаточно, однако стандартные коммутаторы имеют обычно до 24 портов, что физически ограничивает количество компьютеров работающих от одного коммутатора. Выходом из этой проблемы является организация сети с использованием нескольких коммутаторов по древовидной топологии.

Практическая работа:

Коммутатор, концентратор устройства предназначенные для физического, логического соединения.

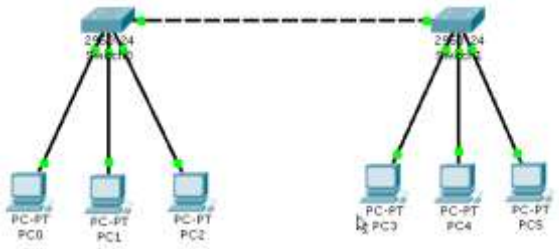


Рисунок 12.1 Топология «Дерево»

Произведём организацию ЛВС с несколькими коммутаторами. Обратите внимание, что соеденение между коммутаторами перекрёстное.

Адресное пространство представлено в таблице ниже:

№	Имя устройства	IP адрес	Маска подсети
1	PC-PT0	192.168.0.1	255.255.255.0
2	PC-PT1	192.168.0.2	255.255.255.0
3	PC-PT2	192.168.0.3	255.255.255.0
4	PC-PT3	192.168.0.4	255.255.255.0
5	PC-PT4	192.168.0.5	255.255.255.0
6	PC-PT5	192.168.0.6	255.255.255.0

Задания

3. Создать локальную вычислительную сеть топологии «дерево» на основе коммутатора
4. Путём симуляции «реального времени» произвести проверку работоспособности сети
5. Путём пошаговой симуляции: произвести сравнительный анализ поведения сети при передачи данных между ПК в пределах одного коммутатора, и ПК где пакет передаётся через соседние коммутаторы.

Контрольные вопросы:

6. Какие существуют стандарты прямой обжимки кабеля
7. В чём отличия между прямой и обратной обжимкой кабеля
8. В каких случаях используется прямая обжимка
9. В каких случаях используется обратная обжимка кабеля
10. Назовите особенности организации топологии «дерево», от какой топологии она происходит

Литература:

Осн. 5[40-52]

Лабораторная работа № 13

Тема: Организация локальной вычислительной сети с использованием DHCP сервера

Цель работы: Организация DHCP сервера и его настройка

Теоретические сведения:

Локальные компьютерные сети в малом офисе можно довольно просто организовать, если в них используется сравнительно небольшое количество компьютеров. Но если сеть состоит из 100 и более компьютеров, то сетевая конфигурация каждого компьютера может быть проблематична, особенно когда количество компьютеров подключённых к сети динамично меняется, и требуется подключение доступное в настройках даже для простого пользователя, и должны подключатся компьютеры, ранее не подключавшиеся к сети. Для решения этих задач можно использовать DHCP сервер. Задача DHCP автоматически конфигурировать сетевые параметры компьютера:

IP адрес
Маску подсети
Шлюз
DNS

Практическая работа:

Создайте локальную вычислительную сеть из 5-ти компьютеров по топологии «звезда», добавьте компонент «сервер» как это указано на рисунке

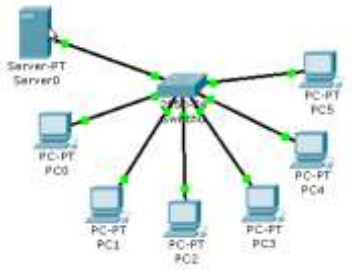


Рисунок 13.1. Топология «Звезда»

Данный компонент может симулировать работу нескольких видов сервера. Один из них это DHCP.

Произвеите конфигурацию DHCP как указано на рис.13.2

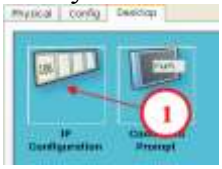


Рисунок 13.2 Конфигурация DHCP

Во вкладке Desktop запустите IP Configuration

Рисунок 13.3 вкладка «IP Configuration»

Произведите настройку сервера согласно рис.13.4

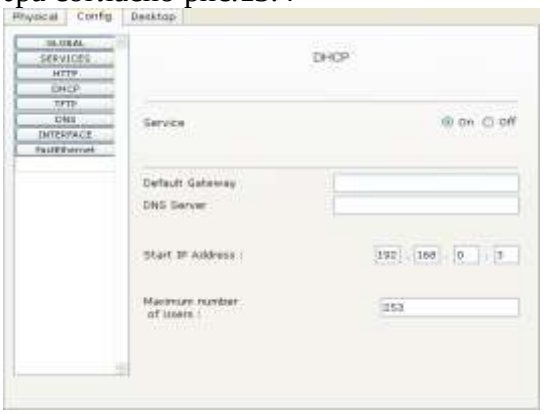


Рисунок 13.4 Настройка сервера

В DHCP сервере есть ряд настроек
Service – включение/выключение функции DHCP сервера
Default Getway – адрес шлюза, который будет раздаваться другим компьютерам
DNS Server – адрес DNS сервера, который будет раздаваться другим комьютерам
Start IP adress: стартовый адрес, с которого будут раздаваться адреса
Maximum number of Users: максимальное колличество компьютеров, подключаемых динамически.

Задания

6. Создать локальную вычислительную сеть топологии «дерево» на основе коммутатора с DHCP сервером
7. Путём симуляции «реального времени» произвести проверку работоспособности сети
8. Произвести анализ поведения сети, в которой есть компьютеры настроенные на DHCP адресацию, а также компьютеры с ручными сетевыми настройками.

Контрольные вопросы:

11. Дать определение «Сервер»
12. Для чего используется DHCP сервер?
13. В каких случаях используется динамическая адресация?
14. Какие настройки передаются через DHCP сервер?
15. Можно ли в сети, где используется DHCP сервер, использовать статическую адресацию вычислительных устройств?

Литература:

Осн. 5[55-64]

Лабораторная работа № 14

Тема: Соединение подсетей вместе путём использования маршрутизатора

Цель работы: Организовать соединение между двумя подсетями

Теоретические сведения:

Когда корпоративная сеть состоит более чем из 255 компьютеров, появляется необходимость организовывать несколько подсетей. Например
Может быть подсеть:

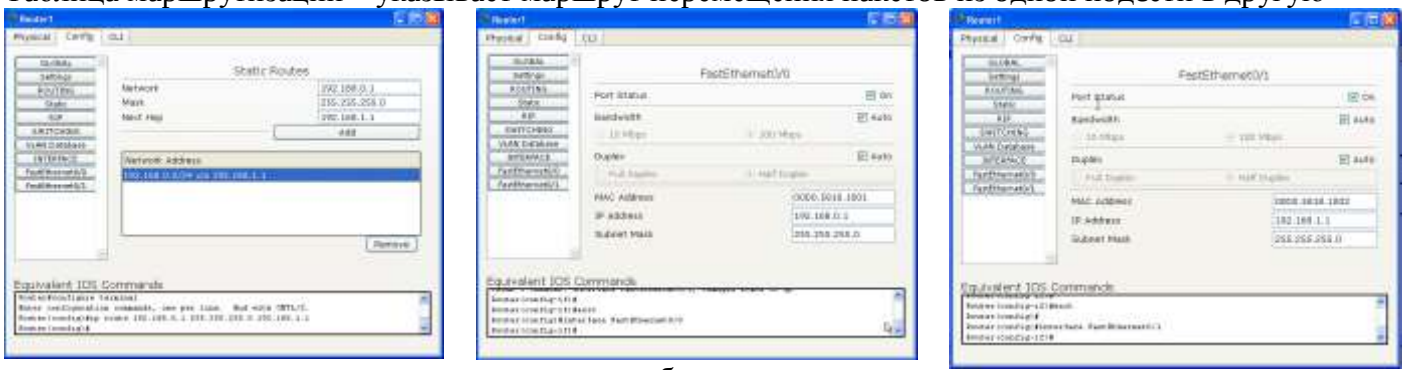
192.168.0._ Или 192.168.1._
Компьютеры подключённые к подсети 192.168.0._ могут видеть только компьютеры в пределах данного адресного пространства, но не смогут передавать данные, компьютера на адресное пространство 192.168.1._
Для решения данной задачи существуют устройство: маршрутизаторы
Эти устройства имея «таблицу адресации» соединяют подсети в единое информационное пространство

Практическая работа:

Постройте сеть как указано на рисунке 1.
Раздайте статические адреса следующим образом
Компьютеры, подключённые к Switch1 должны иметь адреса 192.168.0.3-192.168.0.5
Компьютеры, подключённые к Switch2 должны иметь адреса 192.168.1.3-192.168.1.5

Рисунок 14.1. Первичная организация ЛВС из 2-х подсетей

После распределения адресного пространства, произведите конфигурацию маршрутизатора, как указано на рисунке.
Основными параметрами являются:
Таблица маршрутизации – указывает маршрут перемещения пакетов из одной подсети в другую



а б *в*

Рисунок 14.2 Таблица маршрутизации

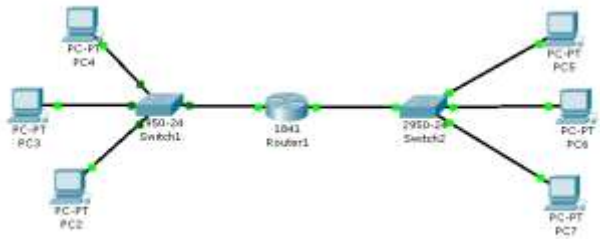


Рисунок 14.3. Организация ЛВС из 2-х подсетей

Задания

1. Создать локальную вычислительную сеть из нескольких подсетей с DHCP сервером
2. Путём симуляции «реального времени» произвести проверку работоспособности сети
3. Произвести анализ поведения сети, в которой есть DHCP и статические адреса

Контрольные вопросы:

1. Что такое таблица маршрутизации?
2. В каких случаях используется динамическая адресация?
3. Какие настройки передаются через DHCP сервер?
4. Можно ли в сети, где используется DHCP сервер, использовать статическую адресацию вычислительных устройств?
5. Для чего предназначен маршрутизаторы?

Литература:

Осн. 5[68-75]

Лабораторная работа № 15

Тема: Создание беспроводных компьютерных сетей и анализ поведения и характеристик

Цель работы: Организовать беспроводную вычислительную сеть

Теоретические сведения:

Проводная вычислительная сеть довольно надёжна и имеет хорошие скоростные характеристики, особенно когда идёт речь о передачи данных в пределах ЛВС. Однако не всегда она удобна в использовании, особенно когда у работников нет возможности находиться на одном месте, но крайне необходимо постоянный доступ к сети. Решением данной задачи может стать беспроводная вычислительная сеть. Наиболее распространённый стандарт беспроводной вычислительной сети: WiFi. Существует несколько стандартов WiFi: a, b, g, n, основное отличие: скоростные характеристики, и технология шифрования

В настоящее время наиболее распространены стандарты g и n

Практическая работа:

Выберите Wireless Devices -> Linksys. Данное устройство производит имитацию беспроводного адаптера Linksys WRT300N

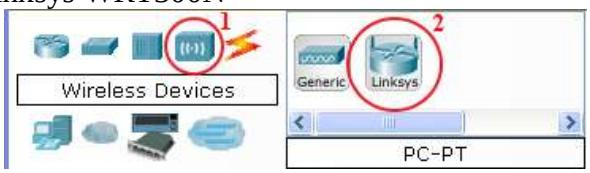


Рисунок 15.1 Имитация беспроводного адаптера Linksys WRT300N

Расставьте устройства, как это показано на рис.15.2

Рисунок 15.2. Порядок расстановки устройств

В данном устройстве существует имитация html интерфейса. В данную модель маршрутизатора также входят функции работы в режиме DHCP сервера, WireWall, и многое другое что может быть реализовано в реальных моделях маршртизаторов.

Для работы с беспроводной сетевой картой, компьютеры должны быть оборудованы соотвествующими адаптерами. Для того, чтобы оснастить компьютер беспроводным адаптером для этого нужно (рис 15.3):

Рисунок 15.3. Имитатор адаптера

1. Отключить устройство нажав на соответсвующую кнопку
2. Удалить сетевой адаптер путём его перемещения в списоку стройств
3. Выбрать тип адаптера Linksys-WMP300N
4. Переместить выбранный адаптер на место удалённого

После выше упомянутых действий, компьютеры должны автоматически подключиться к беспроводному адаптеру и будут готовы к работе.

Особенностью Packet Tracer является возможность имитации сети в её физическом исполнении, т.е можно имитировать физическое расположение компьютеров в кабинете офиса, в здании, городе, районе.Для переключения в этот режим нужно перейти на вкладку Physical, находящуюся слева вверху.

Там соответсвенно можно будет расставить объекты, согласно реальному расположению их в сети. Это особенно актуально для имитации моделей, в которых присуствуют беспроводные вычислилительные сети.

Задания

1. Создать локальную вычислительную сеть из нескольких подсетей с DHCP сервером
2. Путём симуляции «реального времени» произвести проверку работоспособности сети
3. Произвести анализ поведения сети, в которой есть DHCP и статические адреса

Контрольные вопросы:

1. Для чего предназначен маршрутизатор
2. Что такое таблица маршрутизации
3. В каких случаях используется динамическая адресация
4. Какие настройки передаются через DHCP сервер
5. Можно ли в сети, где используется DHCP сервер, использовать статическую адресацию вычислительных устройств

Литература:

Осн. 5[78-84]

Список литературы

Основная:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2000.- 672с.
2. Гук М. Аппаратные средства локальных сетей. Энциклопедия - СПб.: Питер, 2000. - 576с.
3. Microsoft Corporation. Компьютерные сети. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки: Пер. с англ. — 2-е изд., испр. и доп. - М.: Издательско-торговый дом «Русская редакция», 1999-576 с.
4. Технология корпоративных сетей. М. Кульгин. – СПб ПИТЕР, 1999
5. Справочная система по пакету Packet Tracer 5.0

Дополнительная:

1. Нанс Б. Компьютерные сети: Пер. с англ.- М.: Бином, 1996. - 400с.
2. Андэрсон К., Минаси М. Локальные сети. Полное руководство: Пер. с англ. - К.: ВЕК+, М.: ЭНТРОП, СПб: КОРОНАпринт, 1999 - 624 с.
3. Оглтри Т. Модернизация и ремонт сетей. Учебное пособие - М.: Издательский дом «Вильямс», 2000.- 928с.

Содержание