Tallinna Tehnikaülikool
Automaatikainstituut
Automaatjuhtimise ja süsteemianalüüsi õppetool

Õppeaine: ISP0041 Arvutivõrgud

Laboratoorse töö: Ethernet LAN

Aruanne

Üliõppilane: XXX

Õppejõud: Rein Paluoja

Tallinn 2007

Общее описание работы

Данная лабораторная работа предназначена для освоения базовых знаний по проектированию и построению локальных вычислительных сетей стандарта Ethernet. В ходе работы студентам предоставляется возможность собрать простейший вариант сети, соединив вместе два компьютера под управлением операционной системы Windows. Далее, в топологию сети добавится маршрутизатор (router) со встроенным коммутатором (switch) на 4 порта, что позволит подключить сеть к Интернет и изучить возможности маршрутизатора по настройке функционирования сети.

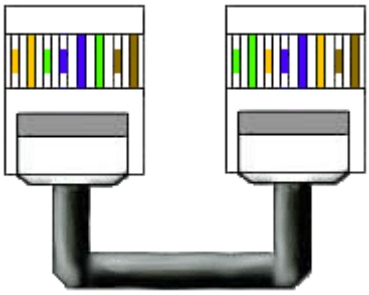
Перечень оборудования

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

Ход работы

1. Собрать одноранговую сеть из 2 компьютеров не используя хаб (hub).

Для соединения 2 компьютеров без коммутатора мы использовали кабель типа кроссовер.



Помимо этого на компьютерах должны стоять сетевые карты, позволяющие соединять компьютеры через гнёзда RJ-45 в локальную сеть.

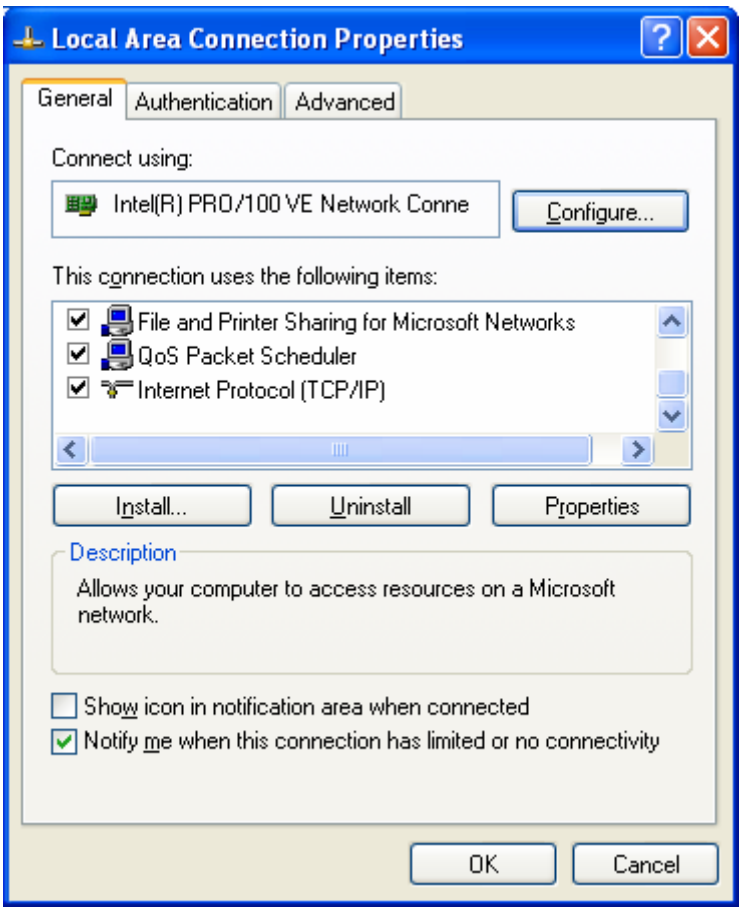
После того как мы выбрали и соединили нужный кабель, мы приступили к настройке операционной системы.

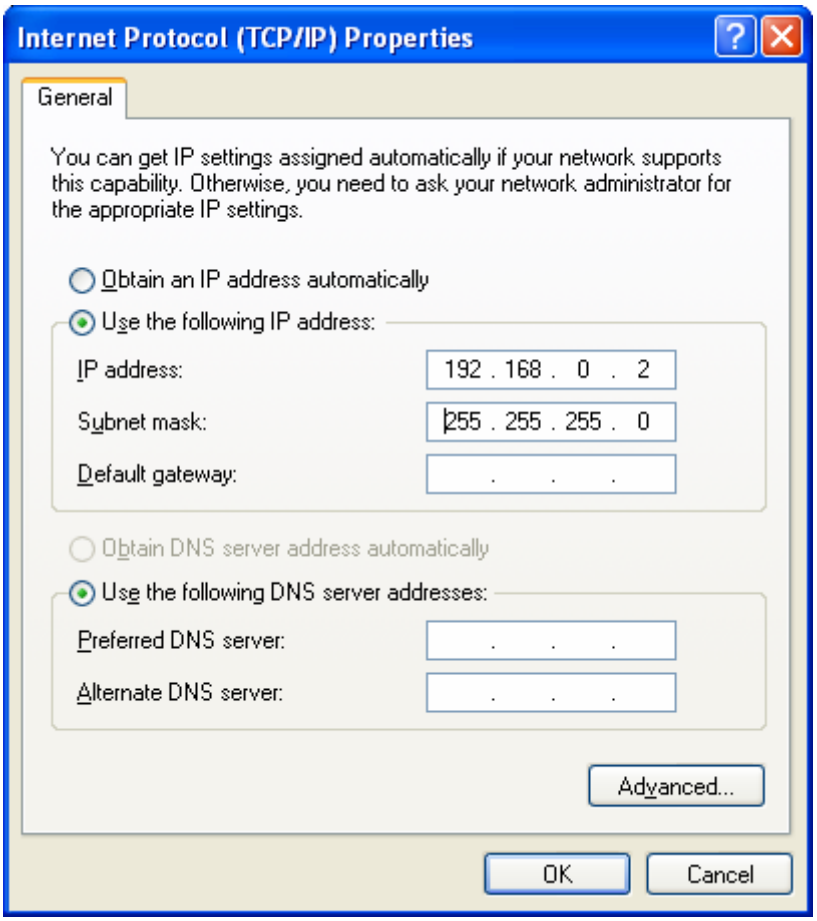
Start→Settings→Control Panel→Network and Dial-up Connections

запустили и устанавливали следующие параметры:

	IP	Mask
Компьютер 1	192.168.0.2	255.255.255.0
Компьютер 2	192.168.0.3	255.255.255.0

IP выбирали из предложенного пула по соображениям, что для локальных сетей отведен диапазон IP-адресов 192.168.X.X – класс C (где X есть число от 0-255). Для нашей цели важно, чтобы IP отличался у разных машин последней цифрой. Преднамеренно начали с 2, т.к. предполагали, что IP адрес рутера есть 192.168.0.1. Маска подсети установилась автоматически – для локальной сети это 255.255.255.0. Маска подсети – это число, показывающее, сколько бит от начала IP отводится под адрес подсети, а сколько под собственно адрес машины. Она должна быть одинаковой на всех компьютерах локальной сети.

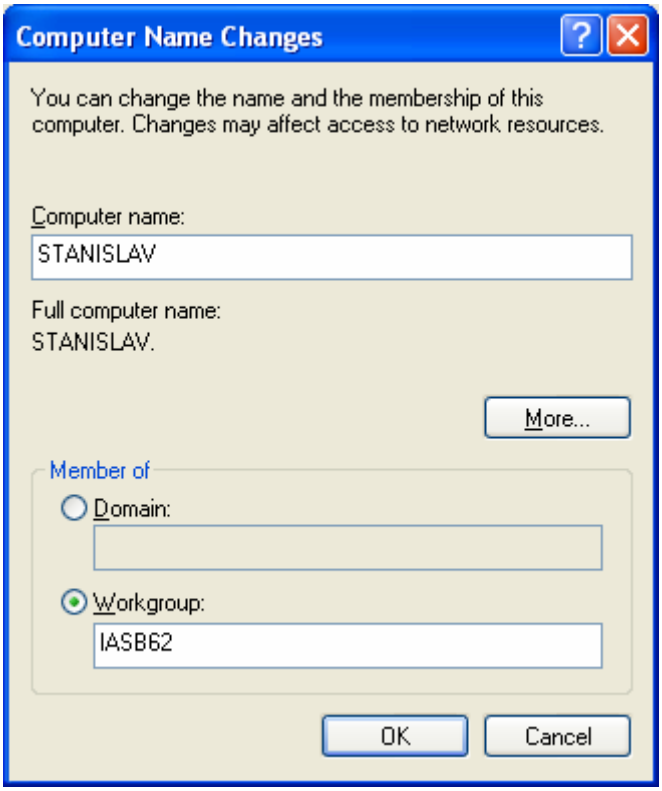

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Intel(R) PRO/100 VE Network Conne
Configure...
This connection uses the following items:
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

После этого настроили рабочую группу, в которой мы будем работать, а так же имена компьютеров для представления в сети. Важным здесь является общая группа, в которой компьютеры видели бы друг друга и смогли обмениваться файлами.

Start→ Settings→ Control Panel →System Network Identification→ Properties

Имя рабочей группы: IASB62
Имена компьютеров:
EKATERINA
STANISLAV



После перезагрузки запустили утилиты PING и IPCONFIG

IPCONFIG – показал нам параметры сети

Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.0.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Это означает, что мы успешно присвоили IP нашим компьютерам.

PING - посылает пакеты на заданный адрес и приводит статистику пересылки
Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=64
Reply from 192.168.0.3: bytes=32 time<1ms TTL=64
Reply from 192.168.0.3: bytes=32 time<1ms TTL=64
Reply from 192.168.0.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Тем самым мы убедились, что соединение установлено, пакеты доходят до адресата, потерь нет. Остался последний этап – создать и предоставить в общее пользование папку TestShare.

New = >> Folder
Folder properties =>> Sharing =>> Share this folder

2. Собрать и настроить одноранговую сеть более чем из 2 компьютеров.

Третий компьютер также подключаем к локальной сети с именем *IASB62*

Заранее мы не знали, какой IP адрес у рутера, чтобы узнать его, включили автоматическое присвоение IP нашей сетевой картой и запустили утилиту IPCONFIG. Так как компьютер уже подключен к рутеру, то он сразу определил, что:

LAN IP Address. . . . . : 192.168.0.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

Default Gateway и был искомым адресом. Для того, чтобы зайти в настройки рутера, мы набрали http://*192.168.0.1* в браузере.

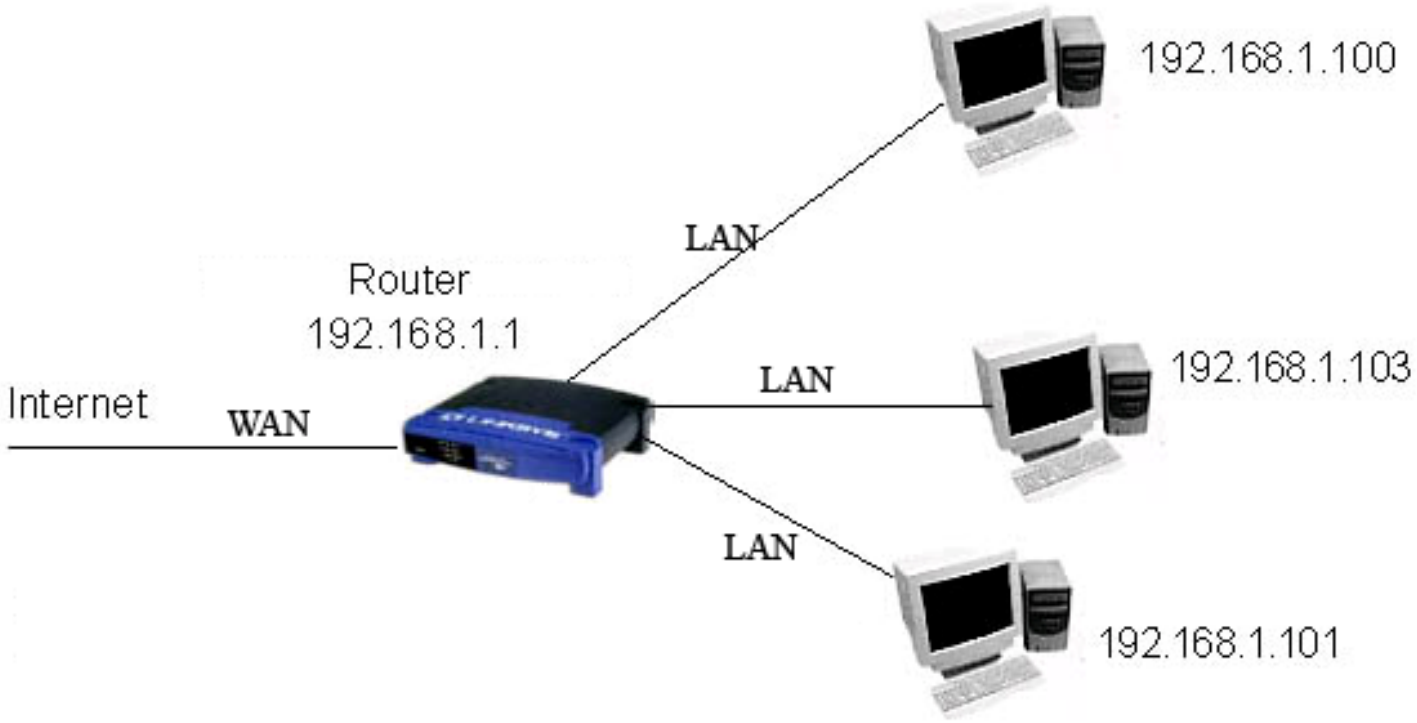
Все настройки для получения Интернет соединения сделали в рутере. Прописали новый WAN IP адрес, маску подсети, шлюз по умолчанию и DNS, чтобы мы могли обращаться к Интернет ресурсам не по адресу, а по имени домена. WAN IP адрес это внешний IP нашего рутера.

WAN IP Address. . . . . : 192.168.0.94
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DNS . . . . . .: 193.40.240.3

Для клиентских машин основной шлюз будет отличаться от рутера. Если *Default Gateway* это адрес устройства, которой знает дорогу в Интернет, а роль такого устройства выполняет у нас рутер, то на трёх имеющихся компьютерах мы прописали именно его IP адрес - *192.168.0.94*

На этом этапе у нашей группы перестал работать DHCP сервер и нам пришлось использовать другой рутер.

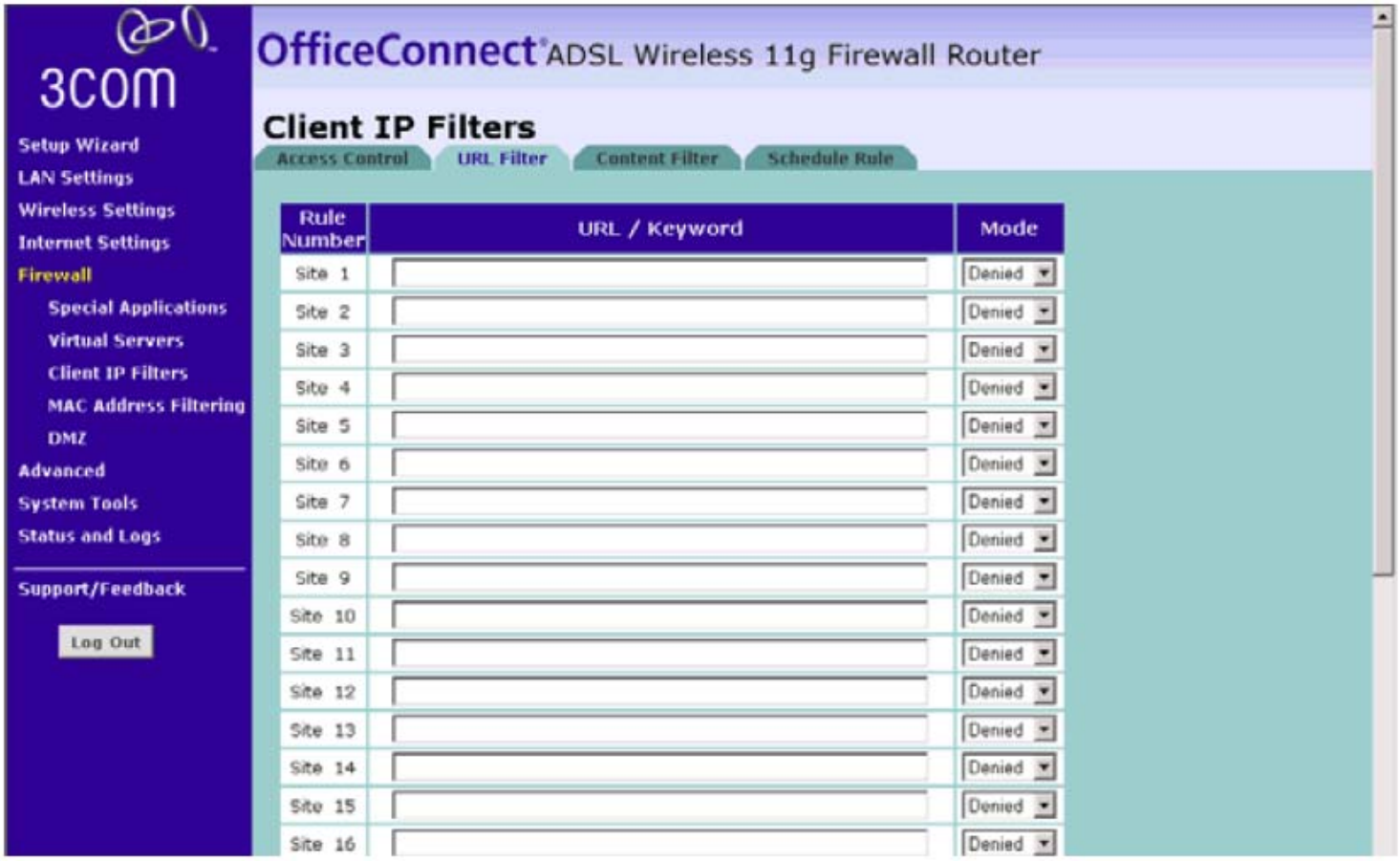
После продолжительных баталий удалось установить LAN IP нового рутера, он же являлся основным шлюзом – *192.168.1.1*
На нём заново сделали все настройки WAN-порта.



DHCP исправно работал, все компьютеры имели доступ к Интернету.

3. Ознакомиться с возможностями рутера по обеспечению безопасности и разграничению доступа.

Чтобы запретить доступ к некоторым сайтам, мы воспользовались дополнительными возможностями рутера.

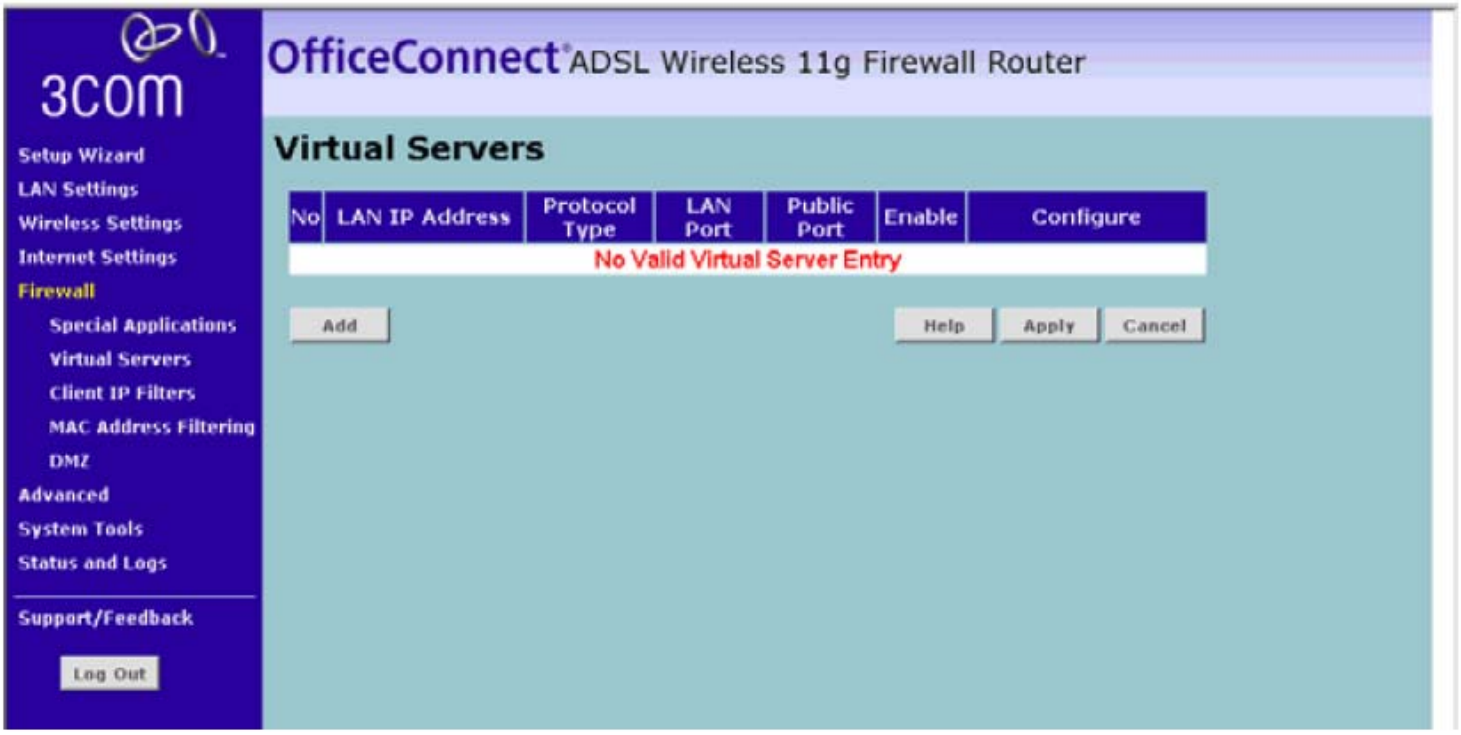


В одной из вкладок настроек рутера нашли URL-Filter, который позволяет ограничить доступ к определённым сайтам:
www.hot.ee и www.neti.ee
После чего добавили один Trusted Computer, на который ограничения не действуют. Сделали это, прописав адрес нужного компьютера – 192.168.1.57 в настройках рутера.

Для того чтобы настроить доступ из внешней сети к web-серверу во внутренней сети нужно было первым делом соединить WAN-port рутера с выходом одного из компьютеров (PC3). В нашем случае Apache web server находился на PC1.

В папке сервера \home\localhost\ мы создали .html файл с нашими именами и в браузере проверили работоспособность сервера, набрав http://localhost. Результатом было изображение наших имён на экране – это означало, что сервер работает. Чтобы он был виден не только в локальной сети, но и за её пределами, мы настроили *Virtual Server*:

В настройках **Firewall =>> Virtual Server =>> ADD** ставим IP компьютера с web-сервером 192.168.1.40, на который будет перенаправляться весь трафик. Указываем порт, которым будем пользоваться для входа из внешней сети.



Далее мы сделали настройки сетевой карты на PC3:

IP Address. . . . . : 192.168.0.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.94

После этого ввели адрес нашего виртуального сервера – то есть внешний адрес рутера (адрес WAN-порта). Веб-сервер был виден во внешней сети.

Теперь оставалось только проверить идут ли пакеты из внешней сети на все компьютеры сети, включая веб-сервер PC1 - 192.168.1.40. Как оказалось, при пересылки, пакеты не доходили. Надо было отключить функцию NAT, которая делала всю локальную сеть видимой для внешней сети как один компьютер-шлюз.

Advanced =>> Security =>> Disable NAT

После чего сервер стал доступным для внешней сети.

Вывод: