Общее описание работы

Данная лабораторная работа предназначена для приобретения практического опыта в области беспроводных локальных вычислительных сетей (WiFi LAN). Также предлагается ознакомится с возможностями рутера фирмы 3Com. Работа построена по принципу от простого к сложному, где в первом задании предстоит собрать простейшую беспроводную сеть, а в последнем объединить несколько сетей между собой и предоставить им доступ в Интернет.

Перечень оборудования

- 3 персональных компьютера с операционной системой Windows 2000 Pro
- WiFi Маршрутизатор 3Com
- Маршрутизатор Prestige 334
- Соединительные провода

Теоретические основы работы

Общие положения

Ожидается, что Вами проделана первая лабораторная работа, и Вы обладаете знаниями и навыками, предусмотренными той работой. Поэтому в данном руководстве не описывается материал касательно базовых средств настройки и диагностики ЛВС, а также материал, описывающий само существо ЛВС. Если Вы чувствуете себя неуверенно, обратитесь к теоретическим основам первой работы.

Об особенностях WiFi сетей

Беспроводные сети по своей функциональности очень схожи с обычными проводными сетями, однако существует несколько отличий, которые необходимо держать в голове.

Во-первых, рассмотрим AdHoc вариант беспроводной сети. Аналогом данной топологии в проводных сетях будет кроссоверное (нуль-хабное) соединение. Особенность состоит в том, что в AdHoc сети можно объединить более двух компьютеров. Для создания AdHoc сети один компьютер выбирается сервером и средствами утилиты поставляемой с сетевым адаптером включается функция точки доступа (Access Point). Остальные компьютеры подключаются к «серверу» как клиенты. При этом «сервер» также подключается сам к себе в качестве клиента.

Во-вторых, проблемы ограничения доступа в WiFi сетях стоят более остро, чем в проводных. В самом деле, если для подключения к проводной сети необходимо добраться до сетевой розетки и установить физическое соединение с помощью кабеля, то для WiFi сети достаточно просто попасть в зону действия точки доступа. Таким образом, если Вы установили незащищенную WiFi сеть у себя в квартире, то ваши соседи также смогут к ней подключиться. Для ограничения доступа применяется два базовых метода: ограничение по MAC адресу, и шифрование (Все это настраивается в рутере). MAC адрес сетевого адаптера легко узнать с помощью команды “IpConfig /all”. Этот адрес устанавливается на заводе и является уникальным. По поводу шифрования следует отметить, что существует несколько вариантов настройки этой опции. В том числе и такой, где ключ шифрования передается клиенту по запросу (то есть любой может запросить этот ключ и подключиться к сети (это нужно, например, во время процесса настройки сети)).

И, наконец, проблемы среды передачи данных. Имеются в виду не погодные условия ухудшающие качество связи, а выбор канала передачи данных. Для создания новой WiFi сети не следует выбирать канал, который уже используется сетью, в зоне

действия которой Вы находитесь. В лабораторной работе не следует выбирать каналы 7 и 11 (используются Институтом Автоматики). Оценить степень помех в сети при использовании одного канала двумя сетями Вы сможете при построении AdHoc сети, поскольку утилита адаптера для настройки такой сети не предоставляет возможности выбора канала (имеется в виду модель WiFi адаптера, применяемая в лабораторных работах).

О маршрутизации

Когда хост PC1 посылает что-либо хосту PC2, и оба они принадлежат одной и той же подсети, то пакеты между этими хостами проходят «напрямую». Если же 2 хоста не принадлежат одной и той же подсети, они не могут обмениваться данными непосредственно, а обращаются, вместо этого, к маршрутизатору (router). Router имеет «таблицу маршрутизации», в которой записано, какой пакет куда посылать. Каждый рутер имеет ограниченное представление о своем сетевом окружении, таким образом, он не хранит в себе информацию о целой всемирной сети (это практичеки невозможно). Вместо этого рутер имеет Default Gateway – адрес рутера высшей иерархии, которому отсылаются все пакеты, которые не могут быть посланы, используя собственную таблицу маршрутизации.

Существует специальный протокол (RIP – Routing Information Protocol), с помощью которого записи автоматически добавляются (и удаляются) в таблицу маршрутизации. Тем не менее, иногда приходится работать с таблицей маршрутизации (Route Table) вручную. Запись в route table состоит из 4 элементов.

1) Сеть назначения – IP адрес сети, куда в конечном итоге должен попасть пакет (например: 192.168.1.0 – последний ноль означает «сеть», а не один компьютер)
2) Маска подсети – маска подсети сети назначения – определяет размер сети назначения (например 255.255.255.0=254 компьютера, 255.255.255.224=30 компьютеров)
3) IP Шлюза – IP адрес компьютера в подсети отправителя, через который пойдет пересылка.
4) Метрика – целое число указывающее, сколько шлюзов должен пройти пакет пока не достигнет сети назначения (имеет смысл приоритета при пересылке пакетов: 1-наивысший приоритет, 15 - низший).

Несколько примеров записей в таблицах маршрутизации представлено ниже

Nr	Destination IP	MASK	Gateway IP	Metric
1	192.168.1.0	255.255.255.0	192.168.1.1	1
2	192.168.3.5	255.255.255.255	192.168.1.1	2
3	192.168.2.0	255.255.255.0	192.168.1.2	2
4	122.133.0.0	255.255.0.0	194.126.115.32	5

Таблица 1. Примеры записей в таблицах маршрутизации

Согласно первой записи, все пакеты из сети 192.168.2.0/?* (мы не знаем величину сети 192.168.2.0, для простоты предположим 255.255.255.0), которые предназначены для компьютеров сети 192.168.1.0/24* будут направляться в шлюз (192.168.2.1/192.168.1.1). Шлюз имеет как минимум два интерфейса (2 сетевых адаптера). Поскольку таблица маршрутизации хранится внутри шлюза, то значение Gateway IP=192.168.1.1 (все пакеты, пришедшие в шлюз для сети 192.168.1.0, должны быть направлены в интерфейс 192.168.1.1). Если бы таблица маршрутизации хранилась в компьютере внутри сети

* маска подсети может записываться двумя способами: аналогично IP адресу: 255.255.255.0 и обычным числом н-р: 24. Эти варианты эквивалентны. Метка в виде числа имеет смысл количества бит со значением единицы, в маске. Поскольку маска состоит из 4 октетов, то всего для записи маски используется 4*8=32 бита. Таким образом, в маске 255.255.255.255 все 32 бита равны единице, иными словами такая маска = 11111111. 11111111. 11111111. 11111111. Напротив маска 128.0.0.0 = 10000000.00000000.00000000. 00000000 = 1 в численном представлении.

192.168.2.0, то значением Gateway IP был бы интерфейс шлюза, «смотрящий» в эту сеть (192.168.2.1). Метрика «1» указывает на то, что этот шлюз непосредственно соединен с сетью назначения (192.168.1.0). Таким образом, все компьютеры, принадлежащие сети 192.168.2.0/24 смогут посылать пакеты компьютерам сети 192.168.1.0 (но не наоборот). Для обратной связи нужно добавить еще одну запись: «*route add –p 192.168.2.0 mask 255.255.255.0 192.168.2.1*», При условии, что интерфейс шлюза 192.168.1.1/192.168.2.1 в сети 192.168.2.0/24 имеет IP адрес 192.168.2.1. Представленный синтаксис команды добавления маршрута (“route add”) используется для работы из командной строки. В лабораторных работах используются рутеры с Web интерфейсом конфигурирования, благодаря чему в использовании командной строки нет необходимости.

Вторая строка таблицы1 описывает маршрут из сети 192.168.2.0/? к конкретному компьютеру сети 192.168.3.0/? с IP адресом 192.168.3.5 (на конкретный компьютер указывает значение маски 255.255.255.255). В данном примере сеть 192.168.3.0/24 находится за шлюзом 192.168.1.2/192.168.3.1 (то есть пакет из сети 192.168.2.0/24 в сеть 192.168.3.0/24 должен пройти через промежуточную сеть 192.168.1.0/24).

Третья строка описывает обратный маршрут из сети 192.168.3.0/? в сеть 192.168.2.0/24 через еще одну промежуточную подсеть.

Ход работы

Часть 1
Задание: Собрать AdHoc вариант сети из двух компьютеров (см рис1).
Уточнение: Продемонстрируйте руководителю работой процесс передачи файла по сети с одного компьютера на другой.
Уточнение: Ответьте на вопрос, можно ли соединить в одну AdHoc сеть более двух компьютеров (В другой группе есть еще 2 компьютера с картами WiFi).
Уточнение: В качестве SSID и WiFi канала используйте название и номер вашей группы соответственно.

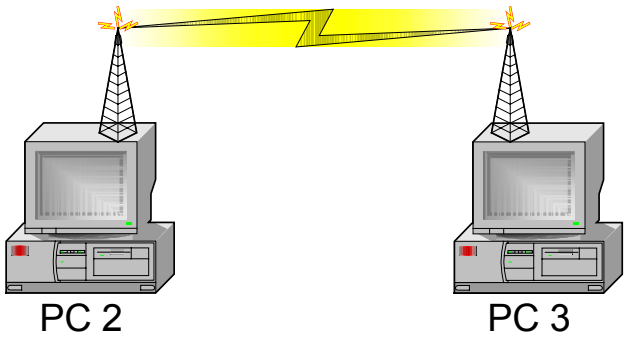

Рис. 1 AdHoc сеть

Часть 2
Задание: Собрать более сложный вариант сети согласно топологии рисунка 2
Уточнение: При выборе канала в настройках WiFi рутера 3Com не использовать каналы 7 и 11.
Уточнение: Договоритесь с другой группой о выборе каналов (или включите соответствующую опцию рутера)

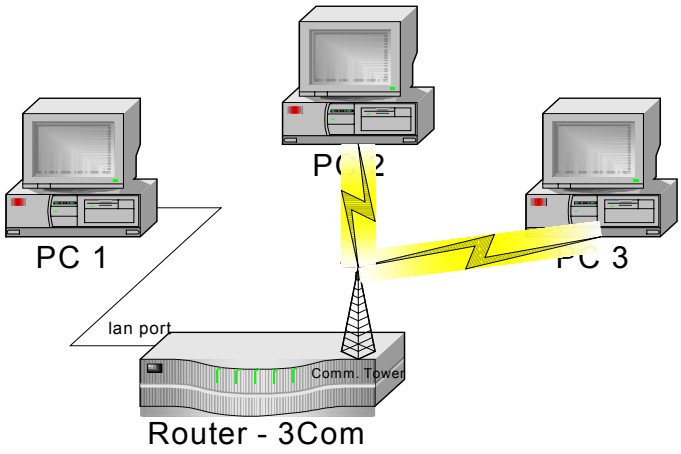

Рис. 2

Часть 3

Задание: Настроить сеть предыдущей части, исключив доступ неавторизированных компьютеров. Изучить возможности WiFi маршрутизатора 3Com по ограничению доступа.

3.1 Настройте URL фильтр аналогично первой лабораторной работе.

3.2 Настроить права доступа запретив PC1 доступ везде (в том числе и в локальной сети), PC2 должен получить доступ только к HTTP ресурсам, PC3 должен быть ограничен только URL фильтром.

3.3 Настройте доступ к Apache из внешней сети используя топологию рис2. переключив PC2 на wan порт рутера.

Часть 4

Задание: подключить сеть к Интернет согласно топологии рисунка 3.1 и 3.2

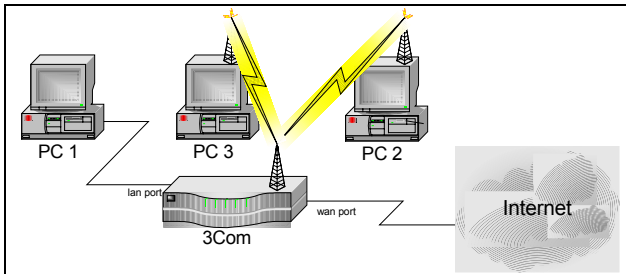

Рис. 3.1

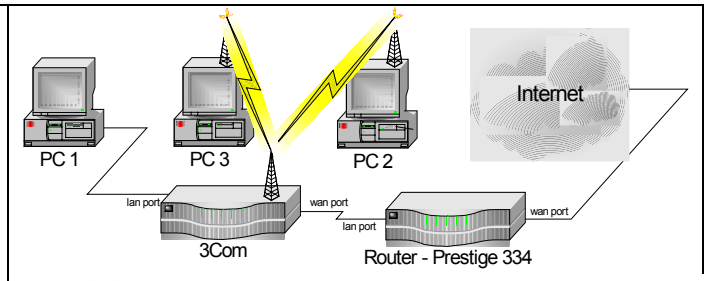

Рис. 3.2

Часть 5

Задание: Настроить сеть (см рис 4) таким образом, чтобы PC1 «видел» PC2.

Подсказка: В данном случае PC1 представляет собой Интернет. Значит рутеры надо настроить так, чтобы компьютеры внутренней сети были видны извне.

Подсказка: Возможно придется внести изменения в таблицу маршрутизации

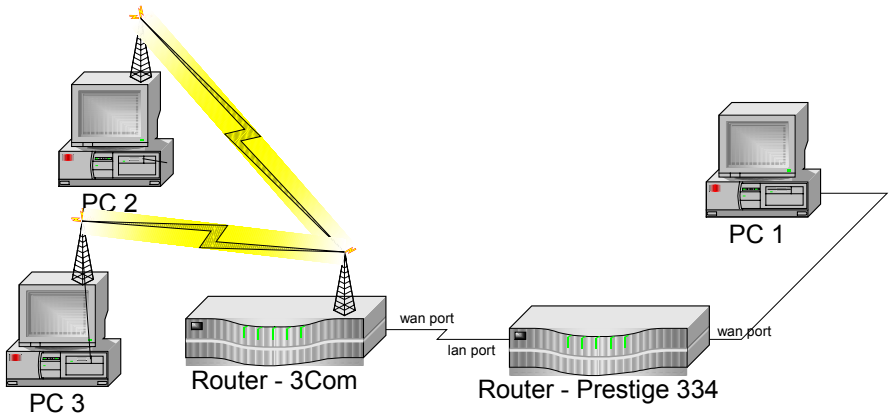

Рис. 4

Часть 6.
Задание: Объединить сети обеих групп в одну и подключить эти сети к Интернет (см. рис5).
Уточнение: Компьютеры подсети I должны «видеть» компьютеры подсети II и наоборот

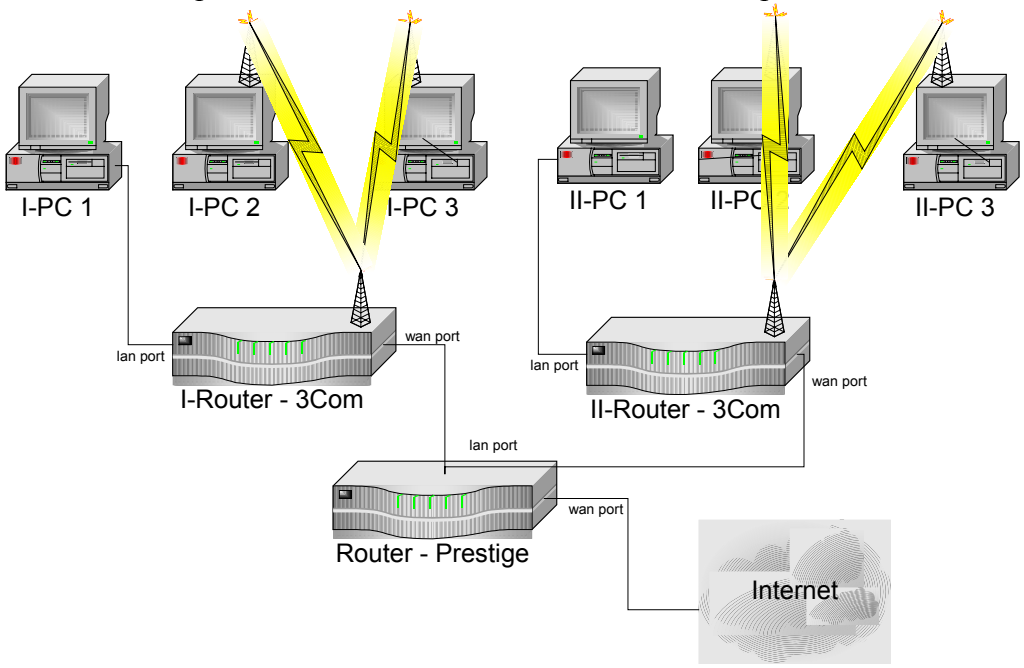

Рис. 5 Объединение сетей

Часть7. Напишите отчет о проделанной работе, аналогично отчету к первой лабораторной работе.

Для подготовки работы использованы следующие материалы:

1) Что такое маршрутизация и как она конфигурируется?, Февраль 2005, http://winfaq.com.ru/winnt/693.htm