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
- Соединительные провода

Теоретические основы работы.

Для того, чтобы данная лабораторная работа не вызвала у Вас сложностей, необходимо обладать следующими знаниями:

1) Знать чем отличается Ethernet кросс-кабель (crossover) от обычного (прямого) кабеля и для чего предназначен каждый тип кабеля.
2) Знать где устанавливаются настройки сети в Win2k (IP, NetMask, Gateway, DNS_servers, Workgroup). Также надо знать, за что отвечают эти настройки.
3) Знать как пользоваться базовыми средствами диагностики сети встроенными в Windows (для данной работы достаточно Ping и Ipconfig)
4) Знать что такое NAT, DHCP
5) Знать что такое Firewall.
6) Знать что такое web-сервер (в данной работе используется Apache) и в какой папке находится web-страница. Также Вам не помешают базовые знания HTML.
7) Знать что такое рутер (маршрутизатор) и как он настраивается (во время работы Вам будет предоставлено руководство (мануал)).

Часть необходимых знаний Вы почерпнете из данного руководства. Остальные знания могут быть получены в ходе лабораторной работы и в ходе самостоятельной предварительной подготовки (используйте Интернет и конспект лекций).

Общие положения

Локальная сеть (ЛВС) представляет собой коммуникационную систему, позволяющую совместно использовать ресурсы устройств, подключенных к сети, таких как принтеры, плоттеры, диски, модемы, приводы CD-ROM и другие периферийные устройства. Локальная сеть обычно ограничена территориально одним или несколькими близко расположенными зданиями. Каждый компьютер в составе ЛВС должен иметь следующие компоненты:

- сетевой адаптер;
- патч-кабель;
- сетевая операционная система (и/или сетевые программы).

Сетевой адаптер

Сетевой адаптер представляет собой плату (рис1), которая обычно устанавливается внутрь системного блока компьютера (сейчас в торговых точках предлагаются также USB

и PCMCIA сетевые адаптеры, которые оказываются дороже обычных). Функцией сетевого адаптера является передача и прием сетевых сигналов из кабеля. Адаптер воспринимает команды и данные от сетевой операционной системы (ОС), преобразует эту информацию в один из стандартных форматов и передает ее в сеть через подключенный к адаптеру кабель.

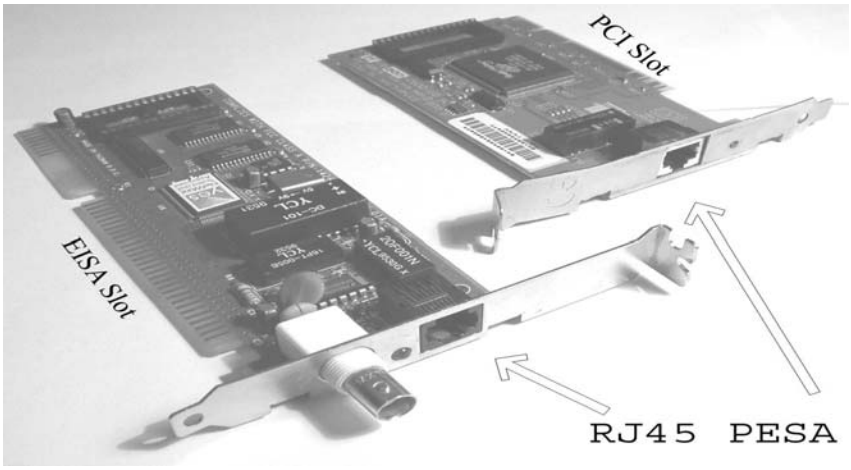

Рисунок 1. Сетевые адаптеры

Сетевой кабель

Существует три типа кабелей (витая пара, коаксиальный кабель, оптоволокно), которые могут применяться для построения сетей Ethernet. Мы будем использовать неэкранированный кабель из скрученных пар (UTP – unshielded twisted pair) или экранированный кабель из скрученных пар (STP – shielded twisted pair)

Характеристики кабеля:

- диаметр проводников 0.4~0.6 мм, 4 скрученных пары (8 проводников, из которых для Ethernet используются только 4, для Gigabit Ethernet – все 8). Кабель должен иметь категорию 3 или 5 и качество data grade или выше (на практике используется CAT5e (Category 5 enhanced) – категория 5 расширенная)
- Максимальная длина сегмента: 100 метров
- Приемлемые разъемы: 8 контактные RJ-45 (рис 2)

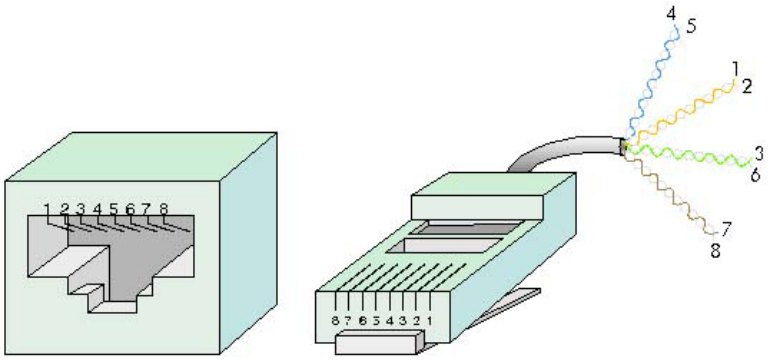

Рисунок 2. Розетка RJ-45 (слева), вилка RJ-45 (справа)

Стандарт TIA/EIA 568 A/B

Данный стандарт определяет правила обжима сетевых кабелей типа витая пара. Характеристики стандарта приведены на рисунке 3. Контакты на рисунке пронумерованы идентично контактам на вилке RJ45.

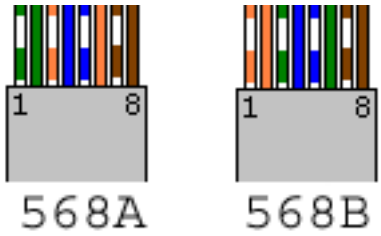

Рисунок 3. Стандарт TIA-568A/B

Расположение проводов в вилке RJ45 по стандарту TIA-568A/B.			
TIA-568A		TIA-568B	
1-	зеленый/белый	1-	оранжевый/белый
2-	зеленый	2-	оранжевый
3-	оранжевый/белый	3-	зеленый/белый
4-	синий	4-	синий
5-	синий/белый	5-	синий/белый
6-	оранжевый	6-	зеленый
7-	коричневый/белый	7-	коричневый/белый
8-	коричневый	8-	коричневый

Используя стандарт TIA-568 можно создать два типа кабелей: прямой кабель и кроссовер. Первый тип на обоих концах имеет разводку разъема типа 568A или 568B. Такой кабель применяется для соединения компьютеров с использование активных сетевых устройств (концентраторов (хабов) или коммутаторов (свичей)). Эти устройства (рис 4) коммутируют линии посылки и приема сигналов сетевых адаптеров, таким образом, снимая эти обязанности с кабельной системы.

Рисунок 4. 5 портовый свич.
(порт 1 – uplink - работает в кроссрежиме)

Рисунок 5. Ножницы для обжима разъемов RJ45, RJ11

В случае же если в сеть объединяются только два компьютера, то использование хабов представляется нецелесообразным. В этом случае применяется кроссовер (нуль-хабный провод). В таком кабеле один конец обжимается по стандарту 568A, а другой по стандарту 568B. Таким образом, линии посылки сигнала одного адаптера будут соединены с линиями приема другого напрямую.

На рисунке 5 представлен обжимной инструмент для подготовки кабеля и обжима разъемов RJ45 и RJ11 (В данной работе не используется).

DHCP

Dynamic Host Configuration Protocol – протокол для автоматической настройки клиентских компьютеров для работы в сети. Автоматически выделяется IP адрес, маска

подсети, шлюз по умолчанию (default getaway) и адреса DNS серверов. Всё это позволяет сократить время администрирования больших сетей. Во время тестовых вариантов конфигурации сети, для исключения возможных ошибок DHCP, как правило, отключают.

DNS

Domain Name System – служит для преобразования IP адресов в адреса вида: “www.ttu.ee”. В самом деле, компьютер в сети имеет только IP адрес по которому человеку обращаться неудобно. Используя же DNS сервер, который содержит таблицу соответствия доменных имен IP адресам можно обращаться к http://www.neti.ee именно так, а не по IP (http://194.126.101.67)

IP адреса

Любой компьютер в сети имеет уникальный идентификатор, по которому его можно однозначно опознать в сети. Такой идентификатор называется IP (Internet Protocol) адресом и представляет собой двоичное число из 32 бит (для IPv4). Поскольку бинарное представление числа менее удобно для человека, чем десятичное, то реальное хождение имеют IP адреса в виде 4 десятичных чисел от 0 до 255, разделенных точками. Например: «194.126.115.18». Нетрудно подсчитать, что общее возможное число IP адресов составит $2^{32}=256^4$ = 4 294 967 296.

В одной сети не может быть хостов (компьютеров) с одинаковыми IP адресами (иначе произойдет ошибка и сеть оставит подключенным только один компьютер с конфликтным IP, другие будут отключены). Таким образом, в сети Интернет каждый компьютер должен иметь уникальный IP. Проблема в том, что число компьютеров в организации часто превышает число выделенных ей IP адресов (а кроме компьютеров IP адреса имеет сетевое оборудование, например маршрутизаторы). Один из вариантов решения проблемы состоит в том, чтобы применять динамическое распределение IP (DHCP). В этом варианте только число одновременно включенных в сеть компьютеров не должно превышать число IP, общее же число компьютеров может это число превышать. Другое решение состоит в использовании так называемых приватных IP адресов.

Диапазон приватных IP (см. таблицу 1) предназначен для использования в сетях, не являющихся частью Интернет (внутренние сети организаций). Справедливости ради стоит отметить, что если сеть существует автономно (не имеет подключения к Интернет), то вы можете использовать любые IP. Однако, если автономная сеть в будущем будет подключена к Интернет (для этого применяется NAT), то использование приватного диапазона IP необходимо для исключения конфликтов. Например, возможна ситуация когда при совпадении IP адресов внутренних компьютеров и IP адресов сайтов в Интернет, при обращении к сайтам на самом деле будет происходить обращение к компьютерам внутренней сети.

Класс сети	Приватный диапазон (пул) IP адресов
A	от 10.0.0.0 до 10.255.255.255
B	от 172.16.0.0 до 172.31.255.255
C	от 192.168.0.0 до 192.168.255.255

Таблица 1. Приватный пул IP адресов

Существуют также специальные IP адреса. Адреса, оканчивающиеся на .255 не могут быть присвоены конкретному компьютеру, а применяются для массовой (broadcast) рассылки сообщений в сети. Адреса, оканчивающиеся на .0 обозначают сеть целиком (применяются в описании маршрутизации) и также не присваиваются конкретным машинам.

NAT

Network Address Port Translation – трансляцию сетевых адресов в адреса портов нередко для простоты называют просто NAT (Network Address Translation). Это, однако, не меняет сути вопроса, NAT служит для подключения к Интернет, внутренней сети через один внешний IP адрес. При этом снаружи вся сеть выглядит как один компьютер (снаружи виден только компьютер-шлюз). Помимо прочего, такое подключение обеспечивает и определенную долю безопасности, поскольку доступ к членам ЛВС напрямую неосуществим (эхо-запрос не пройдет). Это свойство позволяет подключить к Интернет практически бесконечное число компьютеров поскольку несмотря на использование в каждой отдельно взятой ЛВС одного и того же приватного пула IP, каждый компьютер общей мега сети (Интернет) не найдет ни одного компьютера с таким же IP как у него (хотя такие компьютеры существуют).

В NAT есть функция предоставления доступа к определенным услугам ЛВС, например Web-серверу. Для этого в рутере (который осуществляет NAT) прописывается пересылка (forwarding) определенных запросов из Интернет в ЛВС. Например, если адрес внутреннего Web-сервера 192.168.1.10, то, зная номер порта (для Web сервера это очевидно «80») мы можем прописать forwarding. Тогда, если внешний адрес рутера 11.11.11.11, то любой пользователь в Интернет, набрав в web-обозревателе запрос http://11.11.11.11 попадет на наш web-сервер.

Firewall

Firewall или брандмауэр служит для защиты сети или компьютера от внешних вторжений. Работает он по принципу сокетов (ограничивает доступ как по IP адресу, так и по номеру порта). Во вкладке «Firewall», рутеров, предложенных для ознакомления в ходе данного курса лабораторных работ, имеются дополнительные функции, например ограничение доступа к определенным URL адресам.

Администрирование Windows

Общие положения

В лабораторных работах применяются сетевые адаптеры стандарта PLUG-and-PLAY, которые уже установлены в данный компьютер. Поэтому инсталляция адаптера (а также установка драйверов) не требуется.

Требуется лишь настройка логического соединения, которая осуществляется в различных версиях операционной системы по-разному.

Для Windows 2000

Войдите в меню Start => Settings => Control Panel => Network and Dial-up Connections.
На экране появится окно (Приложение1 - рис 6). Кликните правой кнопкой мышки на Local Area Connection и выберите вкладку Properties. В открывшемся окне (Приложение1 - Рис 7) выберите пункт Internet Protocol TCP/IP. В открывшемся окне (Приложение1 - Рис8) настраивается конфигурация IP адреса.

Далее на вкладке Start => Settings => Control Panel => System => Network Identification => Properties (Приложение1 - Рис 9) настраивается имя рабочей группы и имя компьютера.

Доступ к папке

При наличии в системе службы доступа к файлам и принтерам для сетей Майкрософт (см Приложение1 - рис 7) станет доступной возможность предоставления доступа к файлам и принтерам вашего компьютера. Для предоставления доступа к

определенной папке (диску или другому устройству) нужно кликнуть правой кнопкой мышки на пиктограмме этой папки и в появившемся меню выбрать пункт “Sharing”.

Утилита PING

Данная утилита применяется для первичной диагностики работоспособности сети. Запустив консольное окно (для Win2k/WinXP клавиша Windows+R => CMD => Enter) и набрав “Ping” без параметров можно получить список ключей (полезным, в частности, может оказаться ключ “–t”).
Команда “Ping 127.0.0.1” произведет диагностику вашего собственного сетевого адаптера. Признаком его исправности будет ответ вида:

```
C:\Documents and Settings\Administrator>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128

Ping statistics for 127.0.0.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

И признаком его неисправности будет ответ вида:

```
Pinging 127.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 127.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Утилита IPCONFIG

Данная утилита предназначена для вывода в консольное окно информации о текущей конфигурации сетевых адаптеров в системе. Вот пример ее использования:

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : host1
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
```

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet Adapter
Physical Address. . . . . : 00-40-95-48-36-54
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.0.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DNS Servers . . . . . : 194.126.115.18
194.126.101.34

Как видно из этого примера используя данную команду можно в частности узнать текущий IP адрес данного компьютера, маску его подсети и имя хоста (имя с которым он будет виден в рабочей группе). Запустив IpConfig без параметров можно узнать список ключей (обратите внимание на ключ «/renew», который обновляет текущую конфигурацию сетевого адаптера по DHCP).

Ход работы

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

1) Выберите из предложенных проводов (патч-кордов) подходящий и соберите сеть, согласно физической топологии (рис 1).
   Подсказка: согласно стандарту TIA568 A/B существует два типа кабелей: прямой и кросс-кабель (crossover).

2) Настройте компьютеры для работы в сети.
   Уточнение: имя рабочей группы установите: _____
   имена компьютеров: _____
   _____
   _____
   Подсказка1: Нужно, чтобы компьютеры были в одной подсети, IP адреса нужно выбрать и пула приватных адресов. IP адреса придется задать вручную.
   Подсказка2: В настройке сети Вам помогут утилиты PING и IPCONFIG.

3) Передайте по сети файл с одного компьютера на другой.
   Уточнение: На компьютере-сервере, на рабочем столе, создайте и предоставьте в общее пользование папку ”TestShare”. В папке создайте текстовый файл и продемонстрируйте руководителю лабораторной работой процесс передачи файла.

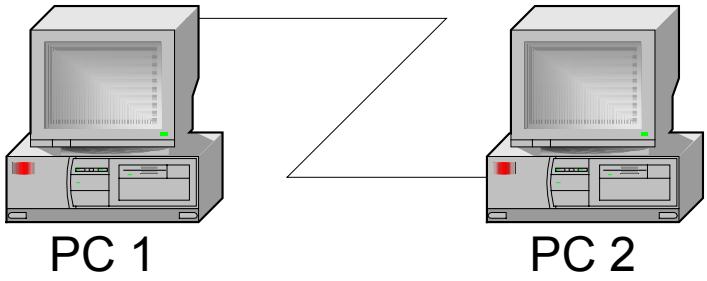

Рис 1. Простейшая сеть

Часть 2
Задание: Собрать и настроить одноранговую сеть более чем из 2 компьютеров.

1) Соберите сеть, согласно физической топологии (рис 2).
   Подсказка: Хотя порты встроенного в рутер коммутатора могут быть самонастраивающимися (MDI/MDX), все-таки принято использовать «прямые» патч-корды (TIA 568 A-A или B-B).

2) Настройте компьютеры для работы в сети.
   Подсказка1: Не рекомендуется использовать DHCP сервер рутера во время настройки сети (поскольку в этом случае конфигурация сетевого адаптера способна изменится без вашего ведома). Во время эксплуатации сети, напротив лучше переключиться на использование DHCP сервера.
   Подсказка2: Если рутер не находится в состоянии настроек по умолчанию, то подключение к нему для конфигурирования может представлять проблему (например потому, что изменен IP адрес LAN порта рутера). Для разрешения этой задачи можно сбросить настройки рутера (кнопка RESET на его корпусе) или используя DHCP получить IP адрес из подсети рутера. Это позволит предположить и IP адрес LAN порта рутера (поскольку он как правило имеет первый адрес в подсети). Также используя IPCONFIG можно узнать IP адрес шлюза по умолчания (Default Getaway), который вероятнее всего является IP адресом LAN порта рутера.

3) Подключите сеть к интернет
   Подсказка1: Придется прописать на клиентских машинах «default gateway».
   Подсказка2: Фактическое подключение к Интернет настраивается в рутере.
   Подсказка3: Для обращения к интернет ресурсам по имени домена, а не по IP адресу у клиентов должен быть доступ к DNS серверу.
   Подсказка4: адрес DNS сервера может быть найден в настройках рутера. Если Вы знаете адрес какого-либо DNS сервера, можете использовать его.

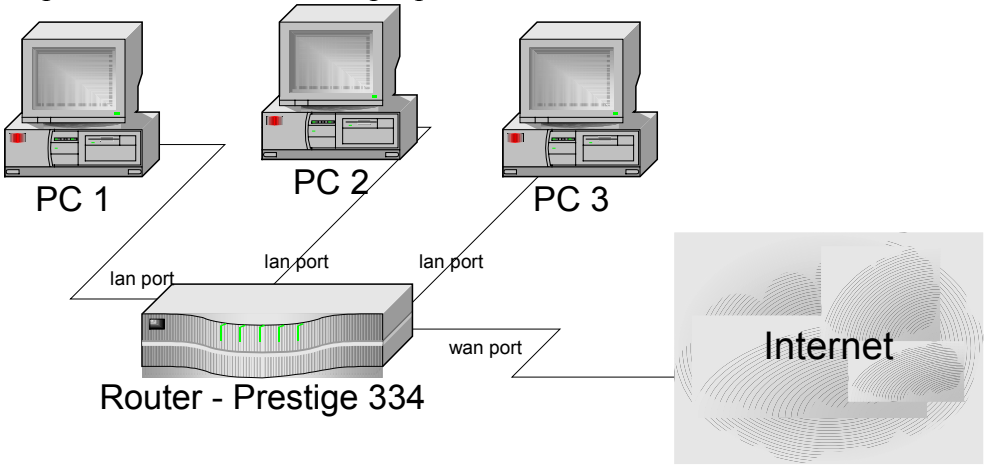

Рис 2. Типичная топология сети малого предприятия

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

1) Запретите доступ к определенным адресам URL.
Адрес1:_____
Адрес2:_____
Уточнение: Продемонстрируйте результат.
Дополнение: Сделайте один “Trusted Computer”, на который запреты не распространяются

2) Настройте доступ из интернет (внешней сети) к web-серверу во внутренней сети (см рис 3 для изменения топологии)
Подсказка: Apache web server – предустановлен на компьютер _____*PC1*_____
Уточнение: При обращении к web-серверу должна выдаваться страница с именами и фамилиями участников Вашей группы.
Подсказка: Знание HTML не требуется, требуется разместить соответствующий файл с Рабочего Стола в нужной директории Web сервера Apache.

3) Настройте сеть таким образом, чтобы все компьютеры внутренней сети были видны из внешней сети (должен проходить Ping)
Подсказка: Обратите внимание на NAT.

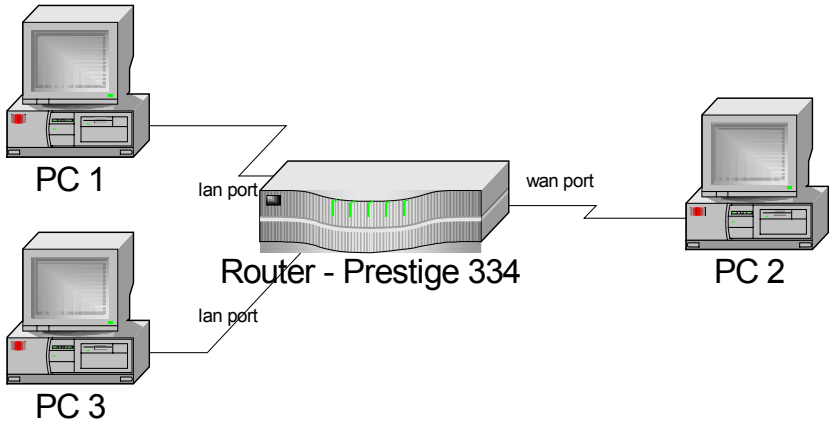

Рис 3. Топология сети для тестирования внутреннего web сервера

Часть 4
Задание: Напишите отчет о проделанной работе.
1) Опишите ход работы.
2) Ответьте на вопросы:
   - Какие, на Ваш взгляд, знания позволяет получить данная работа.
   - Какие знания Вы смогли получить.
   - Какие задания и(или) лабораторные работы можно добавить в данный курс.
   - Оцените качество данного руководства к лабораторной работе (что нужно переделать/добавить/убрать).

Для подготовки работы использованы следующие материалы:

1) Локальные сети для начинающих (на примере LANtastic), Ноябрь 2004, http://networks.hoha.ru/lokal_siti/loc_new/loc_new.htm
2) Монтаж вилки RJ-45 на кабель, Ноябрь 2004, http://www.cad.ntu-kpi.kiev.ua/~netlib/Nets/RJ45/#1421
3) Netwerk-kaarten, Ноябрь 2004, http://www.zeta.be/Info/hardware/netwerken.htm

Приложение 1

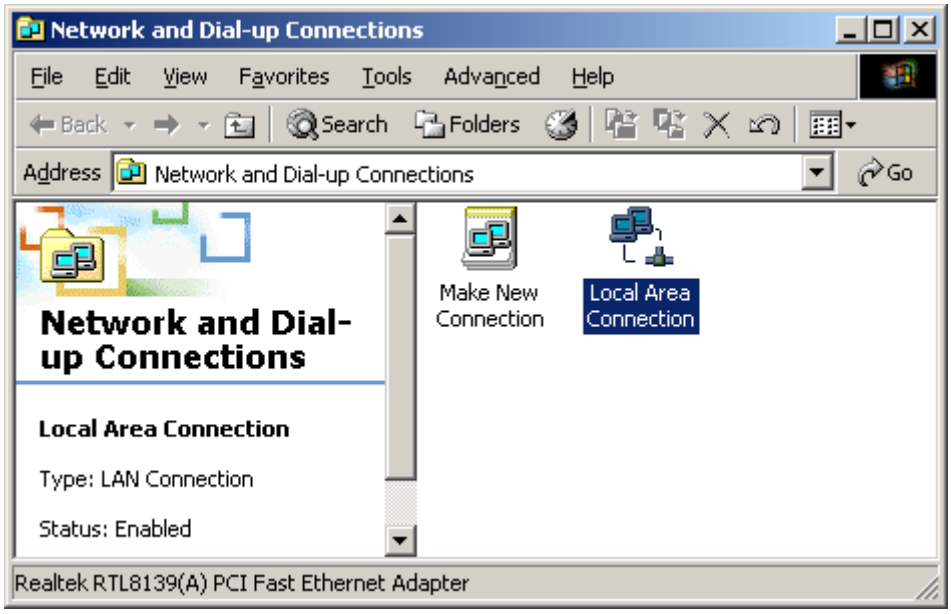

Рисунок 6. Network and Dial-up Connections

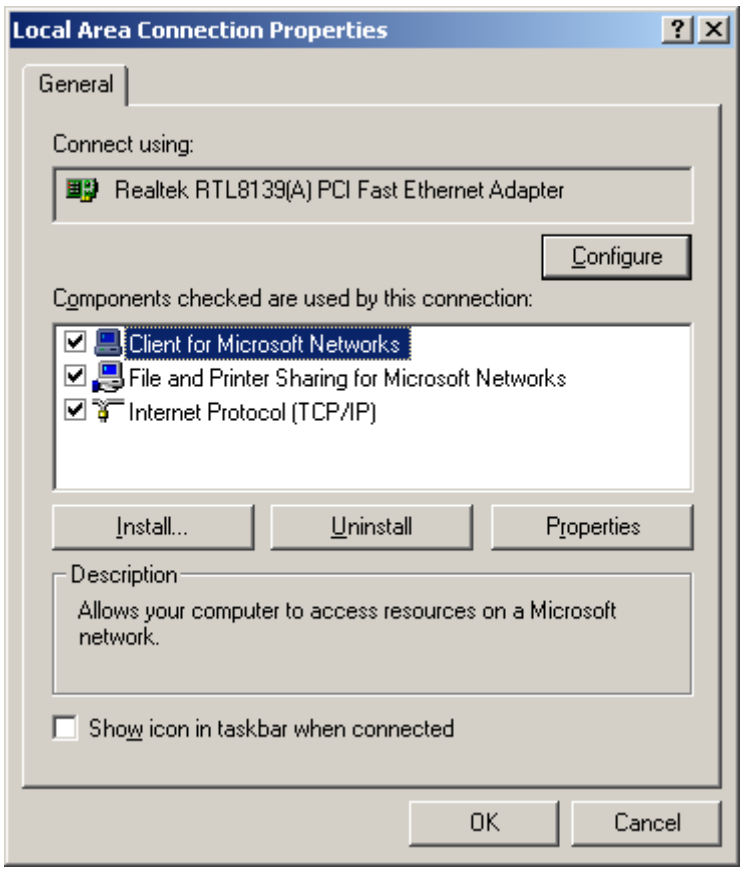

Рисунок 7. Local Area Connection Properties

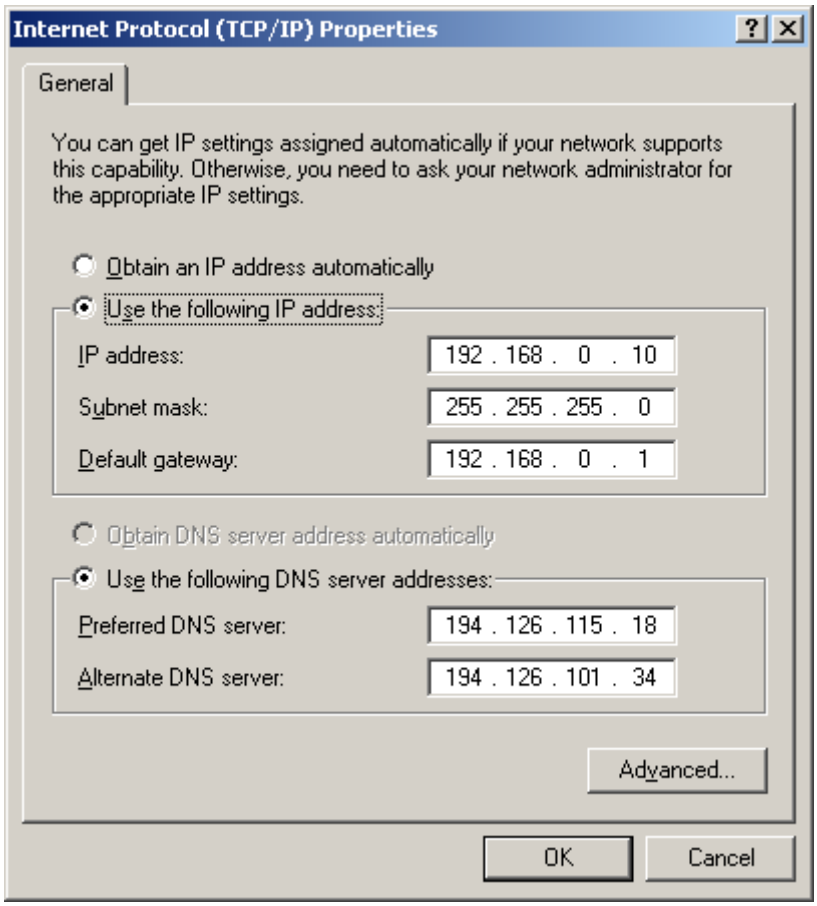

Рисунок 8. Internet Protocol (TCP/IP) Properties

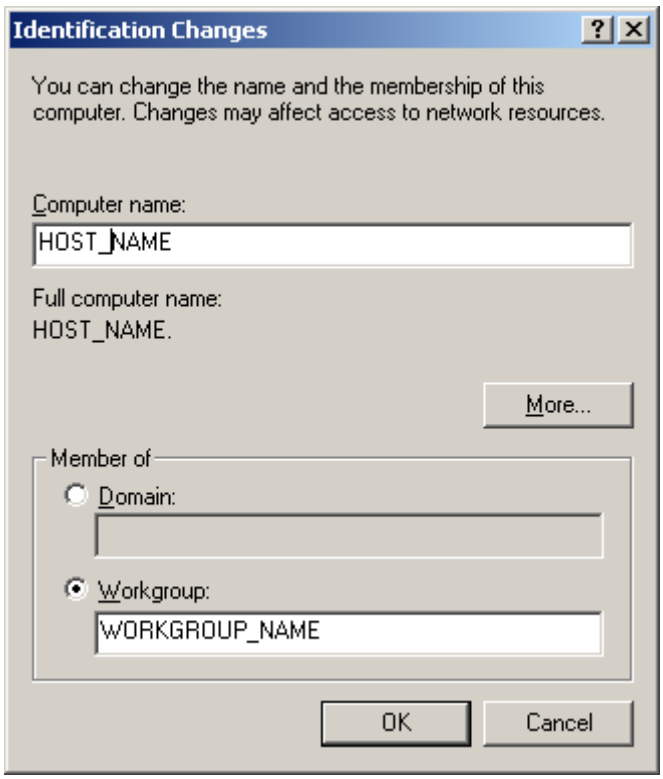

Рисунок 9. Identification changes