Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«Томский государственный университет систем управления и радиоэлектроники».
(ТУСУР)

УТВЕРЖДАЮ

Заведующий кафедрой
«Управление инновациями»

_____ /*А.Ф.Уваров*
(подпись) *(ФИО)*
"____" _____ 2011 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ЛАБОРАТОРНЫМ РАБОТАМ

по дисциплине

ОСНОВЫ КОМПЬЮТЕРНЫХ СЕТЕВЫХ ТЕХНОЛОГИЙ

Составлена кафедрой «Управление инновациями»

Для подготовки специалистов по специальности 220601.65 «Управление инновациями» и бакалавров по направлению 220600.62 «Инноватика»

Форма обучения очная

Составитель
Доцент, к.т.н. _____ Е.Ю. Агеев

Томск 2011 г.

ОГЛАВЛЕНИЕ

Программа моделирования компьютерных сетей Cisco Packet Tracer

Задачи

- Понять основные принципы работы с Packet Tracer.
- Создание/имитация простой сети Ethernet с помощью двух узлов и концентратора.
- Наблюдение поведения трафика в сети.
- Наблюдение за потоком данных широковещательных рассылок по протоколу ARP и обменов пакетами данных (ping).

Подсказка. Чтобы инструкции во время выполнении упражнения отображались, поставьте флажок «Top» (вверх) в нижнем левом углу окна с инструкциями.

На рис. 1 представлен внешний вид главного окна программы Cisco Packet Tracer.

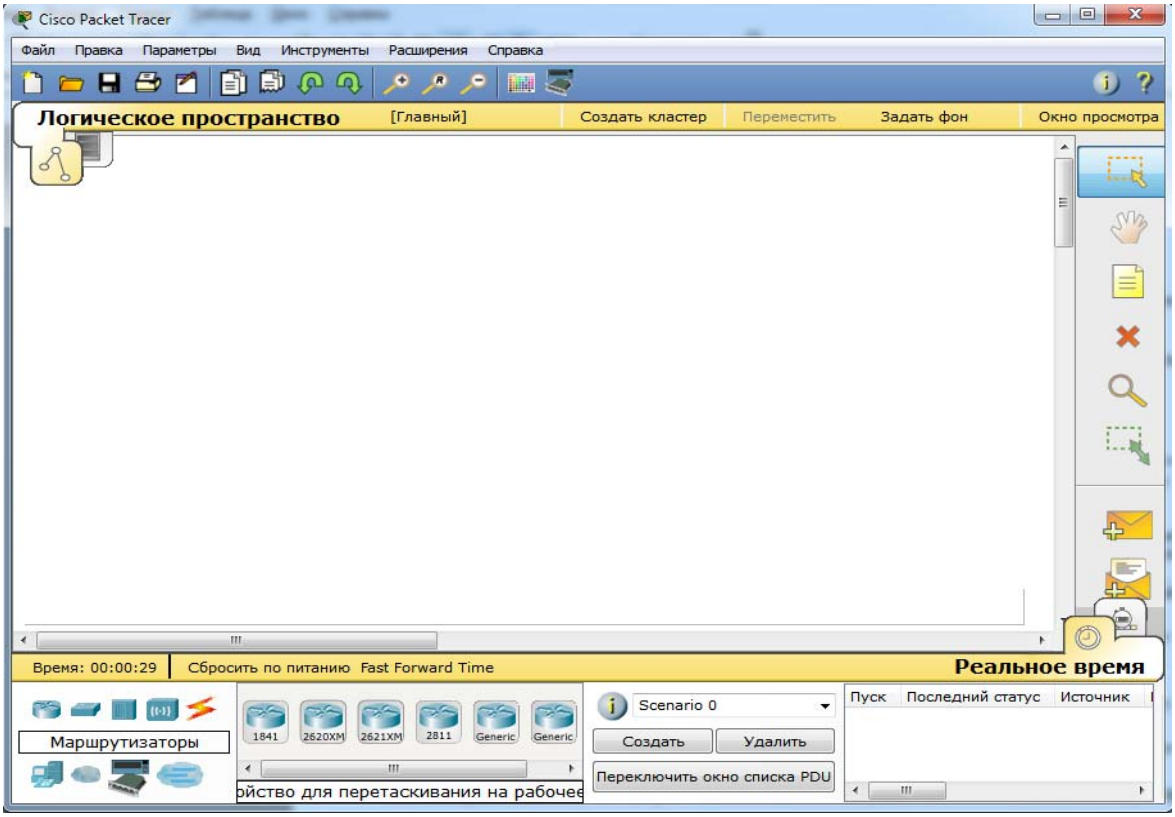


Рис. 1. Программа Cisco Packet Tracer, главное окно в режиме реального времени.

В нижнем левом углу окна Packet Tracer отображены восемь значков, представляющих категории или группы устройств и значок молнии, изображающий категорию кабельных соединений между устройствами, например, Routers (маршрутизаторы)

Switches (коммутаторы)

или End Devices (конечные устройства)

При перемещении курсора над категориями устройств отображается имя категории в окне. Для выбора определенного устройства выберите сначала категорию. После выбора категории устройств в окне справа, рядом со значками категорий появится список устройств. Выберите нужное устройство и перетащите его в основное окно логической схемы сети.
Для наглядного примера создадим логическую схему сети с двумя ПК и концентратором.

Выберите пункт End Devices (конечные устройства) из списка вариантов в левом нижнем углу. Перетащите два однотипных ПК на область проектирования сети (рис. 2).

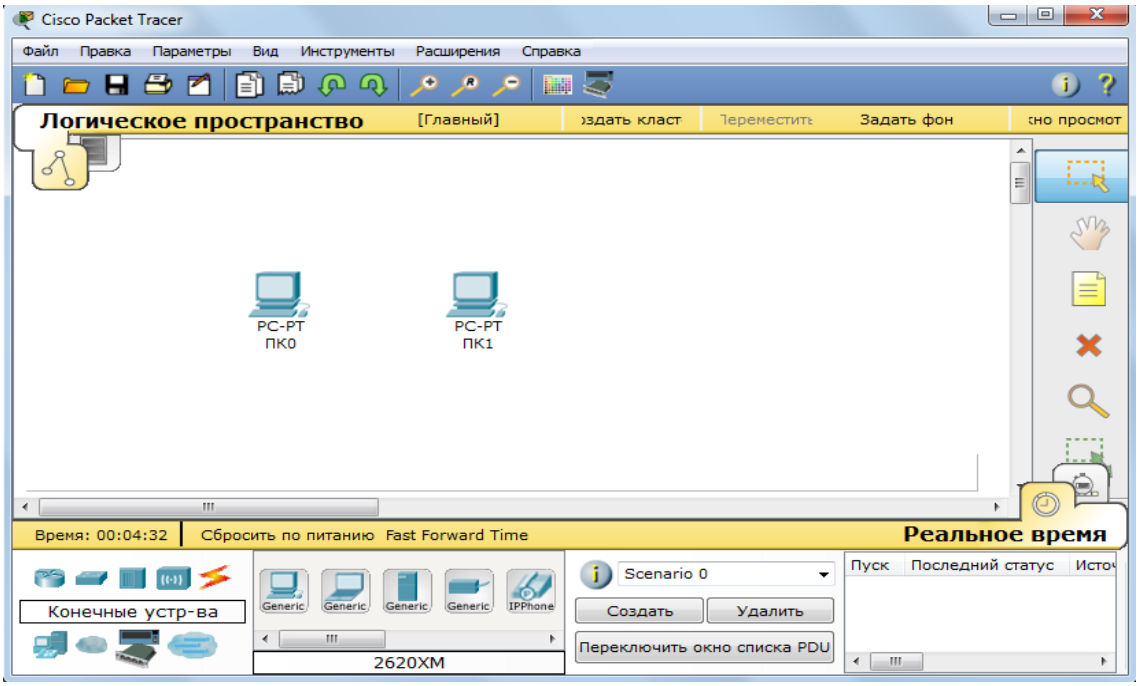


Рис. 2. Перемещение на рабочую область двух компьютеров из категории "Конечные устройства".

Выберите категорию **Hubs** (концентраторы) из списка категорий устройств в левом нижнем углу. Добавьте концентратор к прототипу сети, перетащив его концентратор на область проектирования сети (рис. 3).

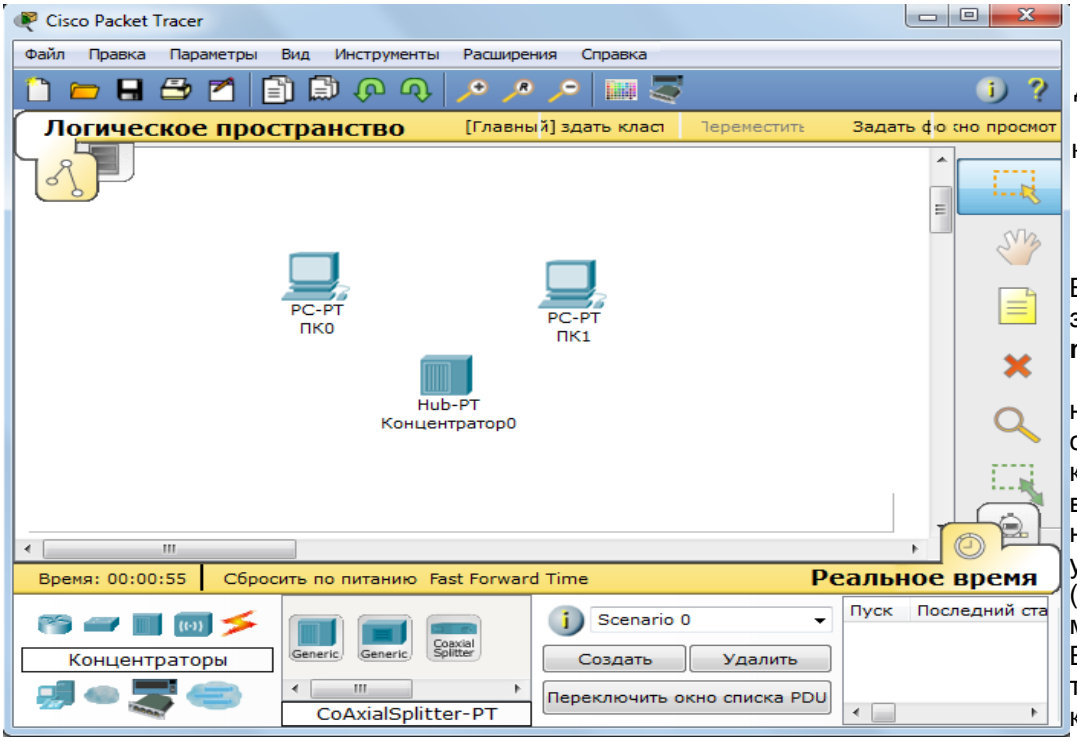


Рис. 3. Добавление концентратора в схему сети.

Выберите значок **Connections** (соединения) из списка категорий в левом нижнем углу (значок молнии). Выберите тип кабеля **Copper Straight-through** (медный прямой). Щелкните первый узел **PC0** и назначьте выбранный кабель разъему интерфейса **FastEthernet**. Щелкните концентратор **Hub0** и выберите порт соединения **Port0** для соединения с **PC0**. Повторите этот шаг для второго ПК **PC1** для его подключения к **Port1** на концентраторе (рис. 4).

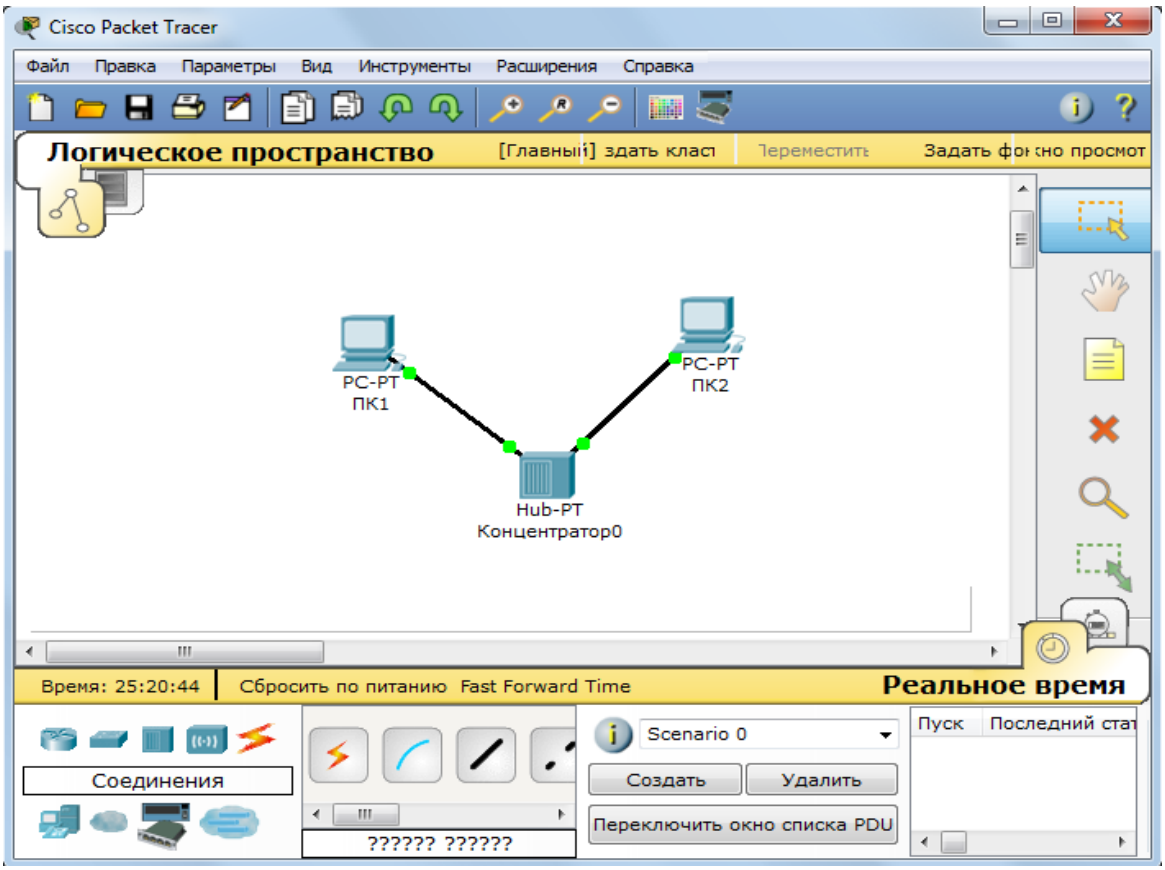


Рис. 4. Добавление соединений устройств.

*На концах кабельного соединения должны появиться зеленые точки. Они изображают состояния светодиодных индикаторов на сетевых адаптерах. Если этого не произошло, проверьте выбранный тип кабеля.

Шаг 2. Настройка имен узлов и IP-адресов на компьютерах

а. Щелкните значок PC0. Появится окно PC0.

б. В окне PC0 выберите вкладку **Config** (конфигурация). Измените **Display Name** (отображаемое имя) ПК на **PC-A** (рис. 5).

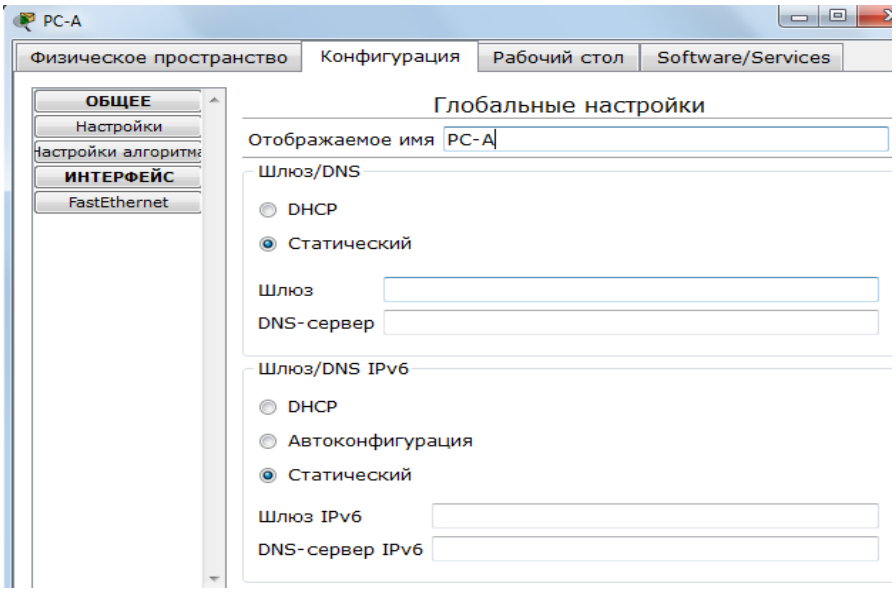


Рис. 5. Изменение имени компьютера.

Выберите вкладку **FastEthernet** слева и добавьте IP-адрес **192.168.1.1** и маску подсети **255.255.255.0**. Закройте окно конфигурации PC-A, нажав на кнопку **x** в правом верхнем углу окна (рис. 6).

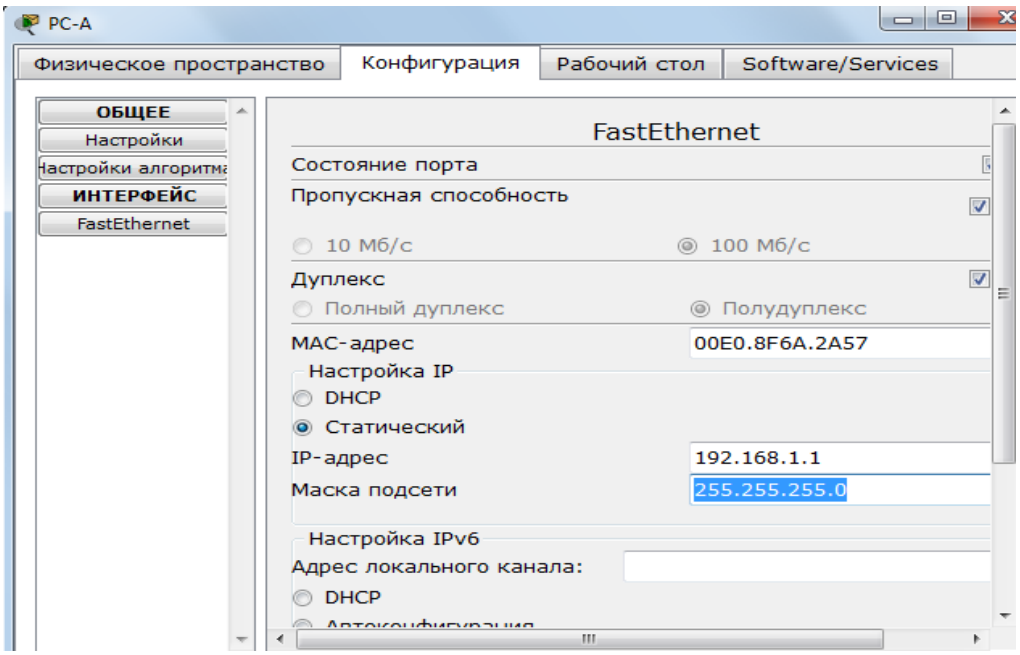


Рис. 6. Настройка IP-адреса и маски подсети.

в. Щелкните значок PC1.

г. Выполните аналогичные настройки. Выберите вкладку **Config** (конфигурация). Измените **Display Name**(отображаемое имя) ПК на **PC-B**. Выберите вкладку **FastEthernet** слева и добавьте IP-адрес **192.168.1.2** и маску подсети **255.255.255.0**. Закройте окно конфигурации PC-B.

Шаг 3. Наблюдение за потоком данных от PC-A к PC-B при создании сетевого трафика

а. Включите режим **Simulation** (моделирование), выбрав вкладку, частично скрытую за вкладкой **Realtime** (в реальном времени) в нижнем правом углу. На вкладке изображен секундомер (рис. 7).

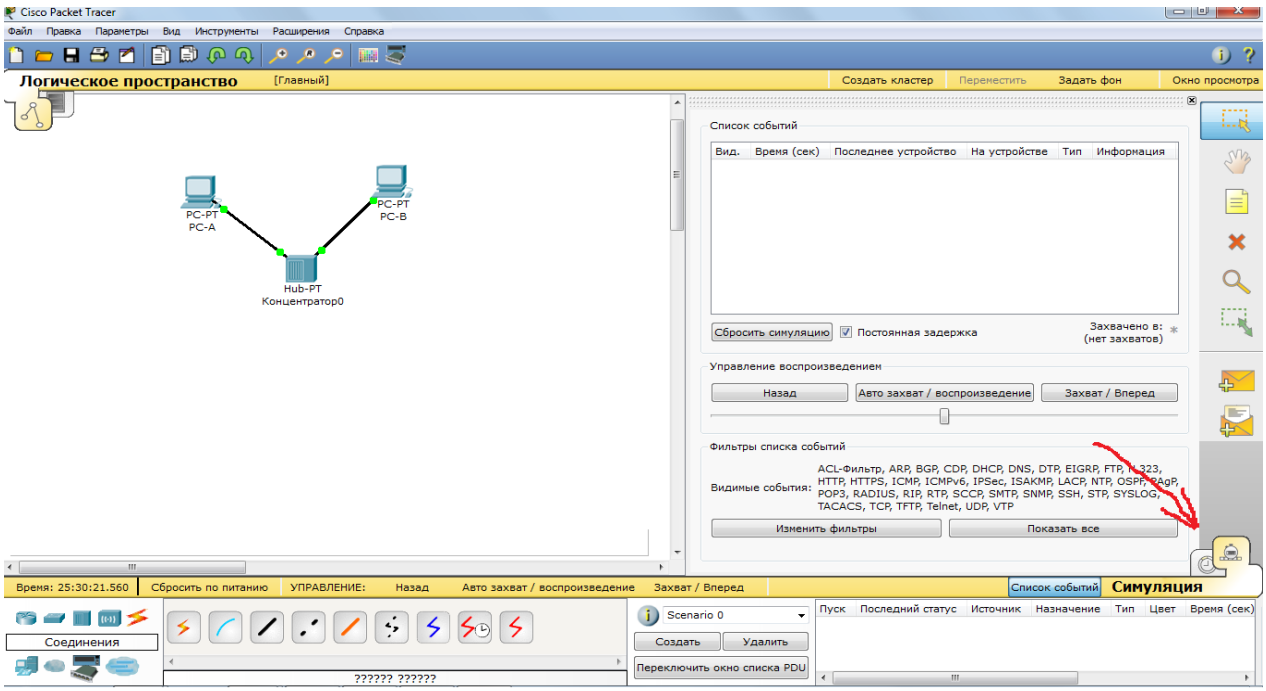


Рис. 7. Переключение в режим симуляции.

б. Нажмите кнопку **Edit Filters** (редактировать фильтры) в области **Event List Filters** (фильтры списка событий). После нажатия кнопки **Edit Filters** (редактировать фильтры) откроется всплывающее окно. Во всплывающем окне щелкните пункт **Show All/None** (показать все/ничего) для отмены выделения всех фильтров. Выберите только фильтры **ARP** и **ICMP** (рис. 8).

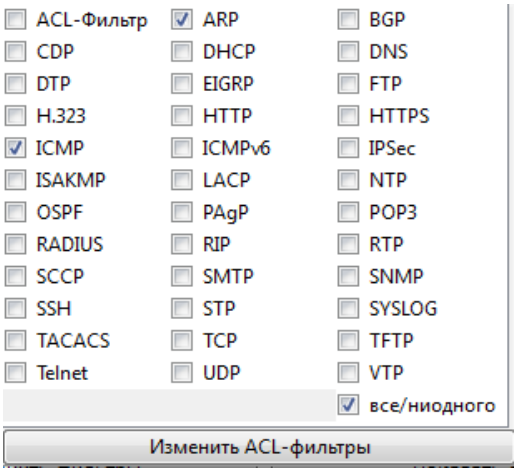


Рис. 8. Изменение настроек фильтра пакетов.

в. Выберите **Simple PDU** (простой PDU), щелкнув значок с изображением закрытого конверта на вертикальной панели инструментов (рис. 9). Переместите курсор в область отображения на экране. Щелкните **PC-A** для определения источника. Переместите курсор на **PC-B** и щелкните для определения адресата.

Рис. 9. Простой PDU.

**Обратите внимание, что два конверта теперь находятся рядом с PC-A (рис. 10). Один конверт - это сообщение, передаваемое по протоколу ICMP, другой - сообщение, передаваемое по протоколу ARP. Event List (список событий) на панели «Simulation» (панель моделирования) точно отобразит, какой из конвертов представляет сообщение, передаваемое по протоколу ICMP, а какой - сообщение, передаваемое по протоколу ARP (рис. 11).

Рис. 10. Отправка обычного эхо-пакета в режиме симуляции.

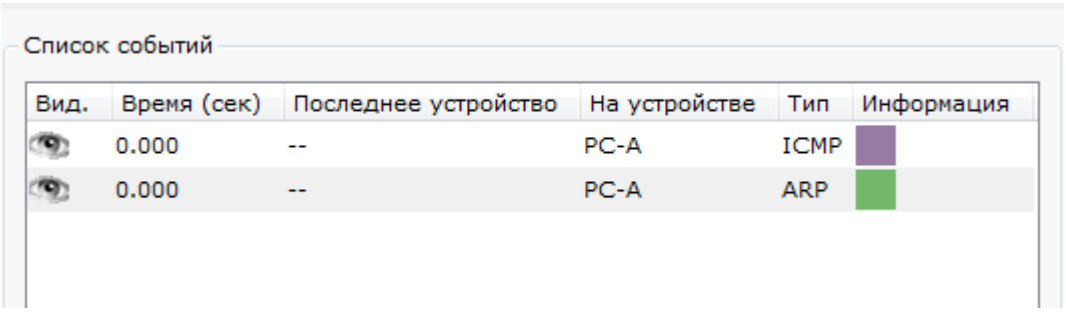


Рис. 11. Окно списка событий с подробной информацией о пакетах.

г.

Нажмите кнопку **Auto Capture / Play** (автозахват / воспроизведение) в области **Play Controls** (регуляторы воспроизведения) на панели «Simulation» (панель моделирования). Под кнопкой **Auto Capture / Play** (автозахват / воспроизведение) имеется горизонтальная полоса с

вертикальной кнопкой (ползунком), регулирующей скорость моделирования. При перетаскивании ползунка вправо/влево увеличивается/снижается скорость моделирования.

д. Воспроизведение анимации закончится при появлении окна с сообщением *No More Events* (больше событий нет). Это означает, что все запросы событий выполнены. Нажмите кнопку **OK** для закрытия окна с сообщением.

е. Нажмите кнопку **Reset Simulation** (восстановить моделирование) на панели «Simulation» (панель моделирования). Обратите внимание, что конверт типа ARP отсутствует. Процесс моделирования вернулся в исходное состояние, но при этом изменения конфигурации или записи в динамической таблице, например, записи в ARP-таблице, отменены не были. ARP-запрос не обязателен для выполнения команды **ping**, поскольку PC-A уже имеет MAC-адрес в ARP-таблице (рис. 12).

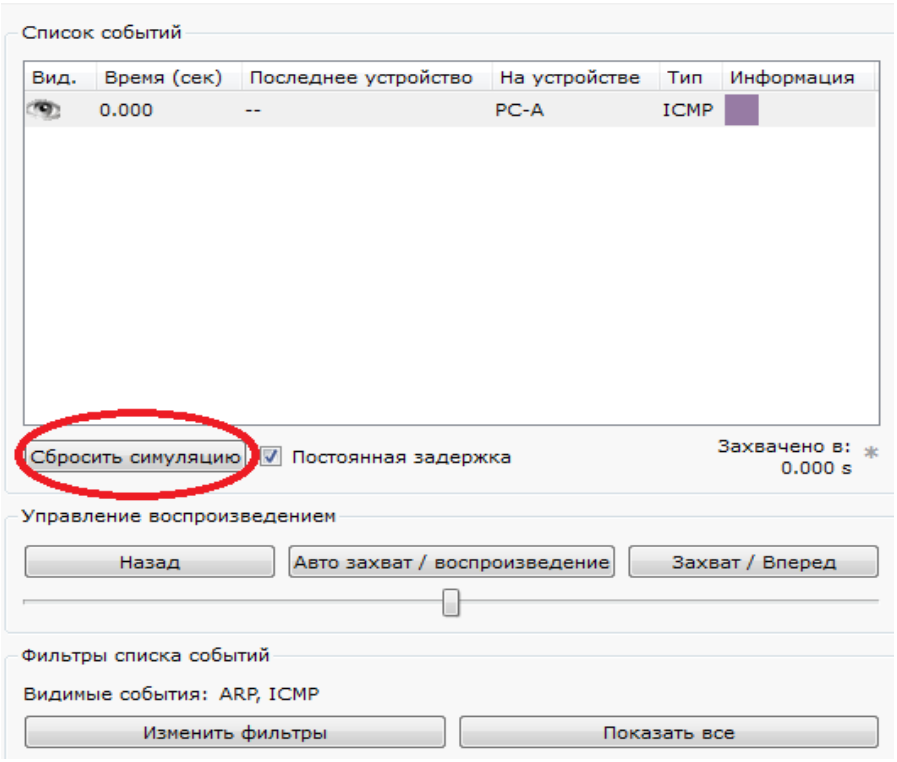


Рис. 12. Сброс симуляции.

ж. Нажмите кнопку **Capture / Forward** (захват / вперед). ICMP-конверт переместится от отправителя к концентратору и остановится. Кнопка **Capture / Forward** (захват / вперед) позволяет запустить моделирование на один шаг вперед. Нажимайте кнопку **Capture / Forward** (захват / вперед) до тех пор, пока не выполните событие.

з. Нажмите кнопку **Power Cycle Devices** (Управление(включение-выключение) питанием устройств) снизу слева, над значками устройств. С помощью этой кнопки вы можете выключить/включить силовое питание одновременно на всех устройствах в окне моделирования, перезагрузив таким образом все устройства.

и. Откроется окно с запросом подтвердить сброс. Нажмите кнопку **Yes** (да). ICMP- и ARP-конверты появятся снова. Кнопка **Reset Network** (сброс сети) отменит все несохраненные изменения конфигурации и сотрет все записи в динамической таблице, например, записи ARP- и MAC-таблицы.

Лабораторная работа №1 Аппаратные средства персонального компьютера

Часть 1. Определение емкости устройства хранения данных

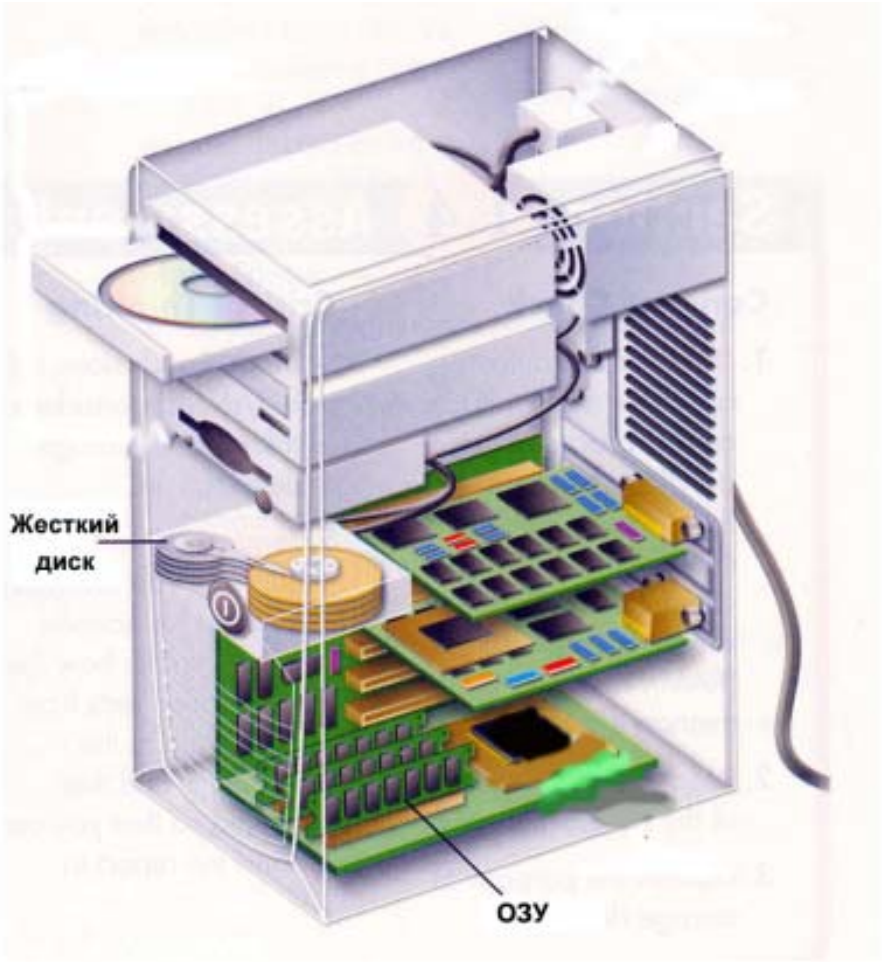


Рис. 1. Основные компоненты компьютерной системы внутри системного блока.

Задачи

• Определить объем установленного в ПК ОЗУ (в МБ).
• Определить размер установленного в ПК жесткого диска (в ГБ).
• Определить используемое и доступное пространство на жестком диске (в ГБ).
• Проверить другие типы устройств хранения (дискеты, компакт-диски, DVD-диски).

Исходные данные / подготовка

Устройства хранения многих компонентов ПК измеряется в мегабайтах (МБ) - 2 в 20-ой степени байт и гигабайтах (ГБ) - 2 в 30-ой степени байт. Эти значения несколько больше, чем 1 миллион байт и 1 миллиард байт, соответственно. К таким компонентам относятся ОЗУ, жесткие диски и оптические носители, такие как компакт-диски и DVD-диски. В данной работе требуется определить емкость и доступное пространство для различных компонентов компьютера.

Необходимо использовать следующие ресурсы:
• компьютер с установленной ОС Windows XP.

Шаг 1. Идентификация ОЗУ компьютера

а. В ОС Windows XP существуют два способа просмотра панели управления: классический вид и вид по категориям. Эти возможности доступны в зависимости от того, какой из двух видов используется. Если слева видна опция «Переключение к виду по категориям», то в настоящее время используется классический вид. Если отображается опция «Переключение к классическому виду», то в настоящее время используется вид по категориям. На этом шаге необходимо переключиться к классическому виду.

б. В меню «Пуск» выберите пункт «Панель управления». В окне «Панель управления» выберите значок «Система», чтобы открыть диалоговое окно «Свойства системы». Другой способ: эту информацию можно получить, нажав кнопку «Пуск» и правой кнопкой щелкнув значок «Мой компьютер». Затем в раскрывающемся меню выберите пункт «Свойства». Информация об операционной системе и пакете обновлений компьютера указана в верхней части данного диалогового окна. Тип процессора, тактовая частота и объем памяти компьютера указаны в нижней части.

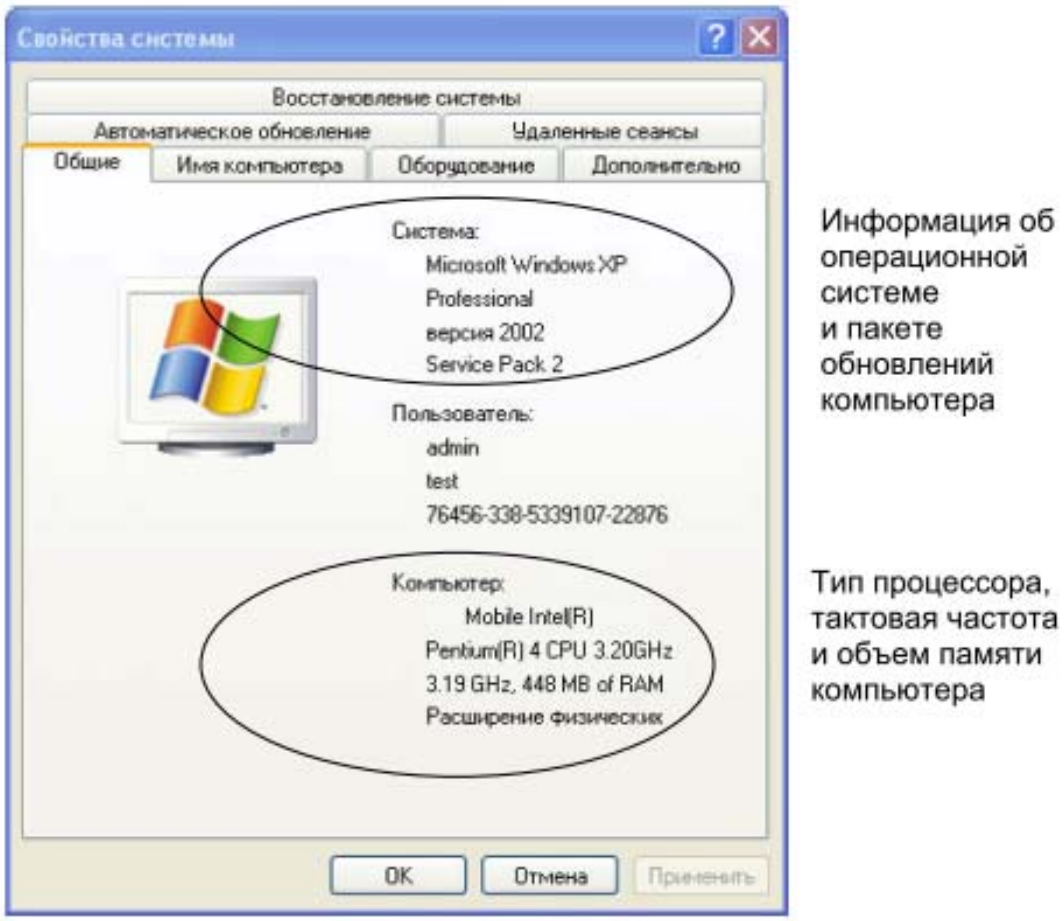


Рис. 2. Информация о характеристиках процессора, оперативной памяти и версии ОС.

в. В данном примере процессор компьютера – Pentium 4 с тактовой частотой 3,2 гигагерц (ГГц). Тактовая частота соответствует числу циклов тактового генератора в секунду, синхронизирующего работу процессора. Число циклов влияет на количество выполняемых процессором за секунду команд. Более высокая тактовая частота означает, что процессор способен выполнять больше инструкций за секунду.

На данном компьютере для ЦП доступно 448 МБ ОЗУ.

г. Проверьте свой компьютер и определите объем ОЗУ, доступного ЦП. Укажите объем ОЗУ вашего компьютера.

Шаг 2. Определение объема жесткого диска

а. Дважды щелкните значок «Мой компьютер» на рабочем столе компьютера. Если значка «Мой компьютер» нет, нажмите кнопку «Пуск» и выберите пункт «Мой компьютер».
б. Правой кнопкой мыши щелкните значок локального жесткого диска в разделе «Жесткие диски» (обычно это диск C) и выберите пункт «Свойства». В результате откроется диалоговое окно «Свойства: Локальный диск (C:)». Общая емкость жесткого диска отображается над значком «Диск C».

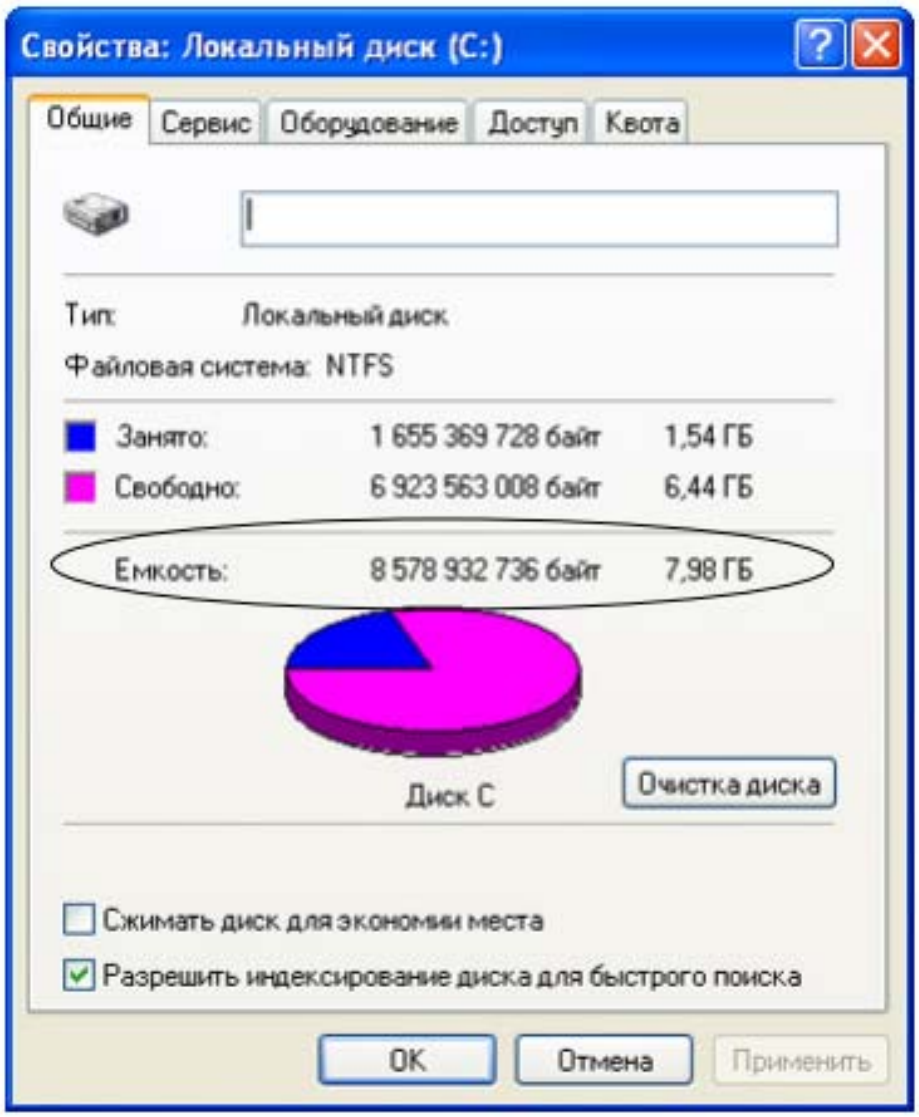


Рис. 3. Объем жесткого диска.

в. Определите объем жесткого диска своего компьютера. Укажите общий объем жесткого диска в ГБ.

_____

г. Оставьте диалоговое окно «Свойства: Локальный диск (C:)» для выполнения следующего шага.

Шаг 3. Определение свободного и используемого пространства на жестком диске
а. В диалоговом окне «Свойства: Локальный диск (C:)» используемое и свободное пространство указывается в байтах и ГБ над разделом «Емкость».

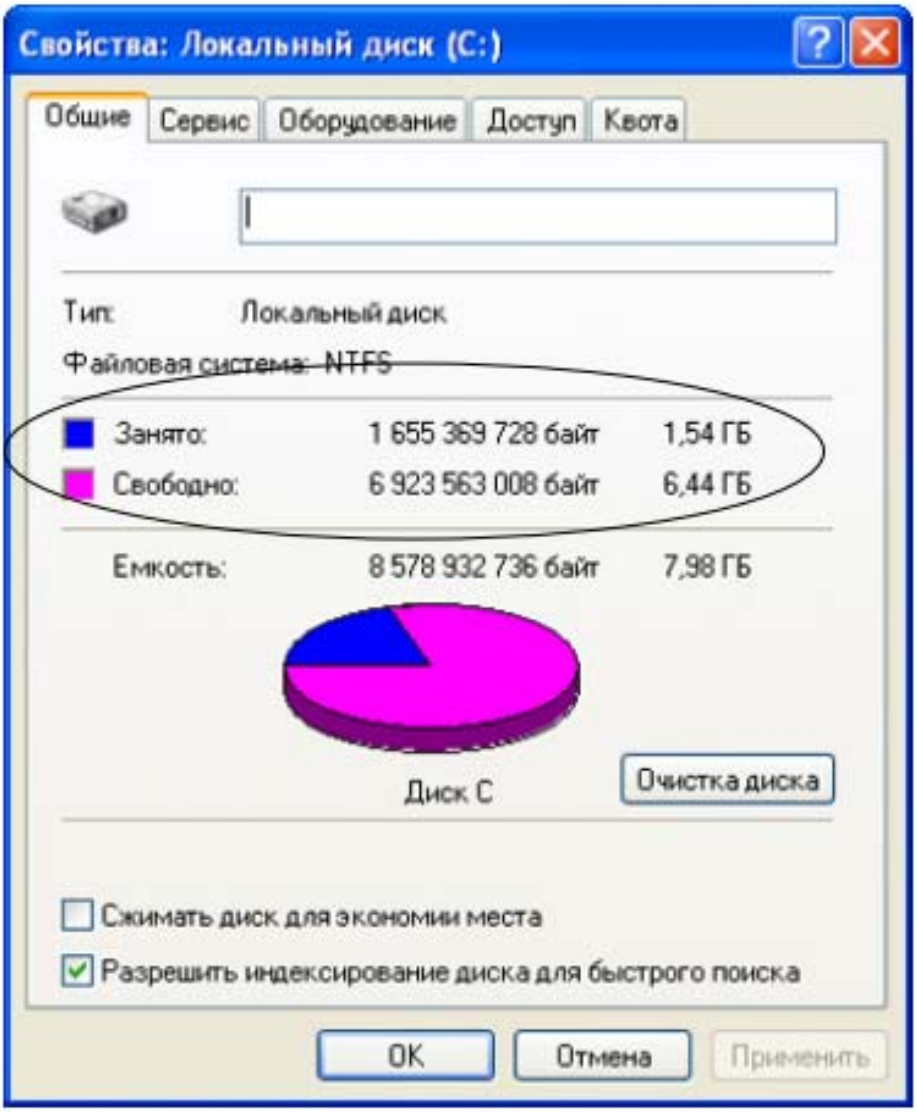


Рис. 4. Распределение занятого и свободного пространства на жестком диске.

б. Какой объем жесткого диска в ГБ используется? _____
_____

в. Какой объем свободного пространства на жестком диске в ГБ?
_____

Шаг 4. Проверка других устройств хранения

а. Правой кнопкой мыши щелкните кнопку «Пуск» и выберите пункт «Проводник». В левой панели выберите ветку «Мой компьютер».

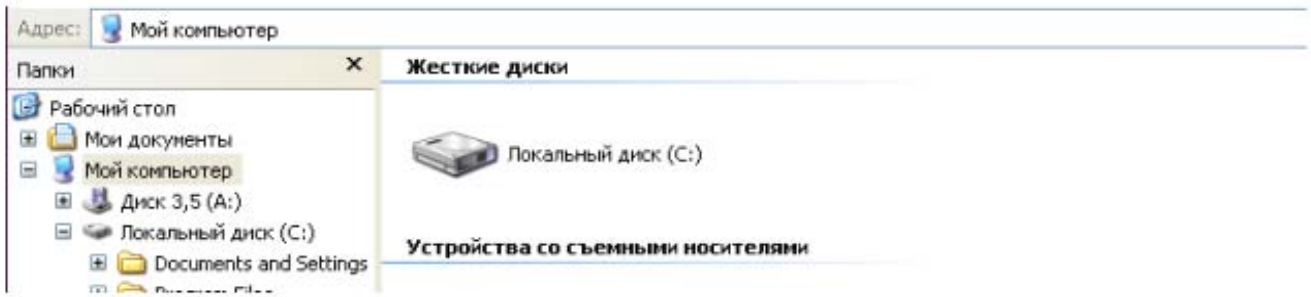


Рис. 5. Логические жесткие диски в ОС Windows.

б. Сколько букв дисков отображается в открывшемся окне? _____
_____

в. Правой кнопкой мыши щелкните значок другого диска, не C:, и выберите пункт «Свойства». Откроется диалоговое окно «Свойства: Съемный диск».

г. Перейдите на вкладку «Оборудование», на которой представлена информация о каждом устройстве и его состоянии работоспособности.

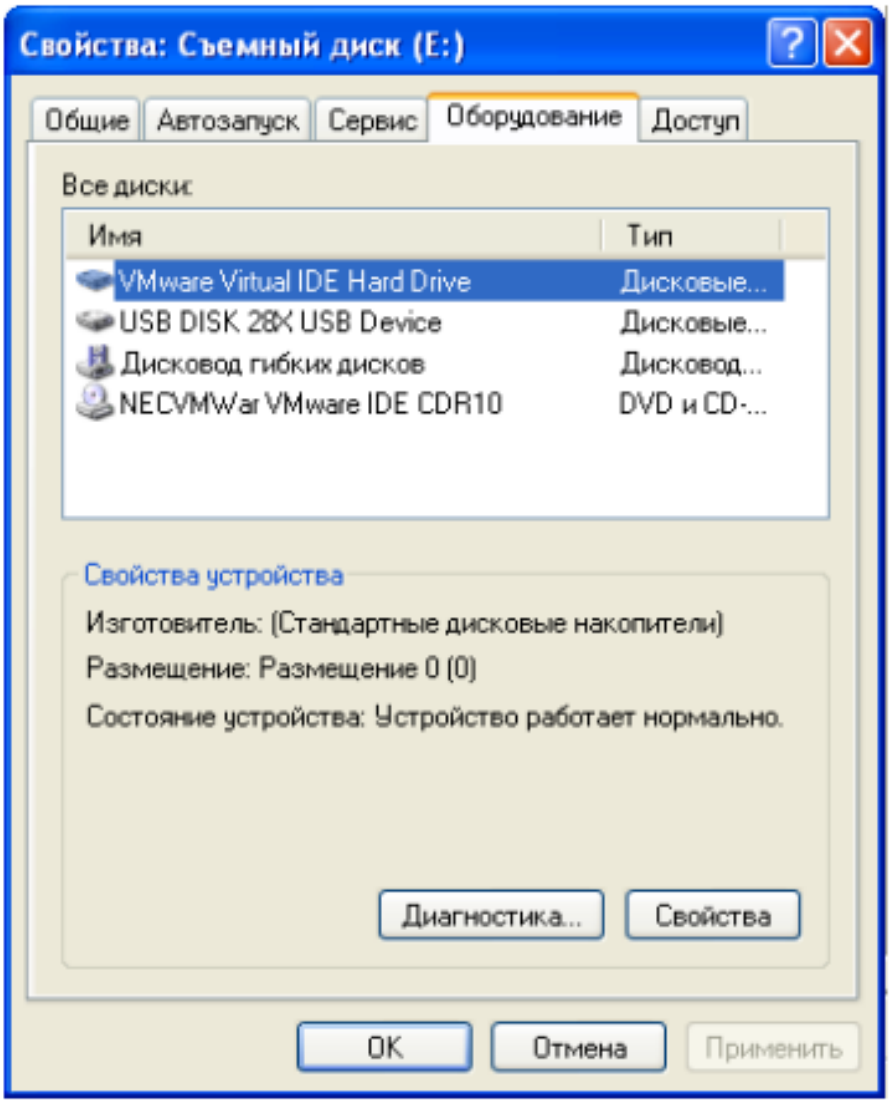


Рис. 6. Связь между логическими дисками и физическими устройствами.

Шаг 5. Вопросы для обсуждения

а. Почему важно знать объем ОЗУ компьютера?

_____
_____

б. Почему важно знать объем жесткого диска, а также объем используемого пространства?

_____
_____

Часть 2. Определение разрешения экрана компьютера

Задачи
• Определить текущее разрешение экрана монитора ПК.
• Определить максимальное разрешение для самого высокого качества цветопередачи.
• Вычислить число пикселей, необходимых для настройки разрешения.
• Определить тип монитора и установленной графической платы.

Исходные данные / подготовка

Разрешение монитора определяет качество изображения на экране монитора. Разрешение определяется числом горизонтальных и вертикальных элементов изображения (пикселей), которые используются для формирования изображения на экране монитора. Обычно число пикселей предопределяется производителем графических плат и мониторов ПК. Самое больше число пикселей, поддерживаемое монитором и графической платой, называется максимальным разрешением. Пример максимального разрешения – 1280 x1024, которое означает, что экран состоит из 1280 горизонтальных пикселей и 1024 вертикальных пикселей. Чем более высокое разрешение задано, тем четче отображается на экране изображение. Максимальное разрешение монитора ПК и число цветов, которое может отобразить монитор, определяется двумя факторами:

• возможностями монитора;
• возможностями графической платы, особенно объемом встроенной памяти.

Необходимо использовать следующие ресурсы:
• компьютер с установленной ОС Windows XP.

Шаг 1. Определение текущего разрешения экрана

а. Чтобы узнать текущее разрешение экрана и настройки качества цветопередачи, правой кнопкой мыши щелкните в пустом месте рабочего стола и выберите в контекстном меню пункт «Свойства». В окне «Свойства: Экран» перейдите на вкладку «Параметры».

Окно «Свойства: Экран» также можно открыть из панели управления, щелкнув значок «Экран».

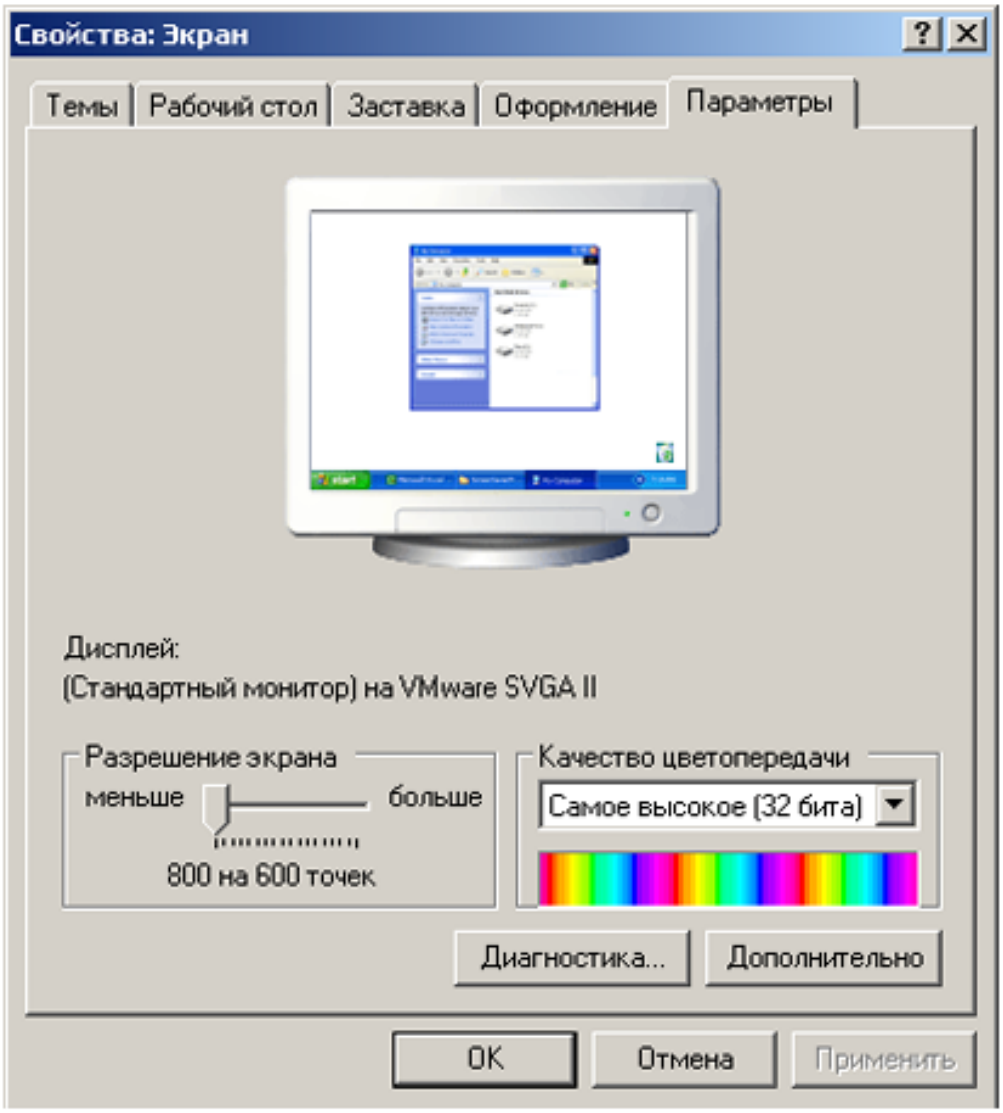


Рис. 7. Настройка разрешения экрана.

б. Запишите текущие параметры ПК, представленные на вкладке «Параметры» окна «Свойства: Экран».
Разрешение экрана (Г x В) _____
Разрешение по горизонтали: _____
Разрешение по вертикали: _____
Значение качества цветопередачи: _____

Шаг 2. Определение максимального разрешения для самого высокого качества цветопередачи

Ползунок в разделе «Разрешение экрана» используется для настройки требуемого разрешения.

а. Подвигайте ползунок, чтобы просмотреть диапазон разрешений экрана, доступных на данном ПК. (Данный диапазон определяется операционной системой, если та распознает графическую плату и монитор.)

б. На основе текущих параметров ПК, представленных на вкладке «Параметры» окна «Свойства: Экран», заполните следующую таблицу.
Минимальное разрешение экранаМаксимальное разрешение экранаДоступные значения параметра

качества цветопередачи
Шаг 3. Вычисление числа пикселей для настроек текущего и максимального разрешений

Экран монитора состоит из рядов пикселей. Число пикселей в каждом ряду – это разрешение по горизонтали. Число рядов – это разрешение по вертикали. Чтобы определить общее число пикселей при некотором разрешении экрана, разрешение по горизонтали умножается на разрешение по вертикали. Например, если текущее разрешение – 1280 x 1024, то общее число пикселей равно 1280 умножить на 1024, или 1 310 720.

а. Вычислите общее число пикселей при минимальном разрешении. _____

б. Вычислите общее число пикселей при максимальном разрешении. _____

Шаг 4. Определение типа установленной графической платы

Подробную информацию о графической плате (также называется адаптером дисплея) можно получить в окне «Свойства: Экран».
а. В окне «Свойства: Экран» нажмите кнопку «Дополнительно».
б. Перейдите на вкладку «Адаптер».

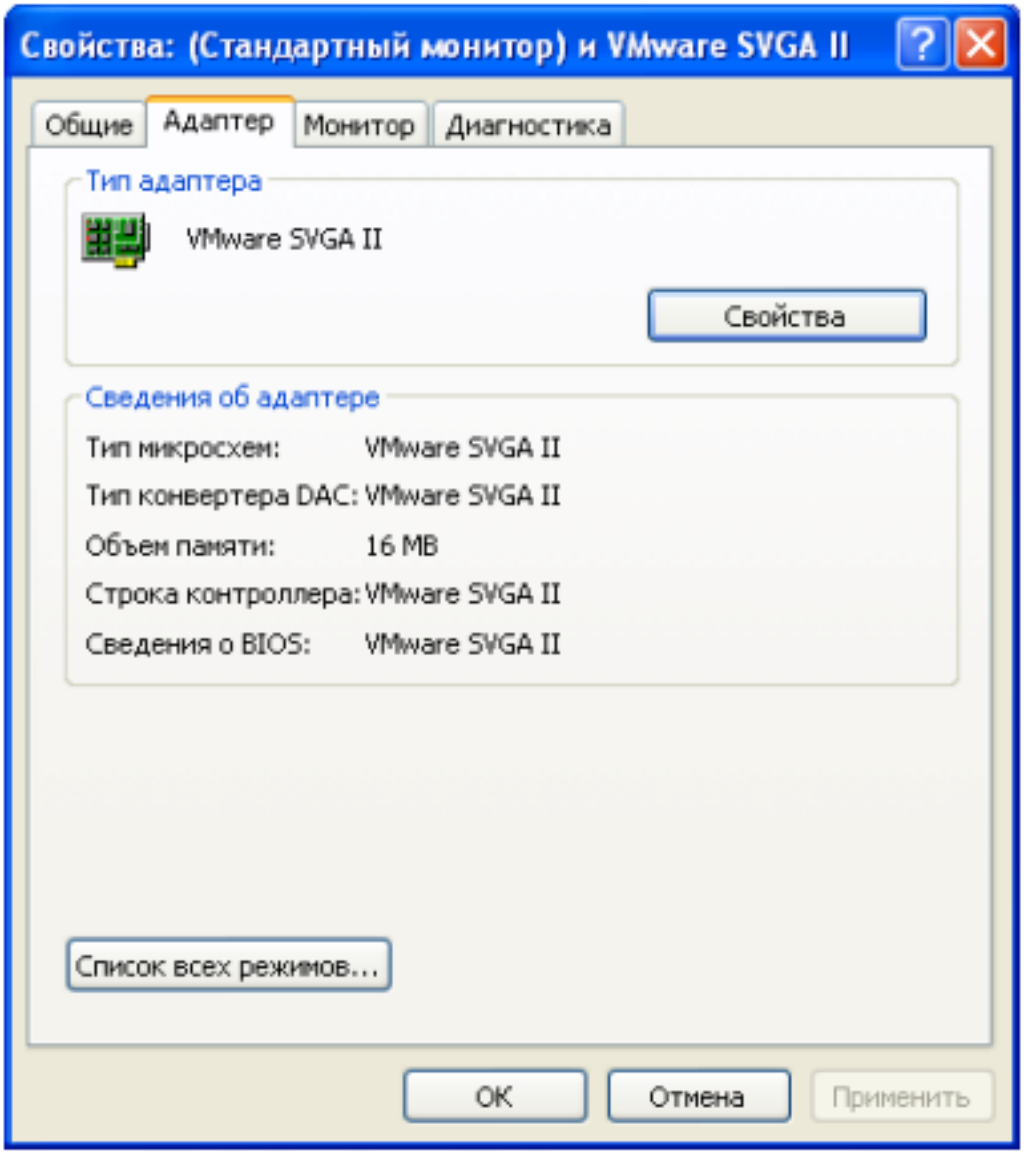


Рис. 8. Характеристики адаптера видеокарты.

в. На основе информации, представленной на вкладке «Адаптер», заполните следующую таблицу.

Производитель и модель графической платы (тип адаптера)	
Объем графической памяти на плате (объем памяти)	

Шаг 5. Определение типа монитора и доступных частот обновления

Подробную информацию о мониторе можно получить в окне «Свойства: Экран». Частота обновления экрана определяет, сколько раз за секунду экран облучается или перерисовывается. Частота обновления 60 герц означает, что экран облучается 60 раз в секунду. Более высокие частоты обновления снижают мерцание экрана, что уменьшает напряжение глаз, однако может негативно повлиять на монитор. Следует устанавливать максимальную частоту обновления, которую монитор может безопасно поддерживать.

а. Перейдите на вкладку «Монитор», чтобы узнать тип монитора и текущую частоту обновления.

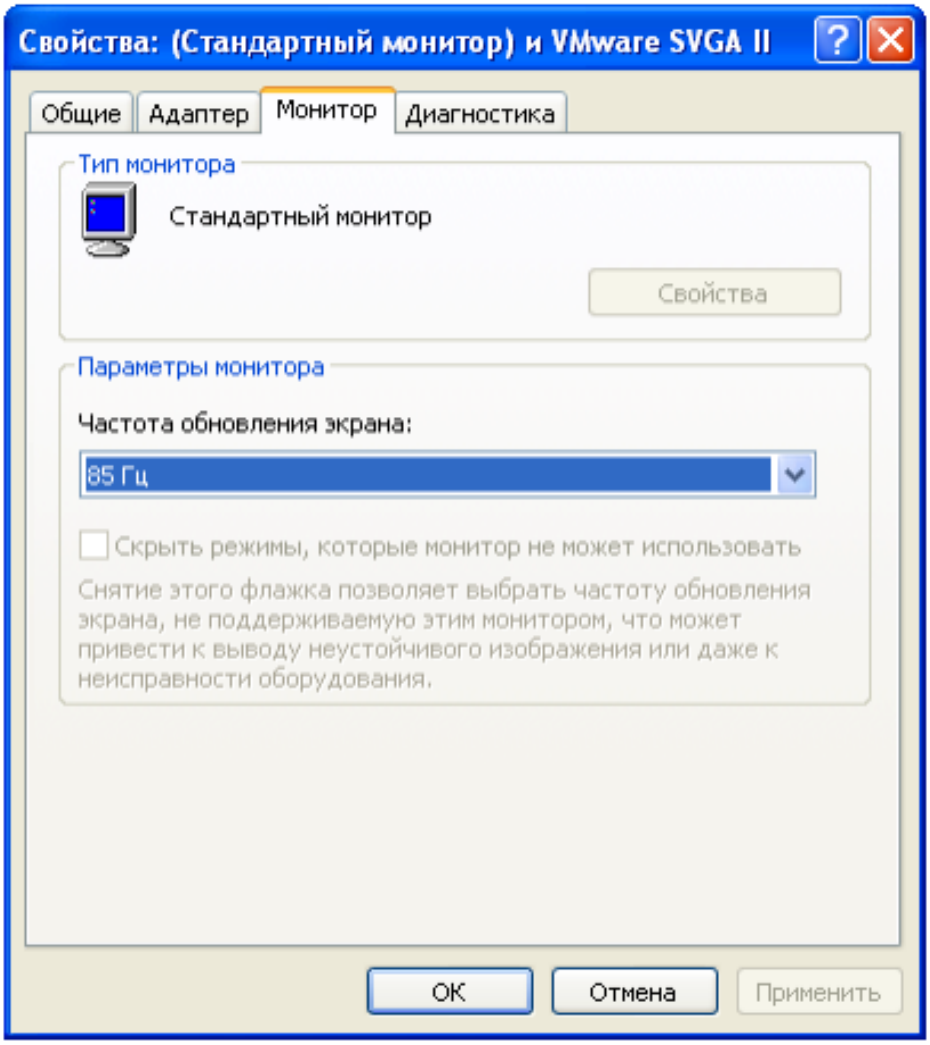


Рис. 9. Настройка частоты обновления экрана.

б. На основе информации, представленной на вкладке «Монитор», заполните следующую таблицу.

Тип монитора	

Поддерживаемые частоты обновления	

в. Что может случиться, если выбрать частоту обновления выше той, которую монитор может безопасно поддерживать?

Лабораторная работа №2 Установка локального и сетевого принтера, проверка его работоспособности

Задачи

• Вручную установить принтер, используя драйвер Windows XP по умолчанию.
• Проверить установку принтера и драйвера и устранить любые проблемы.
• Загрузить и установить последнюю версию драйвера от производителя принтера.

Исходные данные / подготовка

Многие принтеры для дома и малых офисов поддерживают самонастройку (plug-and-play), т.е. ОС Windows XP автоматически обнаруживает принтер и устанавливает соответствующий драйвер. Однако знание процесса установки принтера и обновления его драйвера вручную позволяет устранять многие типы неполадок принтера.

В данной лабораторной работе требуется установить виртуальный принтер на рабочей станции Windows XP. Работа выполняется без реального принтера, однако, большинство шагов в точности такое же, как при подключении физического принтера.

Необходимо использовать следующие ресурсы:

• компьютер с установленной ОС Windows XP;
• подключение к Интернету.

Общая информация о типах принтеров.

Обработка поступающих данных печати и перевод их в приемлемый для печатного механизма вид в любом, даже самом простом принтере осуществляется с помощью встроенного в принтер процессора. Любой встроенный процессор принтера управляется с помощью какого-либо языка команд. Среди таких языков можно назвать, например, Postscript, PCL, ESC/P, HPGL, Lineprinter, Xerox XES/UDK, Luminous LN02Plus и множество других. В настоящее время широкое распостранение получили недорогие GDI-принтеры. GDI, или Graphic Device Interface не что иное как библиотека определенных функций операционной системы Windows для осуществления вывода информации на графические периферийные устройства, такие как дисплеи или принтеры. Таким образом, процессор "GDI-принтера" - не умеет преобразовывать передаваемую ему информацию в выводимое на печать изображение. В отличие от принтеров с мощным встроенным процессором, контроллер GDI-принтера всего лишь выводит информацию в буферную память принтера. Принимаемая программой печати информация представляет собой описание страницы, воспроизводящее уже подготовленные к печати графические примитивы - линии, текст и пр., для обработки которых и вызываются функции GDI. Драйвер печати принтера переводит эту информацию на внутренний язык принтера. Таким образом, основная работа по подготовке изображения к выводу на печать в случае GDI-модели ложится не на принтер, а на компьютер.

Плюсы такой "организации труда" огромны: вам не приходится переплачивать за достаточно дорогую электронную начинку принтера; для владельцев ПК даже средней мощности вопрос небольшой дополнительной нагрузки на CPU просто незаметен. Есть, правда, и минусы, хотя в наше время они достаточно условны, если речь не идёт о работе с операционной системой, отличной от Windows. Ну кому сейчас, к примеру, понадобится печать из-под DOS?

Шаг 1. Добавление принтера

а. В меню «Пуск» выберите пункт «Панель управления». Дважды щелкните значок «Принтеры и факсы». Если данный значок не отображается, щелкните опцию «Переключение к классическому виду» в левой панели.

б. В окне «Принтеры и факсы» щелкните значок «Установка принтера», чтобы открыть мастер установки принтеров. Нажмите кнопку «Далее».

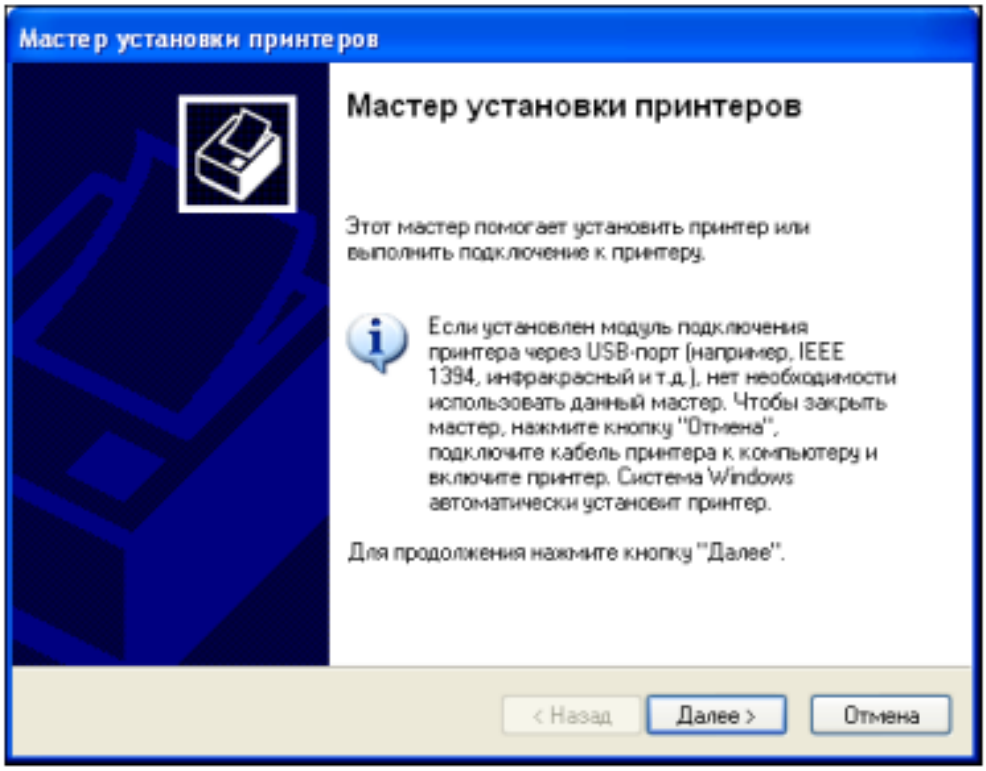


Рис. 1. Мастер установки принтера.

в. Для локального или сетевого принтера установите переключатель «Локальный принтер, подключенный к этому компьютеру» и снимите флажок «Автоматическое определение и установка PnP-принтера». Нажмите кнопку «Далее».

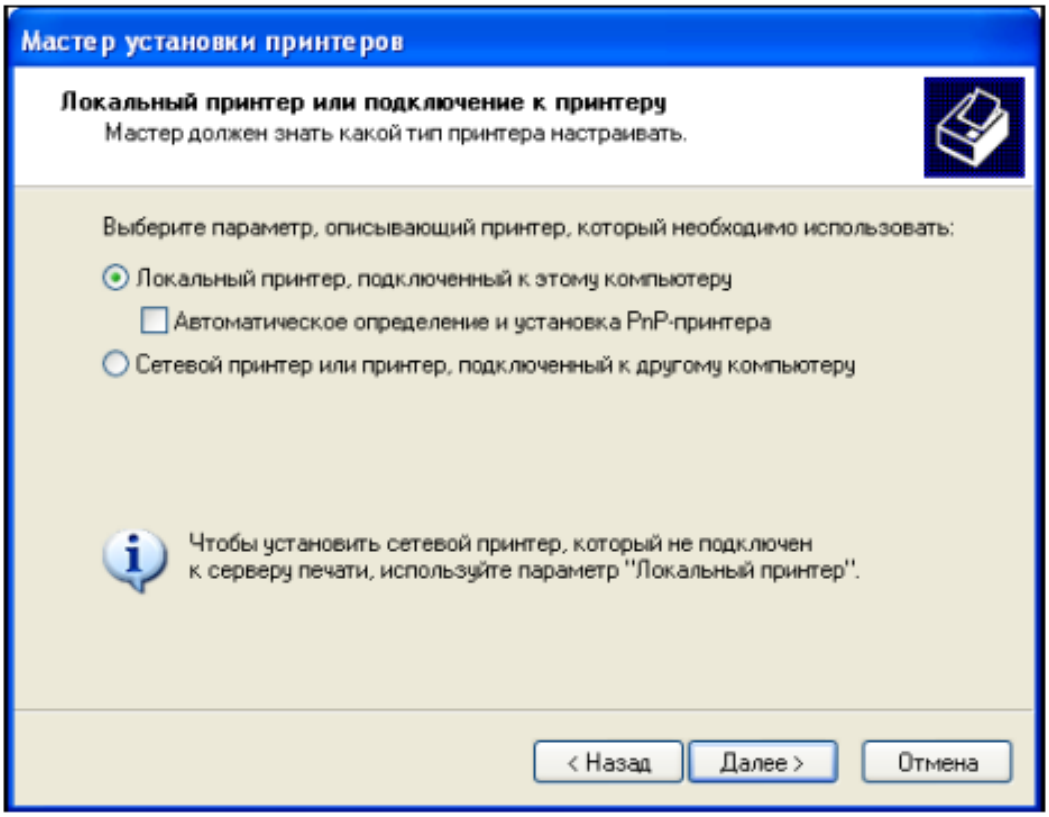


Рис. 2. Выбор типа устанавливаемого принтера.

г. На странице «Выберите порт принтера» установите переключатель «Использовать порт» и выберите LPT1: (Рекомендуемый порт принтера). Нажмите кнопку «Далее».

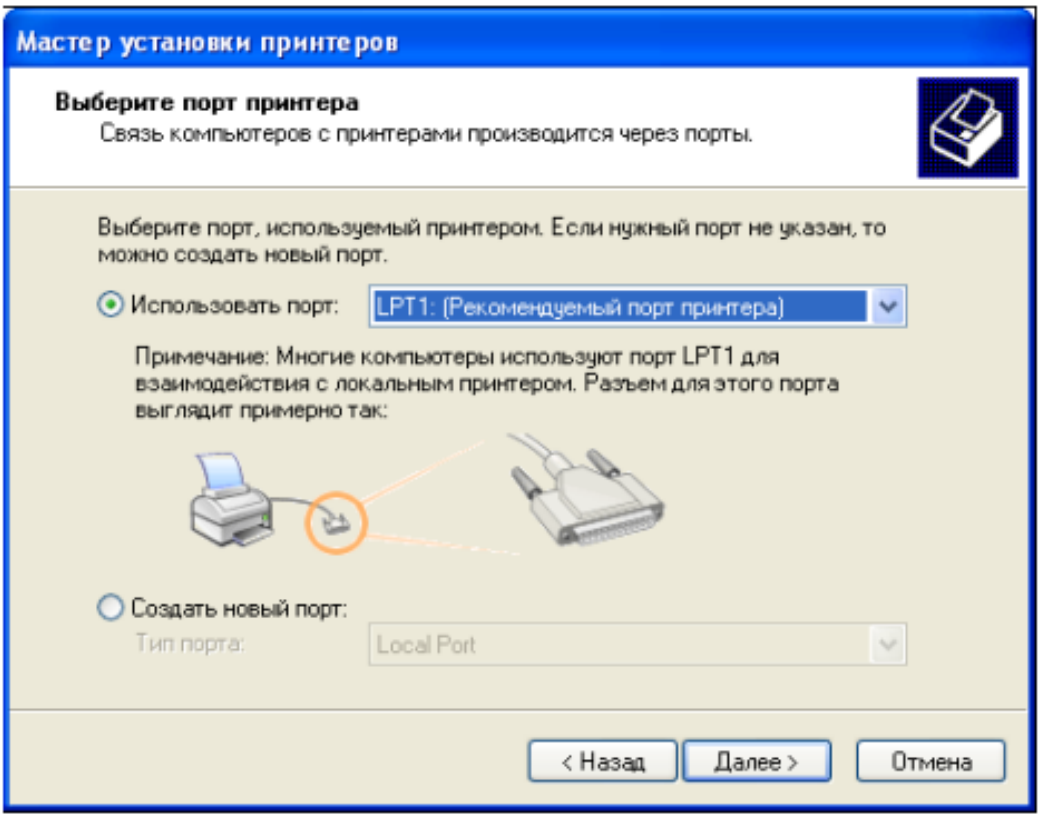


Рис. 3. Настройка физического порта для связи с принтером.

д. Примечание. На этом шаге требуется выбрать драйвер, предоставляемый Windows XP, для HP LaserJet 2200, распространенного черно-белого лазерного принтера для дома и малых офисов.

Если физического принтера нет, выполните следующие действия. Однако если устанавливается принтер, действительно подключенный к компьютеру, то вместо HP LaserJet 2200 выберите производителя и модель принтера, соответствующие подключенному устройству.

На странице «Установить программное обеспечение принтера» выберите «HP» из списка производителей. В списке «Принтеры» найдите строку «HP LaserJet 2200 Series PCL» и щелкните его, чтобы выбрать. Нажмите кнопку «Далее».

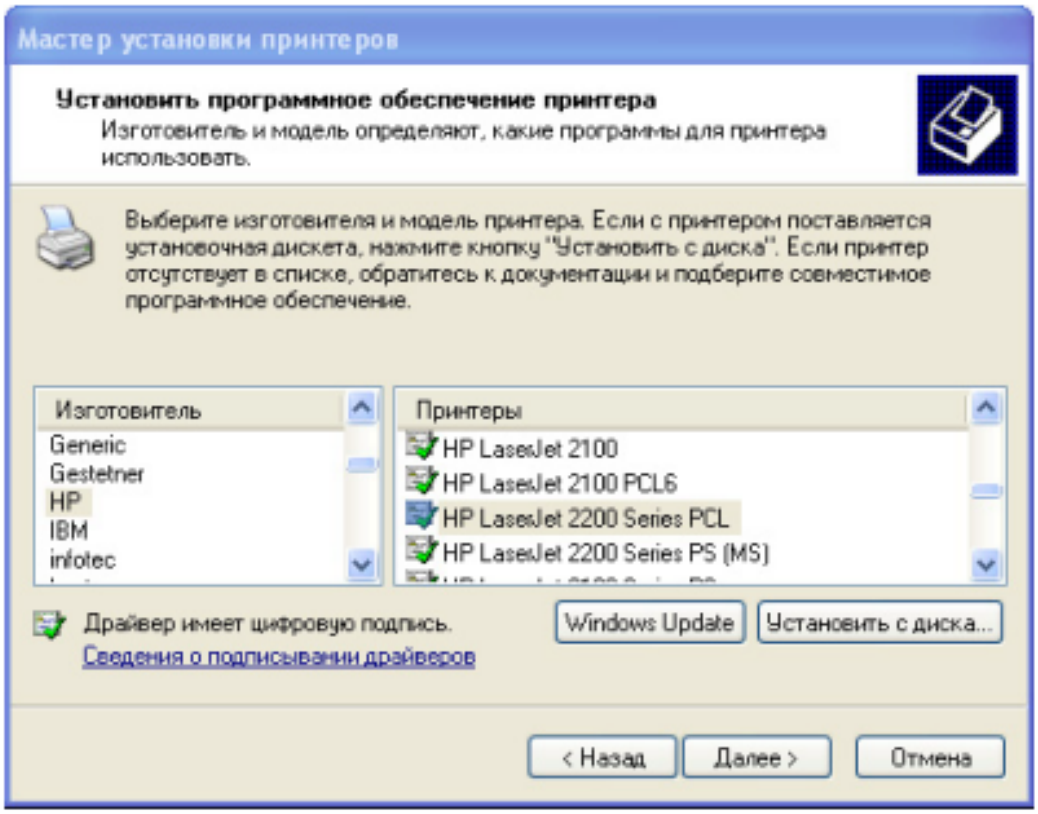


Рис. 4. Выбор драйвера принтера для соответствующего производителя из набора драйверов, имеющихся в составе операционной системы.

е. На странице «Назовите ваш принтер» введите описательное имя принтера. В среде, подобной большому офису с несколькими принтерами одной модели, полезно давать каждому принтеру уникальное имя, чтобы его можно было легко идентифицировать. Выберите «Нет» под вопросом «Использовать этот принтер по умолчанию?» (При подключении настоящего принтера выберите «Да», если необходимо, чтобы приложения Windows использовали этот принтер по умолчанию.) Нажмите кнопку «Далее».

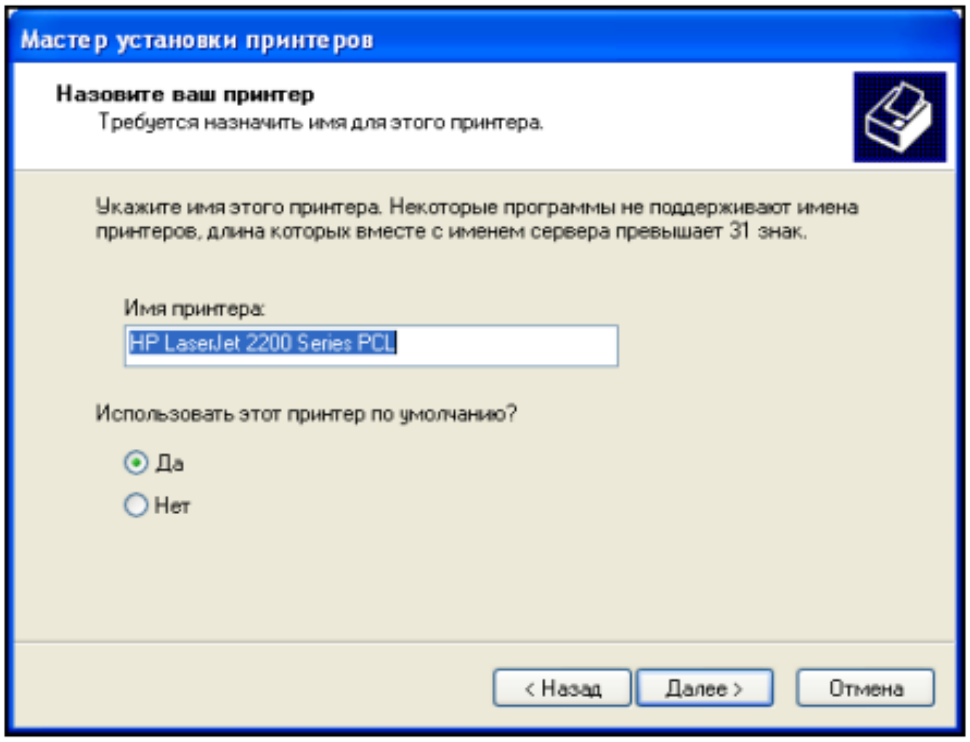


Рис. 5. Задание имени устанавливаемому принтеру.

ж. На странице «Использование общих принтеров» нажмите кнопку «Далее», чтобы принять вариант по умолчанию – «Нет общего доступа к этому принтеру».

з. При установке настоящего принтера нажмите кнопку «Далее» на странице «Напечатать пробную страницу», чтобы напечатать пробную страницу. При установке виртуального принтера HP LaserJet 2200 установите переключатель «Нет», прежде чем нажимать кнопку «Далее».

и. На странице «Завершение работы мастера установки принтеров» просмотрите параметры принтера, а затем нажмите кнопку «Готово».

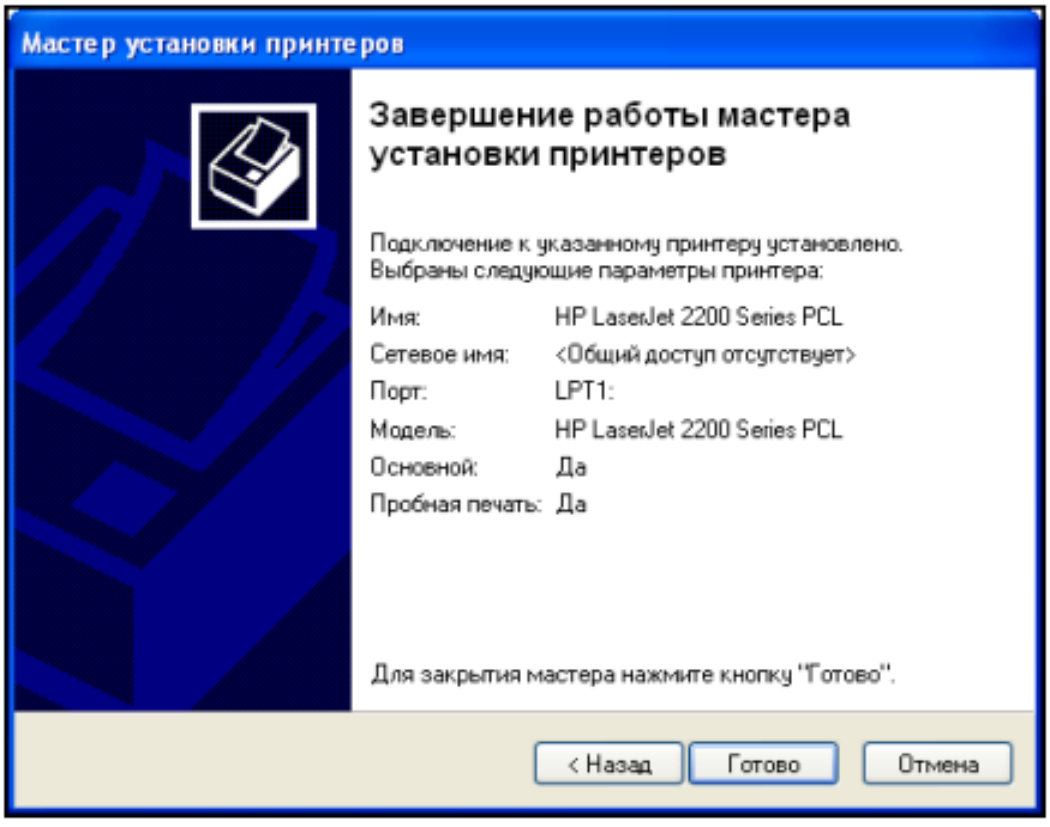


Рис. 6. Завершение работы мастера установки принтера.

Шаг 2. Проверка установки принтера

а. Откройте окно «Принтеры и факсы» из панели управления и убедитесь, что отображается значок только что установленного принтера. Если его нет, повторите шаг 1.

б. Правой кнопкой мыши щелкните значок нового принтера (HPLJ 2200 Series PCL), а затем выберите пункт «Свойства».

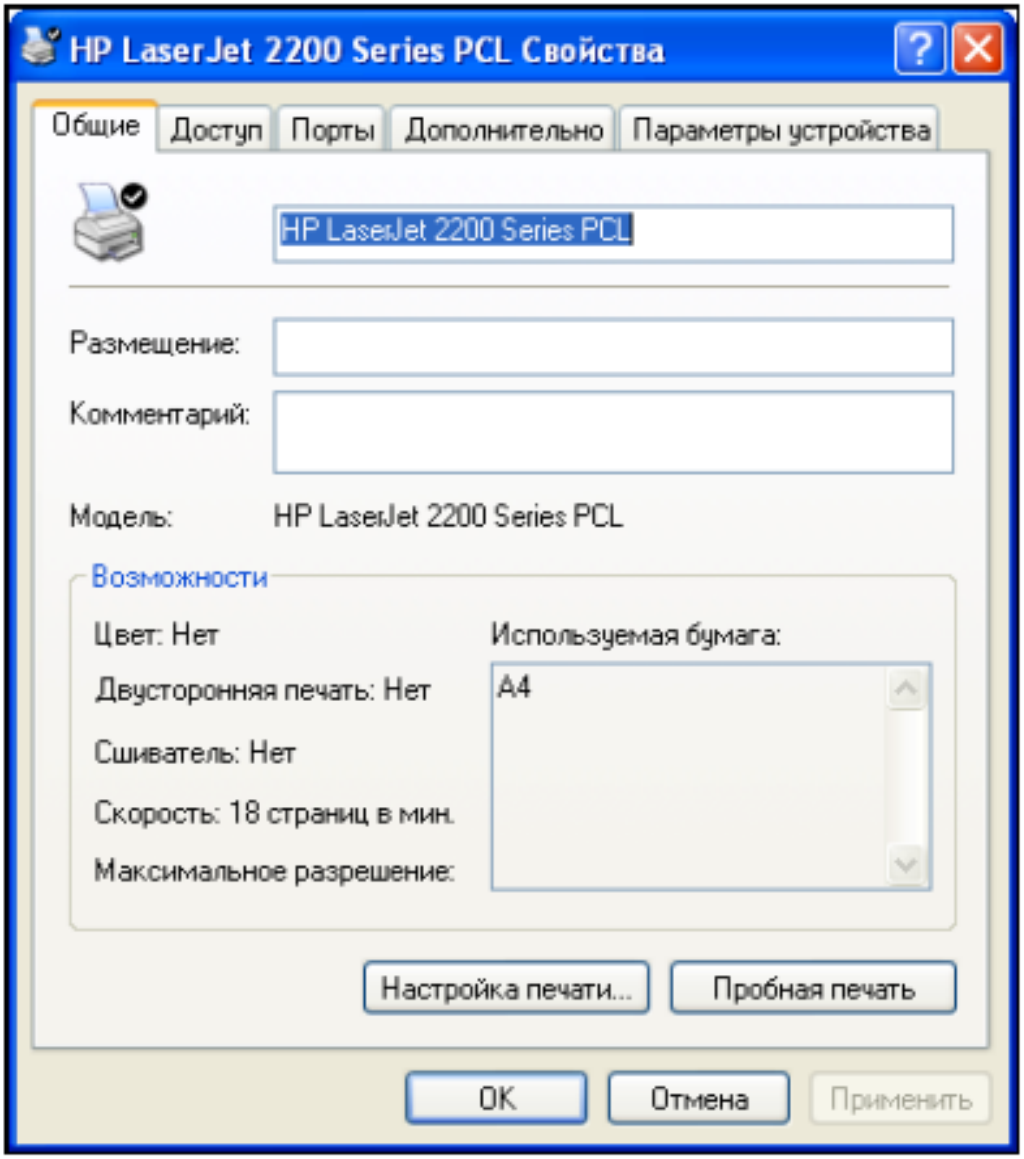


Рис. 7. Проверка свойств установленного принтера.

в. Перейдите на вкладку «Дополнительно» и запишите название драйвера, отображаемое в текстовом поле «Драйвер».
Название драйвера: _____

г. Перейдите на вкладку «Параметры устройства» и проверьте доступные возможности принтера, использующего этот драйвер. Чтобы закрыть окно, нажмите кнопку «Отмена».

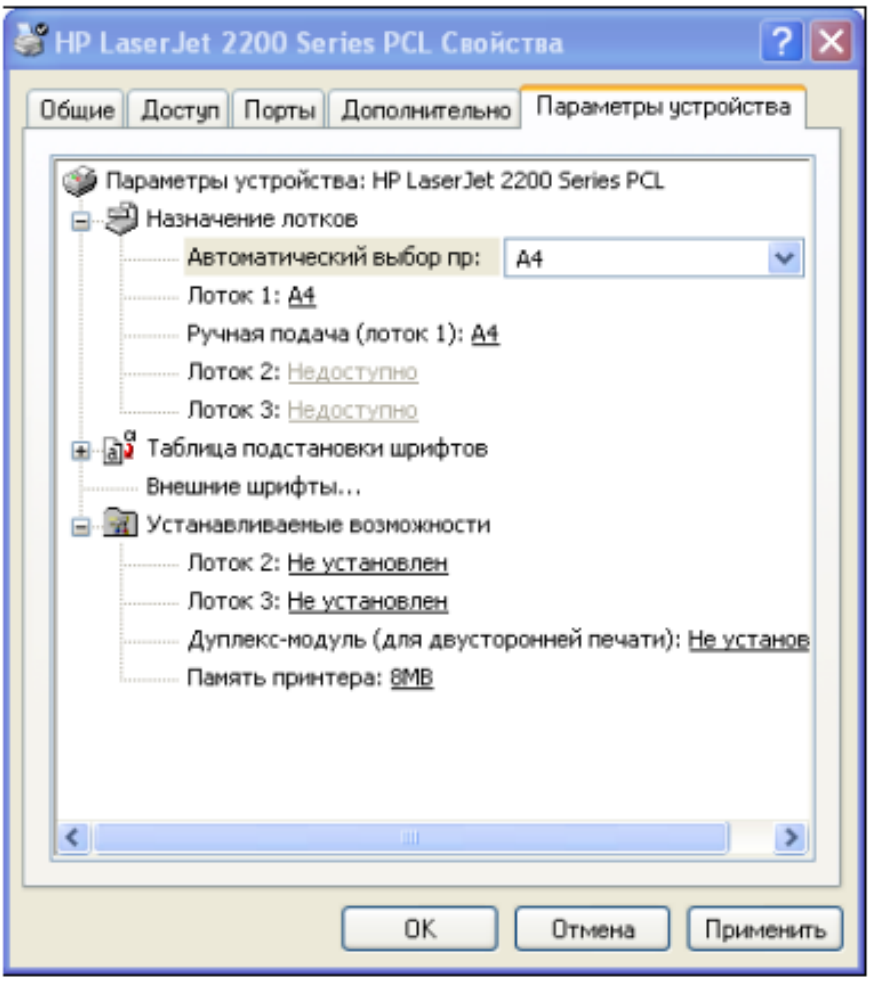


Рис. 8. Возможности регулировки параметров принтера ограничены установленным драйвером устройства.

Шаг 3. Загрузка и установка обновленного драйвера принтера

При использовании мастера установки принтеров для установки принтера установленный вручную драйвер по умолчанию позволяет принтеру функционировать, однако установленный Windows драйвер не всегда поддерживает все доступные возможности устройства. Полнофункциональные драйверы обычно предоставляются производителем устройства.

Обновление драйвера принтера – один из лучших способов устранения неполадок и повышения функциональности принтера. Большинство производителей продолжают обновлять драйверы, чтобы повысить их совместимость с операционными системами, поэтому стоит периодически проверять обновления драйверов и устанавливать их в случае доступности.

На этом шаге требуется посетить веб-сайт компании Hewlett-Packard, чтобы получить обновленный драйвер для принтера HP LaserJet 2200. Если установлен другой принтер, измените настоящие инструкции соответствующим образом.

а. Отройте веб-обозреватель и перейдите на веб-узел http://www.hp.com.
б. Перейдите по ссылке «Software and Driver Downloads» (загрузка программного обеспечения и драйверов).

ПРИМЕЧАНИЕ. На домашних страницах многих производителей есть ссылка на раздел поддержки, в котором можно найти ссылки для загрузки драйверов и других ресурсов.

в. Установите переключатель «Download drivers and software (and firmware)» (загрузить драйверы и программное обеспечение (и микропрограмму)). Укажите модель принтера в текстовом поле «for product» (для продукта) и нажмите кнопку с двойной стрелкой справа от текстового поля.

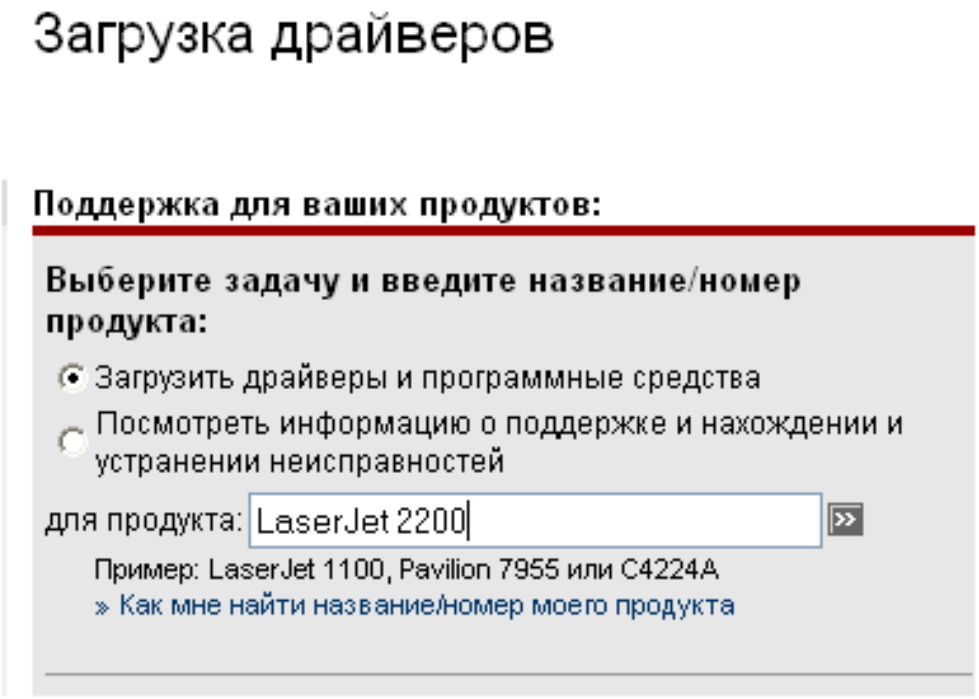


Рис. 9. Использование службы поддержки на сайте производителя для поиска необходимого драйвера.

г. В результатах поиска отображаются доступные продукты. Щелкните «HP LaserJet 2200 Printer» или модель принтера, для которого загружается драйвер.

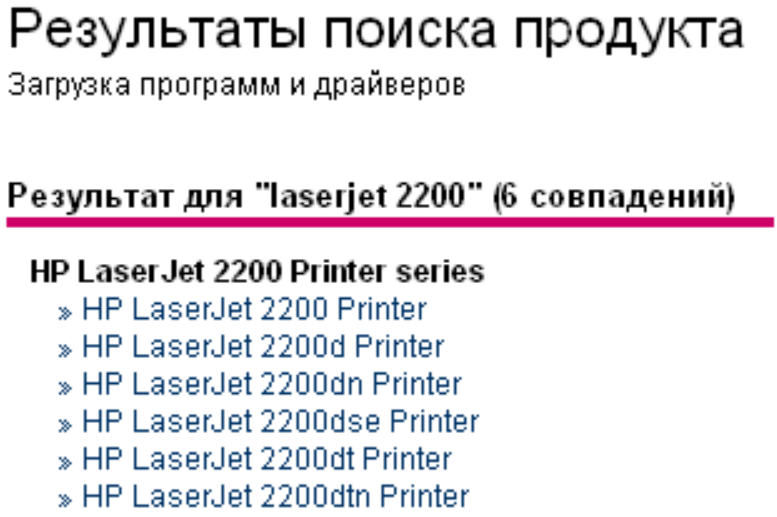


Рис. 10. Результатом поиска может быть несколько версий драйвера.

д. Выберите «Microsoft Windows XP» в списке операционных систем. В появившемся списке драйверов нажмите кнопку «Загрузить» для варианта «HP LaserJet 2200 PCL6 driver».

Драйвер

Описание	Текущая версия	Размер (Мбайт)	Предположительная продолжительность загрузки	Предыдущая версия	
HP LaserJet 2200 PCL5e Driver	4.27.2200.410 22 апр 2004	1.9	56K: 4m 512K: <1m		Загрузить »
hp LaserJet 2200 PCL6 driver	4.27.2200.410 22 апр 2004	1.9	56K: 4m 512K: <1m		Загрузить »
hp LaserJet 2200 PCL5e Point and Print bundle	4.3.2.192 14 июн 2002	6.1	56K: 14m 512K: 1m		Загрузить »
HP LaserJet 2200 PCL6 Point and Print bundle	4.3.2.192 14 июн 2002	6.1	56K: 14m 512K: 1m		Загрузить »
hp LaserJet 2200 PostScript driver	2.0.0.0 14 июн 2002	0.11	56K: <1m 512K: <1m		Загрузить »
hp LaserJet 2200 PostScript Point and Print bundle	2.0.0.0 14 июн 2002	1.6	56K: 3m 512K: <1m		Загрузить »

Рис. 11. Выбор и загрузка нового драйвера.

е. В диалоговом окне загрузки нажмите кнопку «Сохранить».

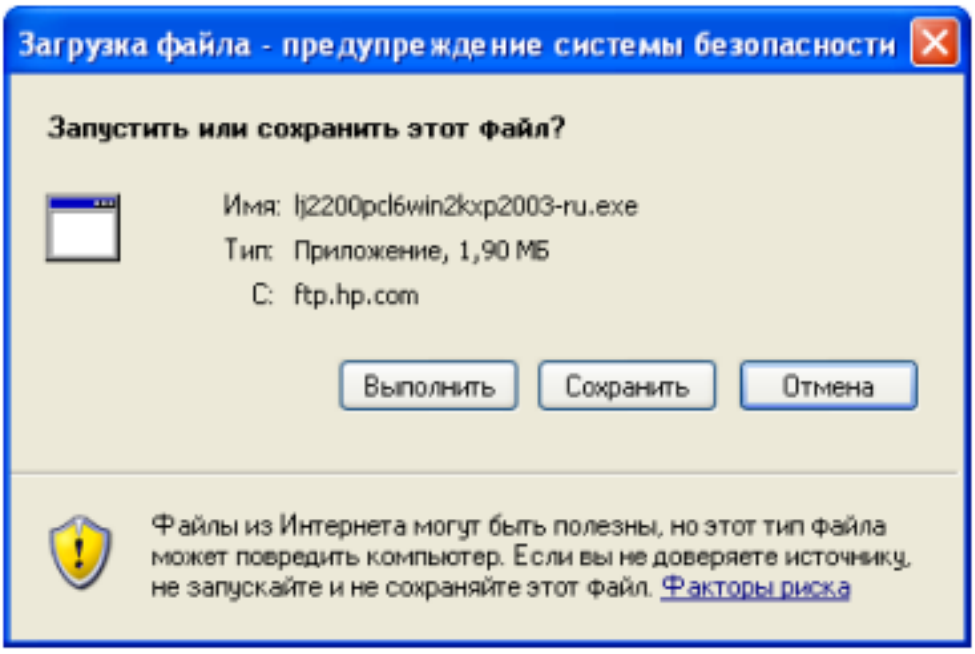


Рис. 12. Сохранение файла с программой установки драйвера.

ж. В диалоговом окне «Сохранить как» щелкните значок «Рабочий стол» в левой панели, чтобы сохранить установочный файл драйвера на своем рабочем столе. Данный файл можно сохранить в любом месте, однако важно знать, где он сохранен.

з. Запишите имя данного файла.

_____

и. Нажмите кнопку «Сохранить». Закройте обозреватель и все прочие открытые приложения.

к. Дважды щелкните значок загруженного файла.

ПРИМЕЧАНИЕ. У имени файла может быть расширение (.exe). Расширения файлов видны, только если в настройках проводника снять флажок «Скрывать расширения для зарегистрированных типов файлов», установленный по умолчанию. Обращайтесь к своему преподавателю за дополнительной информацией.

л. По запросу нажмите кнопку «Run» (выполнить). В открывшемся диалоговом окне установите второй переключатель, а затем нажмите кнопку «Next» (далее), чтобы распаковать файлы в папку c:\lj2200. Нажмите кнопку «Finish» (готово).

Рис. 13. Установка нового драйвера в операционную систему.

м. Повторите шаги 2а и 2б, чтобы открыть страницу «Свойства» нового принтера. Перейдите на вкладку «Дополнительно». Нажмите кнопку «Новый драйвер», а затем – «Далее», чтобы запустить мастер добавления драйверов принтеров.

н. В окне «Выбор драйвера принтера» нажмите кнопку «Установить с диска…».

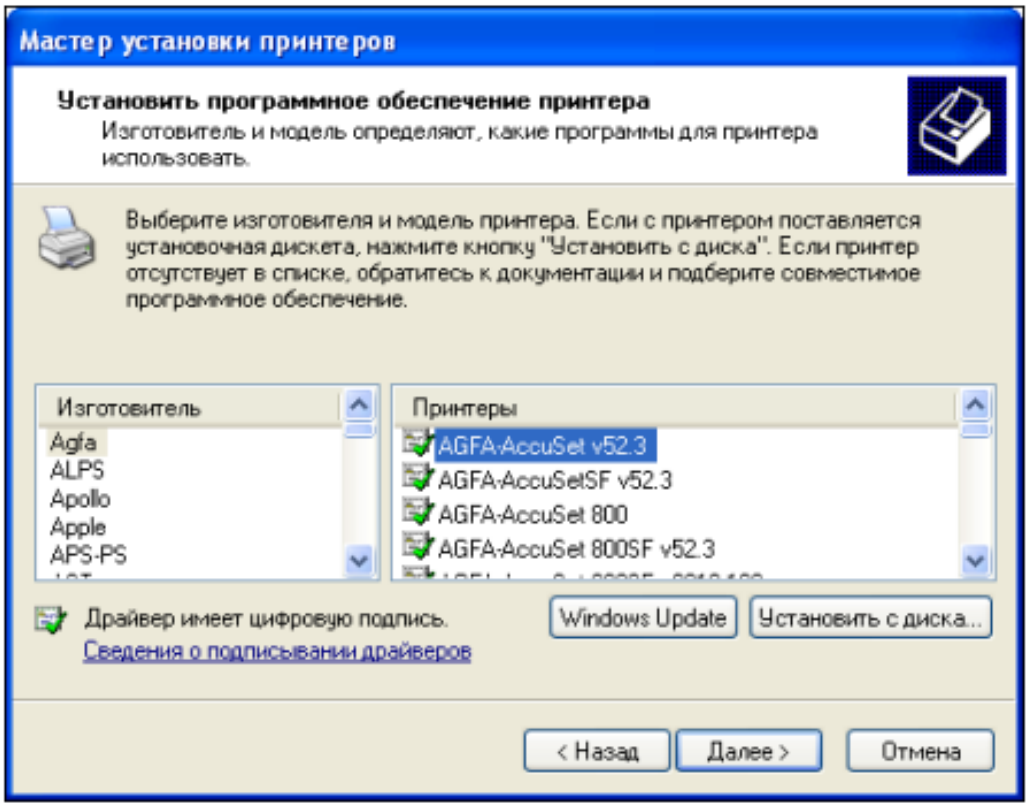


Рис. 14. Обновление драйвера принтера, выбор производителя и модели принтера.

о. В окне «Установка с диска» нажмите кнопку «Обзор» и перейдите к папке, созданной на шаге 3: Мой компьютер > Локальный диск C:\lj2200. Нажмите кнопку «Открыть», после чего выполняется переход обратно к окну «Установка с диска». Нажмите кнопку «ОК».

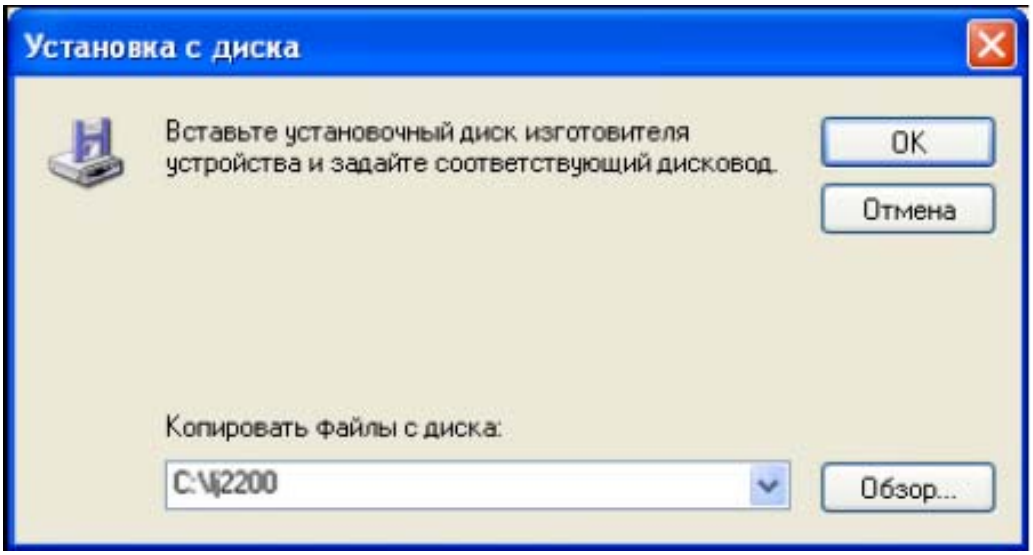


Рис. 15. Определение местоположение драйвера.

п. В окне «Выбор драйвера принтера» выберите HP LaserJet 2200 Series PCL 6, а затем нажмите кнопку «Далее». В следующем окне нажмите кнопку «Готово».

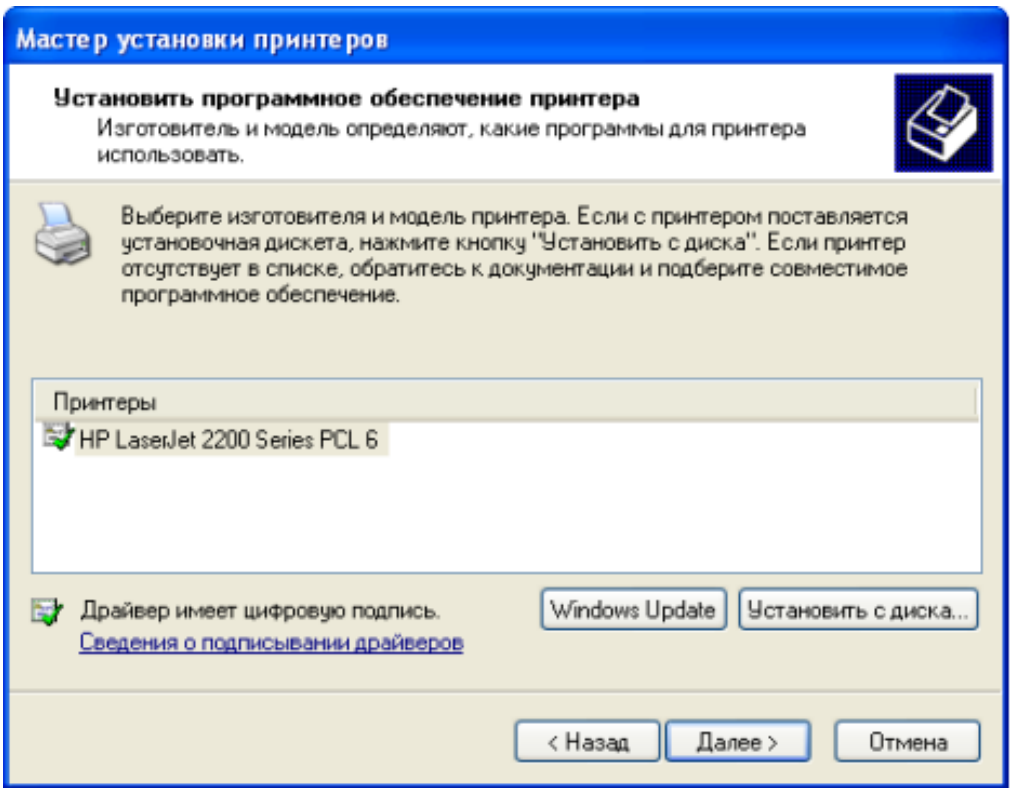


Рис. 16. Завершение процесса установки нового драйвера.

р. После завершения процесса вернитесь к окну свойств принтера и нажмите кнопку «Применить», а затем – «ОК».

Шаг 4. Проверка установки нового драйвера

На этом шаге требуется сравнить свойства драйвера Windows по умолчанию, установленного на первом шаге, с недавно установленным драйвером с веб-узла производителя.

а. В окне свойств нового принтера убедитесь, что кнопка «Применить» отображается серым цветом (недоступна).

б. Перейдите на вкладку «Дополнительно». Какое у драйвера название?

Название драйвера: _____

в. Перейдите на вкладку «Конфигурация». Окно для HP LaserJet 2200 показано на следующем рисунке.

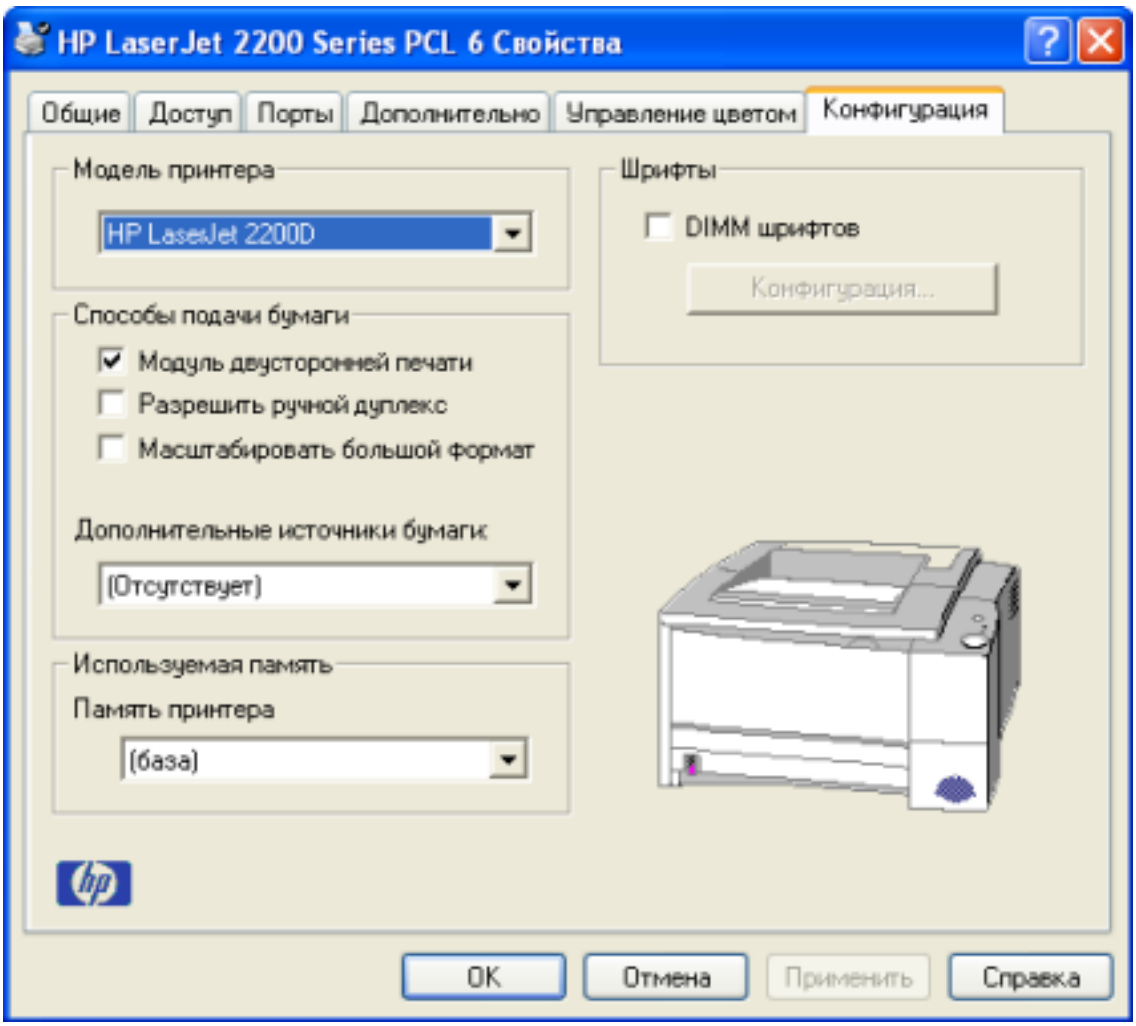


Рис. 17. Изменение набора свойств в окне настройки принтера.

г. Сравните данную вкладку с вкладкой «Параметры устройства» на шаге 2г. Какие есть отличия?

1	
2	
3	

д. Просмотрите некоторые другие вкладки окна свойств, чтобы сравнить новый и старый драйверы. Запишите некоторые отличия.

Установка и настройка сетевого принтера

Сетевые принтеры - выгодная альтернатива принтерам локальным. Один большой и производительный аппарат способен гораздо быстрее справляться с заданиями печати, чем несколько мелких. Чтобы сервис печати был доступен всем пользователям сети принтер должен быть сетевым.

Существует несколько способов "превращения" обычного принтера в сетевой:

1. Через предоставление в общий доступ обычного локального принтера.
2. Через специализированную службу - принт-сервер
3. С помощью встроенной в принтер сетевой карты (специальный тип принтера - сетевой принтер).

1. Настройка локального принтера для общего доступа
Это самый простой в исполнении, но самый ограниченный по возможностям вариант сетевого использования принтера. Он подразумевает, что принтер, который должен быть доступен нескольким пользователям сети, подключен к одному из компьютеров и сделан общедоступным сетевым ресурсом. Настроенный таким образом принтер будет доступен всем пользователям данной сети только тогда, когда включен не только сам принтер, но и тот компьютер, к которому он подключен локально.
До начала настройки принтер должен быть установлен описанным выше способом на компьютере, к которому он физически подключен при помощи параллельного или USB кабеля (с диска, поставляемого с принтером или с использованием драйверов, скачанных с веб-сайта производителя принтера).

1 Шаг. Предоставление принтера в общий доступ. Откройте папку "Принтеры и факсы". Кликнете правой кнопкой мыши на установленном в системе принтере и выберите пункт меню "Свойства". Появится окно свойств, в котором необходимо выбрать вкладку "Доступ":

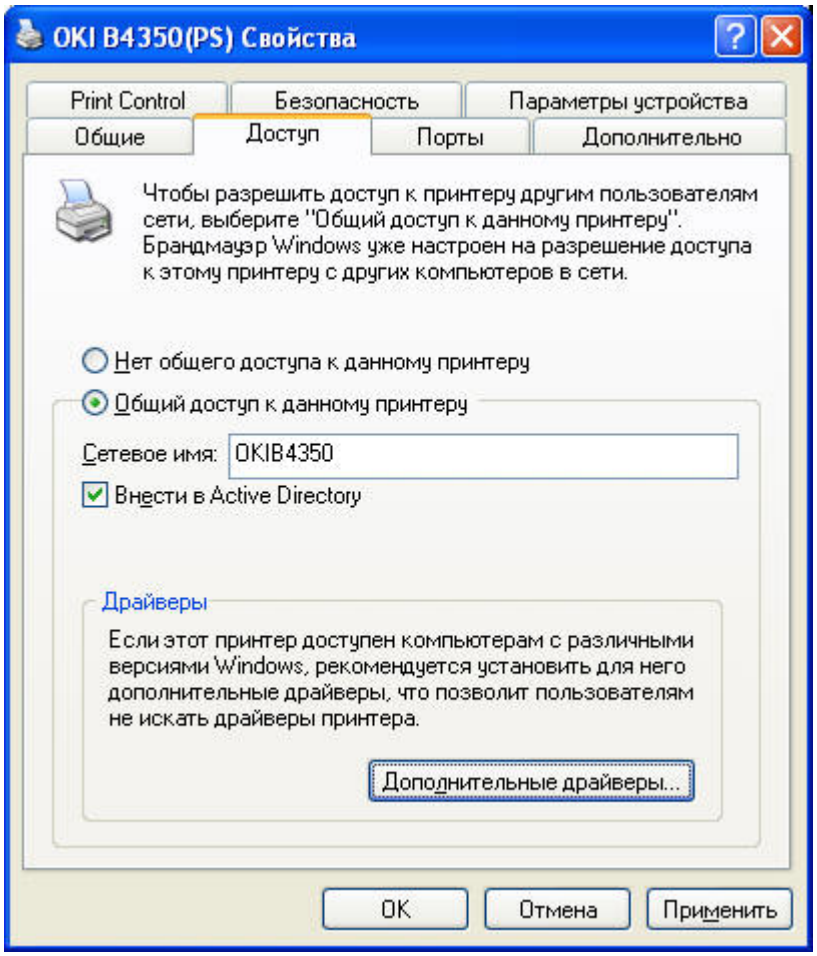


Рис. 18. Предоставление общего доступа по сети к локальному принтеру.

На этой вкладке нужно разрешить общий доступ к принтеру и ввести имя, под которым он будет виден в сети (можно оставить имя по умолчанию, предложенное компьютером). Сетевое имя лучше делать без пробелов. Если на всех компьютерах в сети установлена та же версия Windows, что и на том, к которому подключен принтер, то после этого достаточно нажать кнопку "OK", чтобы завершить эту процедуру. Если в сети есть компьютеры с другими версиями Windows, то нужно нажать кнопку "Дополнительные драйверы" и выбрать из списка те драйверы, которые понадобятся для компьютеров с другими версиями операционной системы:

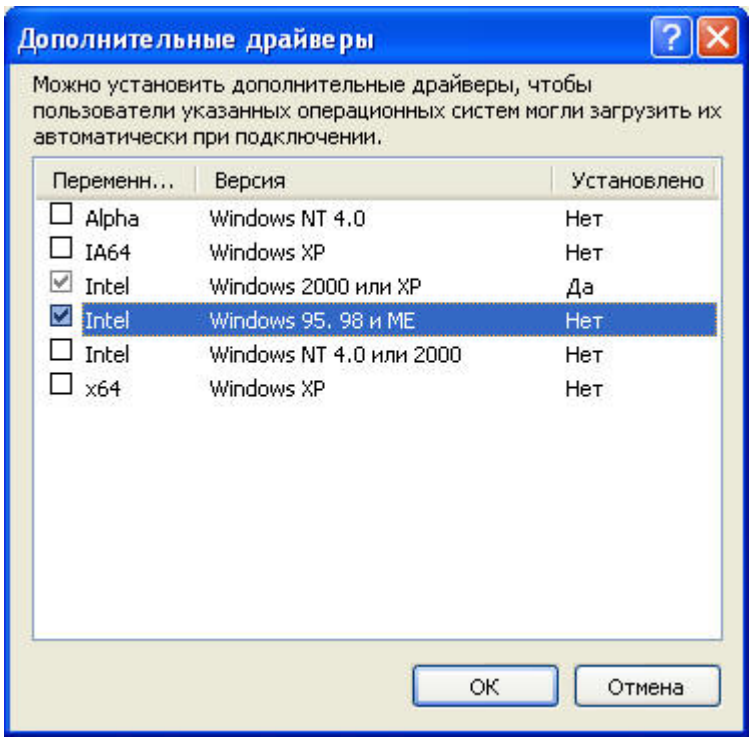


Рис. 19. Поддержка других операционных систем.

Обратите внимание, что если в колонке "Установлено" значится "Нет", то после этого потребуется вставить установочный диск производителя принтера или скачать выбранный драйвер с его сайта!

Для того, чтобы на всех компьютерах в сети мы могли пользоваться созданным общим сервисом печати, на каждом удалённом компьютере нужно запустить мастер установки принтера. Когда появится окно, предлагающее выбрать способ подключения принтера, необходимо выбрать "Сетевой принтер" и нажать кнопку далее:

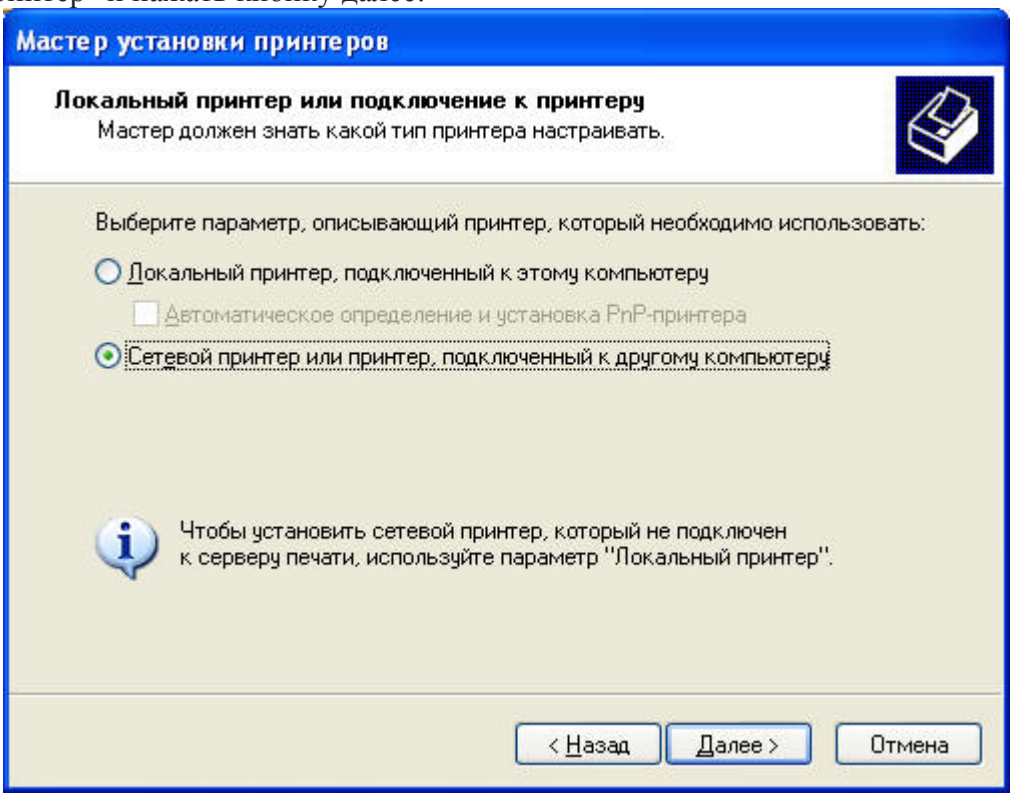
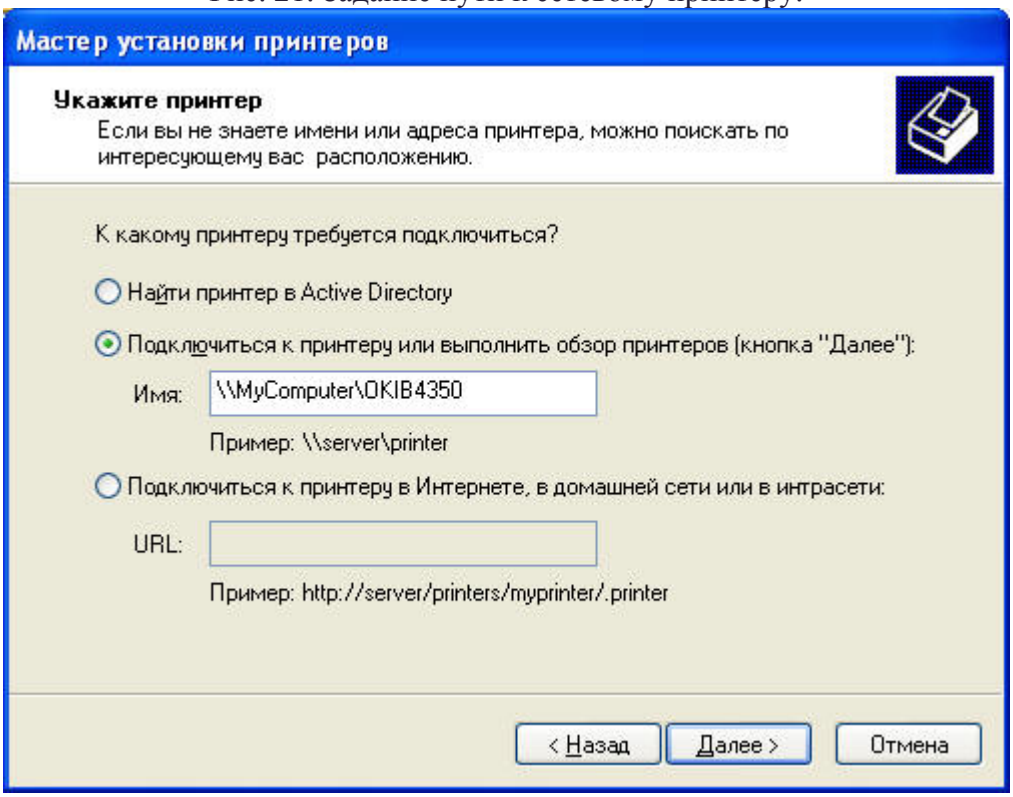


Рис. 20. Установка сетевого принтера в мастере установки.

После этого нужно указать сетевой путь к принтеру. Обратите внимание на синтаксис: это обязательно два обратных слэша, после которых без пробела идёт сетевое имя компьютера, к которому подключен принтер (в примере на рисунке сетевое имя компьютера - "MyComputer"), затем снова обратный слэш и сетевое имя принтера, присвоенное ему на этапе создания общего ресурса (в примере "OKIB4350"):

Рис. 21. Задание пути к сетевому принтеру.



Сетевое имя компьютера, к которому подключен принтер, можно узнать, если нажать на этом компьютере правой кнопкой мышки на иконке "Мой компьютер" и выбрать там Свойства и вкладку "Имя компьютера".

После выполнения указанных действий и нажатия клавиши "Далее", процесс установки драйвера пойдёт автоматически и по его окончании будет предложено распечатать пробную страницу, что обязательно нужно сделать для проверки правильности настройки.

Альтернативный способ установки драйвера на удалённом компьютере. Вместо автоматической установки указанным выше способом, можно пойти другим путём. Установить на удалённом компьютере принтер так, будто он подключен напрямую к этому компьютеру, но не дав возможности системе автоматически определять PnP-принтер на этапе выбора варианта подключения. Далее проще всего выбрать подключение через параллельный интерфейс LPT1 (вне зависимости от того, есть такой интерфейс у принтера или нет):

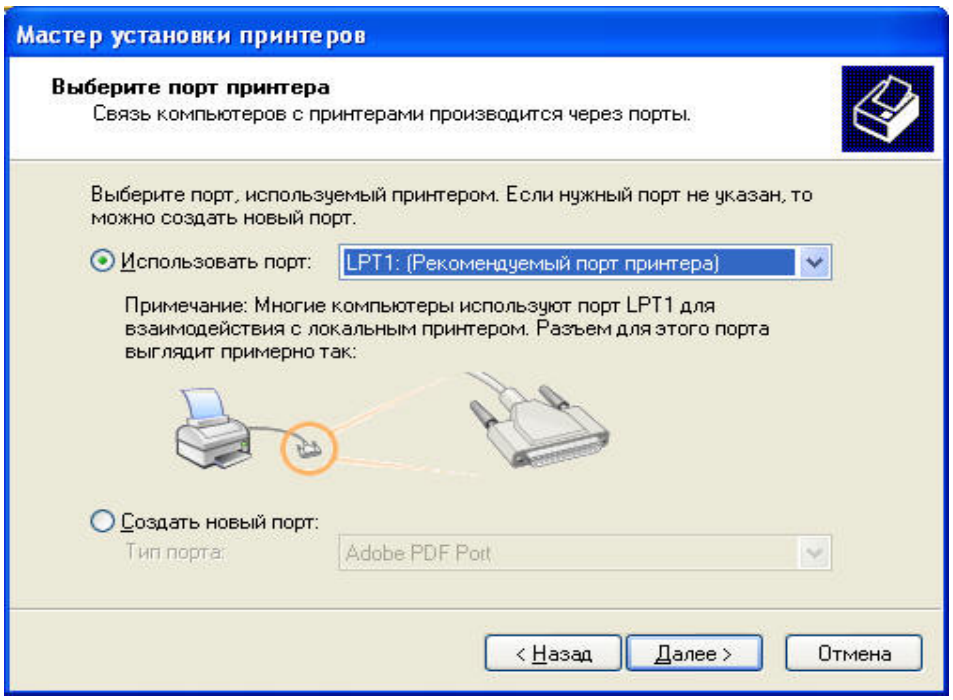
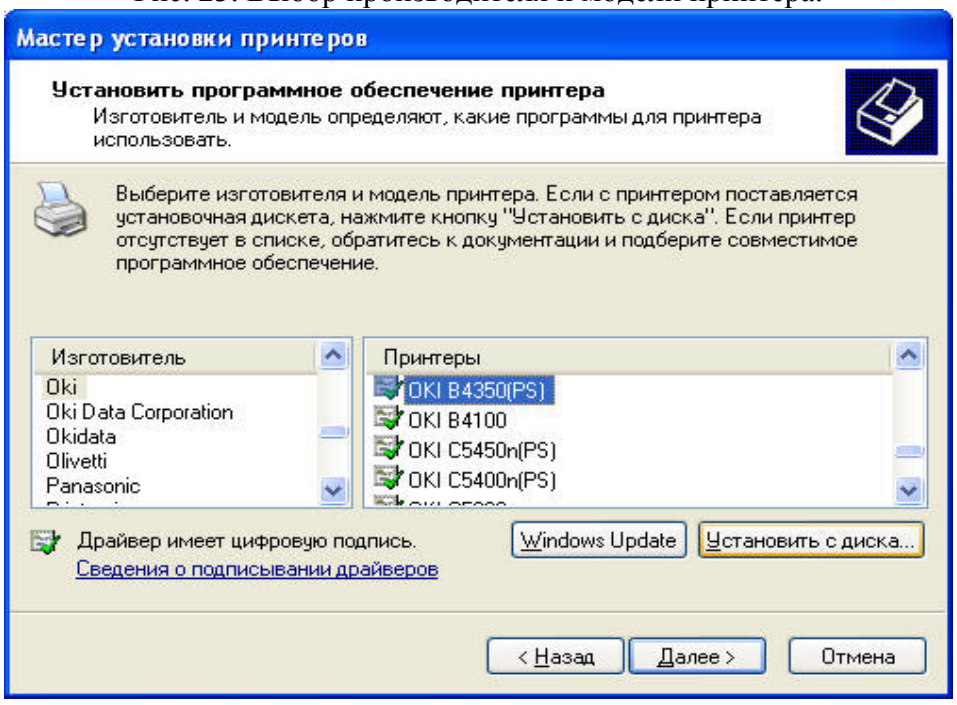


Рис. 22. Выбор порта подключения принтера.

После чего будет предложен выбор драйвера из числа поставляемых вместе с системой. Если драйвер вашего принтера в этом списке присутствует, просто выберите его. Если не присутствует (что всегда бывает в случае подключения GDI-принтеров), то необходимо нажать кнопку "Установить с диска", после чего выбрать место хранения драйвера принтера либо на компакт-диске, поставляемом с принтером, либо скаченного с веб-сайта производителя и разархивированного на вашем компьютере.

Рис. 23. Выбор производителя и модели принтера.



После выбора модели, далее процесс установки пойдёт автоматически и снова будет предложено напечатать тестовую страницу. Сейчас этого делать не стоит, так как физически к нашему компьютеру принтер не подключен и печать не получится. Теперь мы кликаем правой кнопкой мыши на установленном принтере в папке "Принтеры и факсы" и выбираем

"Свойства", после чего в открывшемся окошке выбираем вкладку "Порты" и нажимаем внизу кнопку "Добавить порт". Появится окошко выбора типа порта:

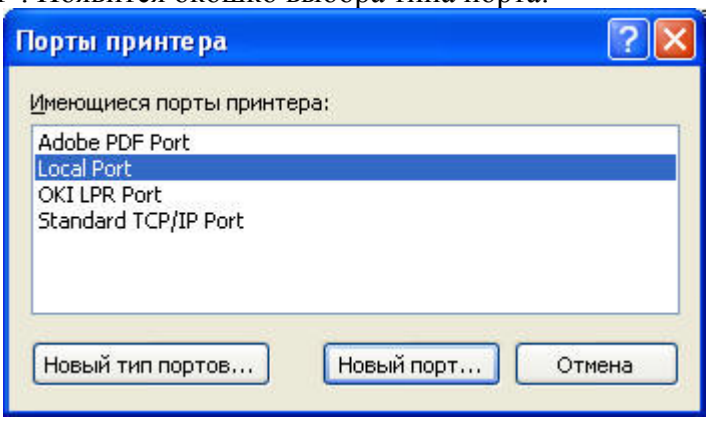


Рис. 24. Выбор типа физического порта для подключения принтера.

Тут нужно выбрать вариант "Local Port" и нажать кнопку "Новый порт". В появившемся маленьком окошке мы вводим путь к нашему сетевому принтеру в том же формате и по тем же правилам, что было описано выше и нажимаем OK:

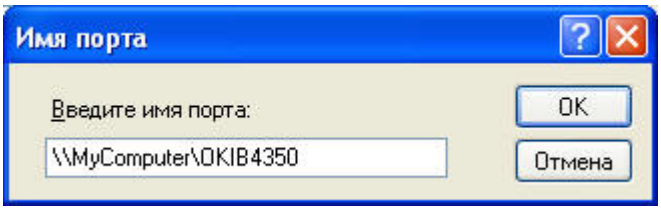


Рис. 25. Указание сетевого места расположения порта принтера.

Теперь сетевой принтер подключен к удалённому компьютеру и можно попытаться на него что-нибудь распечатать. Достоинства такого способа подключения к сетевому принтеру:

- Не требуется никакого дополнительного оборудования помимо того, что уже используется для реализации локальной сети.
- Этот способ является стандартным для сетей Microsoft Windows ещё со времён Windows for Workgroups, прост в установке и не требует дополнительного софта.

Недостатки такого способа подключения к сетевому принтеру:

- Компьютер, к которому принтер подключен физически, обязательно должен быть включен для того, чтобы было возможно пользоваться этим принтером с других компьютеров.
- В процессе печати с удалённых компьютеров тот, к которому подключен принтер, немного замедляет свою работу, занимаясь обработкой данных для печати, что может быть довольно неудобно для человека, работающего на этом компьютере, особенно если компьютер не очень быстрый (в этом случае замедление будет гораздо более заметным).
- Если принтер подключен через параллельный порт, то скорость передачи данных на него будет довольно низкой. Особенно это почувствуется при цветной печати.
- Принтеры, подключенные таким образом, не смогут работать в сети, разделённой на сегменты маршрутизаторами, потому как протокол NetBEUI, используемый для реализации этого подключения, не является маршрутизируемым.

2. Подключение через внешний аппаратный принт-сервер.
Существует множество производителей, которые предлагают различные реализации внешних принт-серверов, позволяющих подключать обычные принтеры к сети (рис. 26).

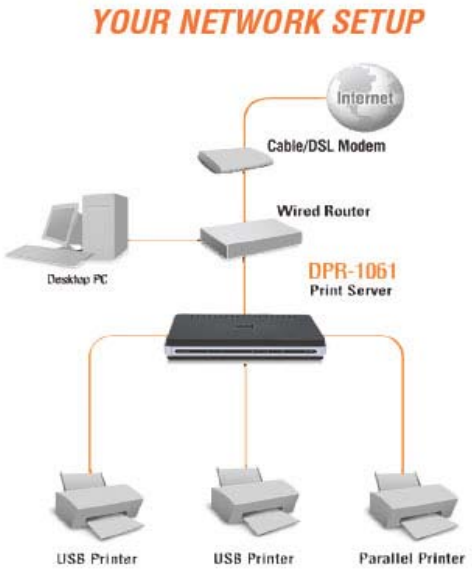


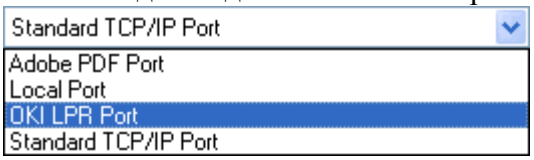
Рис. 26. Аппаратный принт-сервер.

Представлять из себя эти принт-серверы могут либо небольшую "коробочку", в которой с одной стороны есть разъём RJ-45 для подключения сетевого кабеля, а с другой разъём параллельного порта, либо разъём для подключения USB-кабеля. Либо это может быть комбинированное решение, представляющее из себя, к примеру, точку доступа к беспроводной сети, сетевой концентратор, клиента VPN и принт-сервер, подключаемый к принтеру через USB-порт. Но вне зависимости от физической реализации принт-сервера, способ установки принтеров, подключенных к нему, будет одинаков.

Прежде всего необходимо установить сам принт-сервер. Делается это в соответствии с инструкциями, приложенными к нему и при помощи программного обеспечения, поставляемого с принт-сервером. Обычно это специальная программа, которая помимо всего прочего, должна установить в принт-сервере IP-адрес и маску подсети (subnet mask), соответствующие адресации, принятой в вашей локальной сети (например, адрес 192.168.2.100 и маска подсети 255.255.255.0). После того, как мы установили IP-адрес, нужно проверить его работоспособность. Для этого можно воспользоваться программой командной строки ping или зайти на внутренний веб-сервер устройства, введя установленный на устройстве адрес в адресную строку браузера. Убедившись в том, что принт-сервер виден в сети, приступим к установке принтера.

В общем установка выполняется аналогично уже описанным выше примерам. При выборе типа устанавливаемого принтера, несмотря на то, что принтер будет сетевым, мы выбираем вариант "Локальный принтер, подключенный к этому компьютеру", после чего активизируем пункт "Создать новый порт" и выбираем в выпадающем списке "Standard TCP/IP Port":

Рис. 27. Выбор порта TCP/IP для подключения к аппаратному принт-серверу.



Это самый простой вариант, работающий в большинстве случаев. Однако, производители принт-серверов могут предлагать альтернативные варианты реализации IP-стека для печати и эти варианты могут автоматически устанавливаться на этапе установки принт-сервера при помощи приложенной к нему программы. Например, на рисунке 27 видно, что среди вариантов выбора порта подключения присутствует OKI LPR Port, который добавляется при установке в систему принт-сервера OKI. Если мы выберем этот вариант, то при нажатии на кнопку "Далее"

нам будет предложено ввести IP-адрес и имя очереди для нашего сетевого принтера. Здесь необходимо ввести именно тот адрес, который мы присвоили нашему принт-серверу на этапе его установки. Имя очереди - это, обычно, любое удобное для вас слово. Однако, в некоторых случаях необходимо использовать заданные производителем принт-сервера имена очередей, без точного указания которых принтер не сможет работать!
Плюсы такого способа подключения к сетевому принтеру:

- Принтер становится полноценным и самостоятельным сетевым устройством, не требующим работающего компьютера для печати
- Принт-сервер может быть лишь "бонусом" при покупке, скажем, универсального маршрутизатора, совмещенного с небольшим коммутатором и точкой доступа к беспроводной сети Wi-Fi.

Недостатки такого способа подключения к сетевому принтеру:

- Ограниченная возможность контролирования состояния очереди печати и других параметров сетевого принтера. Внешние принт-серверы обычно предлагают лишь возможность определить состояние принтера - готов он к работе или нет, а также задать параметры порта, через который он подключен.
- Для питания внешнего принт-сервера требуется дополнительный источник питания.
- Если для подключения принтеров к принт-серверу используется кабель с параллельным интерфейсом LPT, то из-за невысокой скорости передачи данных по такому кабелю будут возникать задержки при печати, особенно цветных документов.

3. Подключение через "родную" сетевую карту/принт-сервер.
Многие принтеры подразумевают установку в них внутренней сетевой платы, сделанной специально для этой модели (или для нескольких моделей этого производителя). В этом случае плата устанавливается на внутреннюю системную шину принтера и потому данные передаются на принтер на максимально возможной для сети скорости. Кроме того, внутренняя сетевая плата позволяет осуществлять управление принтером через сеть, в то же время, через панель управления принтером можно изменять настройки сетевой платы.
Если принтер оснащён сетевой платой, то производитель, предлагает и соответствующее программное обеспечение, поставляемое вместе с принтером. В этом случае достаточно указать, что принтер является сетевым и программа-установщик настроит всё автоматически. Возможно придётся лишь указать IP-адрес принтера, если он не был ему присвоен автоматически вашим DHCP или BOOTP сервером. Иногда, если адрес не присвоен автоматически, требуется установить его вручную - либо с панели управления принтера, либо с использованием внешней программы, поставляемой на диске или доступной для скачивания на веб-сайте производителя. К примеру, у OKI такая программа называется NIC Setup Utility. Она позволяет найти в сети все сетевые принтеры OKI и присвоить им IP-адреса и маски подсети. Подобные же утилиты есть и у других производителей. Автоматический установщик, находящийся на фирменном диске, обычно устанавливает всё необходимое для работы сетевого диска и нам остаётся только дождаться окончания процесса установки.

Если фирменного диска нет, то необходимо установить компоненты вручную. В этом случае установка не будет отличаться от той, что описана выше для внешнего принт-сервера. Единственным отличием может стать то, что стек TCP/IP протоколов для поддержки сетевой печати может потребоваться установить отдельно вручную. Рекомендуется это делать, а не использовать стандартную систему печати Microsoft TCP/IP Printing, так как при установке фирменного LPR-протокола передача данных будет более стабильной, более скоростной и вам будет доступно несколько полезных функций, таких как, например, объединение принтеров в пул или перенаправленние печати на альтернативные сетевые принтеры.

При установке драйвера вручную, проще всего сначала установить его "на параллельный порт" так, как описано выше, а потом запустив LPR-утилиту переключить принтер на неё.

Плюсы такого способа подключения к сетевому принтеру:

- Это полностью интегрированное, профессиональное решение, позволяющее реализовать сетевую печать наиболее эффективным образом
- Высокая скорость передачи данных на сетевой принтер, не ограниченная медленными интерфейсами
- Возможность удалённого мониторинга сетевого принтера, в том числе через внутренний веб-сервер принтера с отслеживанием всех его состояний.
- Управление сетевыми настройками карты может осуществляться непосредственно с панели управления принтера.
- Нет необходимости использовать дополнительный источник питания или задействовать один из компьютеров в сети.

Ограничения такого способа подключения к сетевому принтеру:

- Принтеры с встроенной сетевой картой имеют более высокую цену.

Лабораторная работа №3 Настройка простого сетевого соединения

Часть 1 Соединение двух персональных компьютеров без промежуточных устройств.

Рис. 1. Прямое соединение двух компьютеров сетевым кабелем.

Задачи

• Построить простую одноранговую сеть и проверить физическое подключение.

• Назначить узлам разные IP-адреса и пронаблюдать за их влиянием на сетевое взаимодействие.

Исходные данные / подготовка

В первой части лабораторной работы требуется построить простую одноранговую сеть с помощью двух компьютеров и перекрестного кабеля Ethernet. Потребуется назначать узлам различные совместимые и несовместимые IP-адреса и отслеживать их влияние на возможность взаимодействия.

Для проведение работы потребуются следующие ресурсы:

• два ПК с Windows XP Professional, на каждом из которых установлена и функционирует сетевая интерфейсная плата;

• перекрестный кабель Ethernet для соединения ПК (предоставляется преподавателем);

Шаг 1. Соединение ПК для создания одноранговой сети

а. Возьмите у преподавателя перекрестный кабель Ethernet для соединения двух ПК.

б. Вставьте один конец кабеля в сетевую плату Ethernet компьютера PC1. Другой конец кабеля вставьте в сетевую плату Ethernet компьютера PC2. При подключении конца кабеля должен быть слышен щелчок, указывающий на то, что кабель вставлен в порт правильно.

Шаг 2. Проверка физического соединения

а. После подключения перекрестного кабеля Ethernet к обоим ПК, внимательно осмотрите каждый порт Ethernet. Световая индикация канала (обычно зеленого или желтого цвета) означает, что между двумя сетевыми платами установлено физическое соединение. Попробуйте отключить кабель от одного из ПК, а затем снова подключить, чтобы проверить, как световая индикация отключается и снова включается.

б. Перейдите в «Панель управления», дважды щелкните значок «Сетевые подключения» и убедитесь, что подключение по локальной сети установлено. На рисунке 2 показан пример активного подключения по локальной сети. При наличии неполадок физического подключения

на значке «Подключение по локальной сети» виден знак X и сообщение: «Сетевой кабель не подключен».

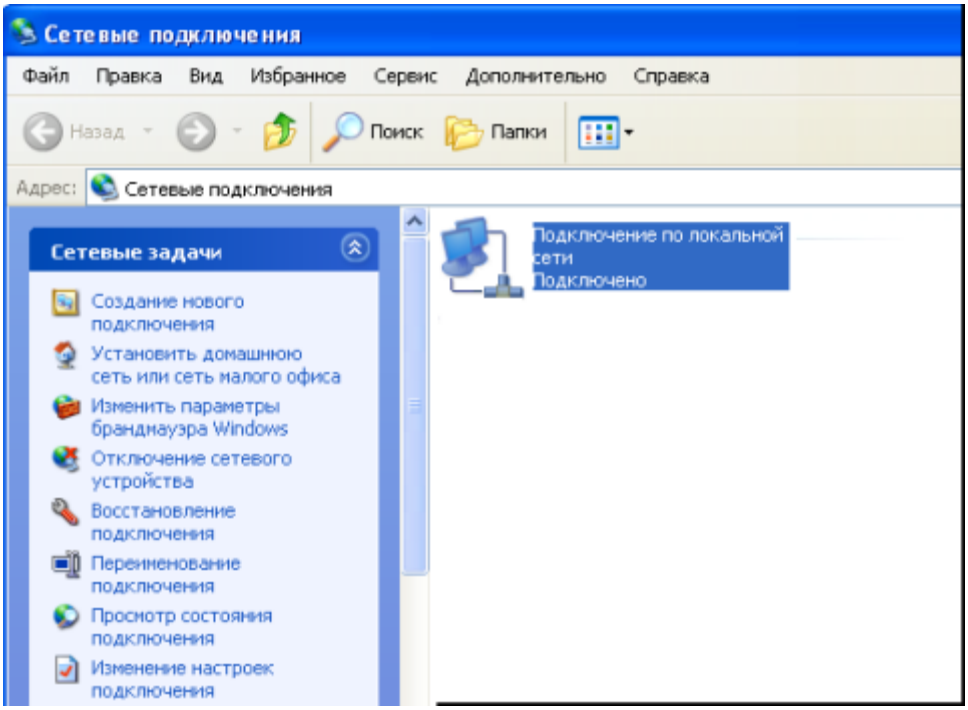


Рис. 2 Состояние сетевого подключения.

в. Если в значке «Подключение по локальной сети» не указывается, что соединение установлено, устраните неполадки, повторив шаги 1 и 2. Можно также попросить преподавателя подтвердить, что используется перекрестный кабель Ethernet.

Шаг 3. Настройка параметров IP для двух ПК

а. Настройте логические IP-адреса двух ПК, чтобы они могли связываться по протоколу TCP/IP. На компьютере PC1 перейдите в панель управления, дважды щелкните значок «Сетевые подключения» и правой кнопкой мыши щелкните значок установленного подключения по локальной сети. В раскрывающемся меню выберите пункт «Свойства».

б. С помощью полосы прокрутки в окне «Подключение по локальной сети – свойства», прокрутите список до элемента «Протокол Интернета (TCP/IP)». Нажмите кнопку «Свойства».

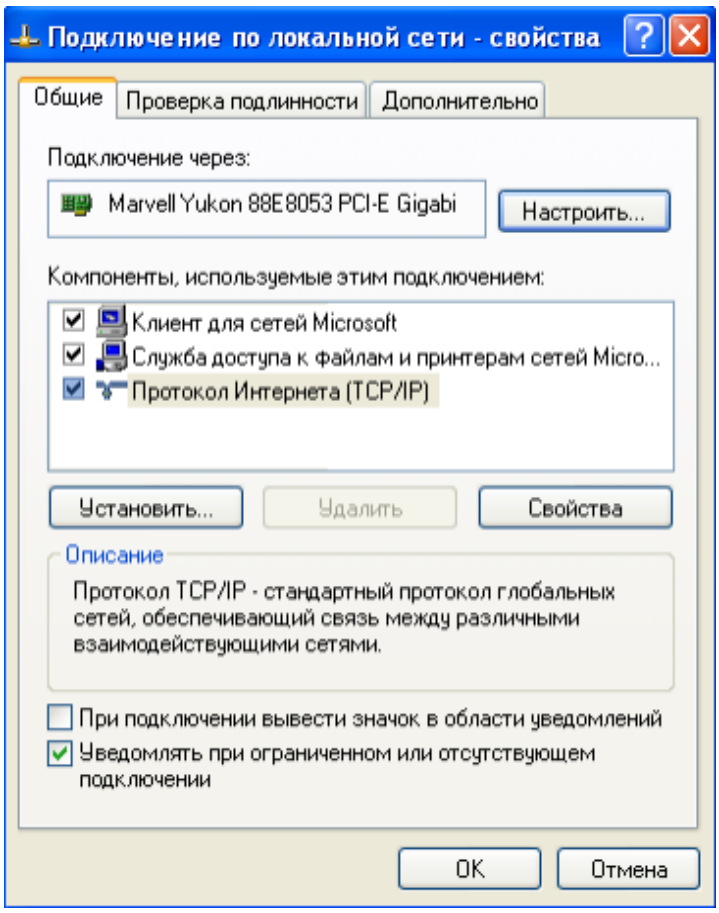
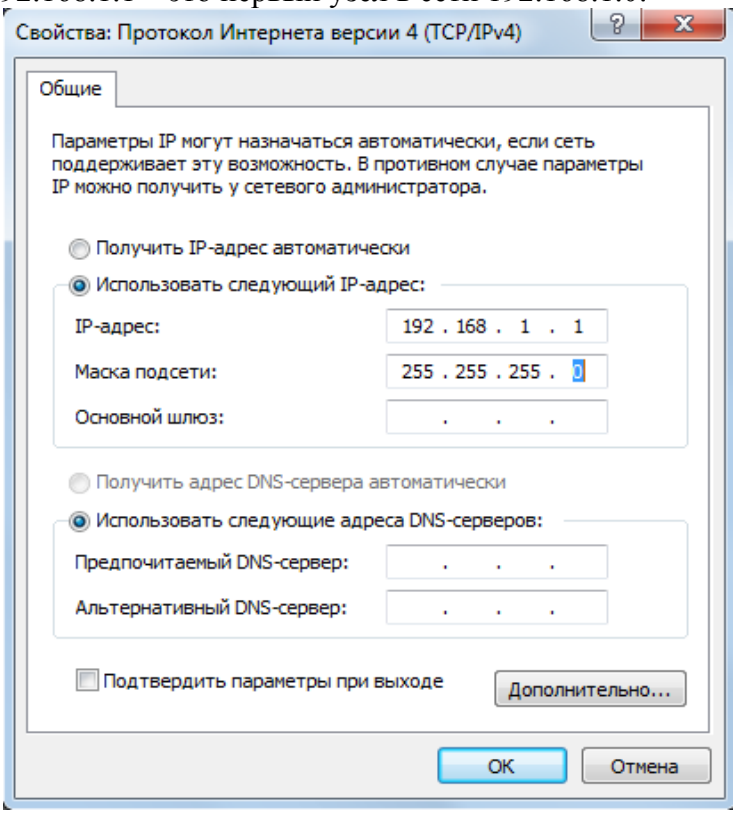


Рис. 3. Настройка свойств протокола Интернета.

в. Установите переключатель «Использовать следующий IP-адрес» и введите IP-адрес 192.168.1.1 и маску подсети 255.255.255.0. С данными IP-адресом и маской подсети номер сети узла – 192.168.1.0, а 192.168.1.1 – это первый узел в сети 192.168.1.0:



-адрес 192.168.1.1 Маска подсети 255.255.255.0 Рис. 4. Настройка статического IP-адреса на сетевом интерфейсе

г. Нажмите кнопку «ОК», чтобы закрыть окно «Свойства: Протокол Интернета (TCP/IP)». Нажмите кнопку «Закрыть», чтобы закрыть окно «Подключение по локальной сети – свойства».

д. Повторите шаги 3a – 3d для компьютера PC2, используя IP-адрес 192.168.1.2 и маску подсети 255.255.255.0. Номер сети данного ПК – 192.168.1.0, а 192.168.1.2 – это второй узел в сети 192.168.1.0.

IP-адрес	192.168.1.2
Маска подсети	255.255.255.0

Шаг 4. Проверка IP-соединения между двумя ПК

ПРИМЕЧАНИЕ. Для проверки соединения TCP/IP на обоих ПК необходимо временно отключить межсетевой экран Windows либо разрешить прохождение эхо-пакетов протокола ICMP. После завершения проверки межсетевой экран Windows следует снова включить.

а. На рабочем столе Windows XP обоих ПК нажмите кнопку «Пуск». В меню «Пуск» выберите пункт «Панель управления» и дважды щелкните значок «Сетевые подключения».

б. Правой кнопкой мыши щелкните значок «Подключение по локальной сети» и выберите пункт «Свойства». Перейдите на вкладку «Дополнительно». Найдите и нажмите кнопку «Параметры».

в. Проверьте, какие у межсетевого экрана настройки: «ВКЛЮЧЕН (ВКЛ.) для порта Ethernet» или «ВЫКЛЮЧЕН (ВЫКЛ.) для порта Ethernet».

_____

г. Если межсетевой экран включен, установите переключатель «Выключить (не рекомендуется)», чтобы отключить межсетевой экран. В дальнейшем межсетевой экран будет снова включен. Нажмите кнопку «ОК» в данном диалоговом окне и в следующем, чтобы применить изменения. Повторите шаги 4a – 4d на втором ПК.

д. Теперь, когда два ПК физически соединены и в них правильно настроены IP-адреса, необходимо убедиться в их способности связываться друг с другом. Команда ping – самый простой способ выполнения этой задачи. Команда ping включена в операционную систему Windows XP:

е. На компьютере PC1 нажмите кнопку «Пуск», а затем выберите команду «Выполнить». Введите команду cmd, а затем нажмите кнопку «ОК». Откроется окно командной строки Windows (см. рисунок ниже).

ж. В командной строке > введите ping 192.168.1.2 и нажмите клавишу ВВОД. Успешное выполнение команды ping подтверждает IP-подключение. Пример выходных данных представлен ниже.

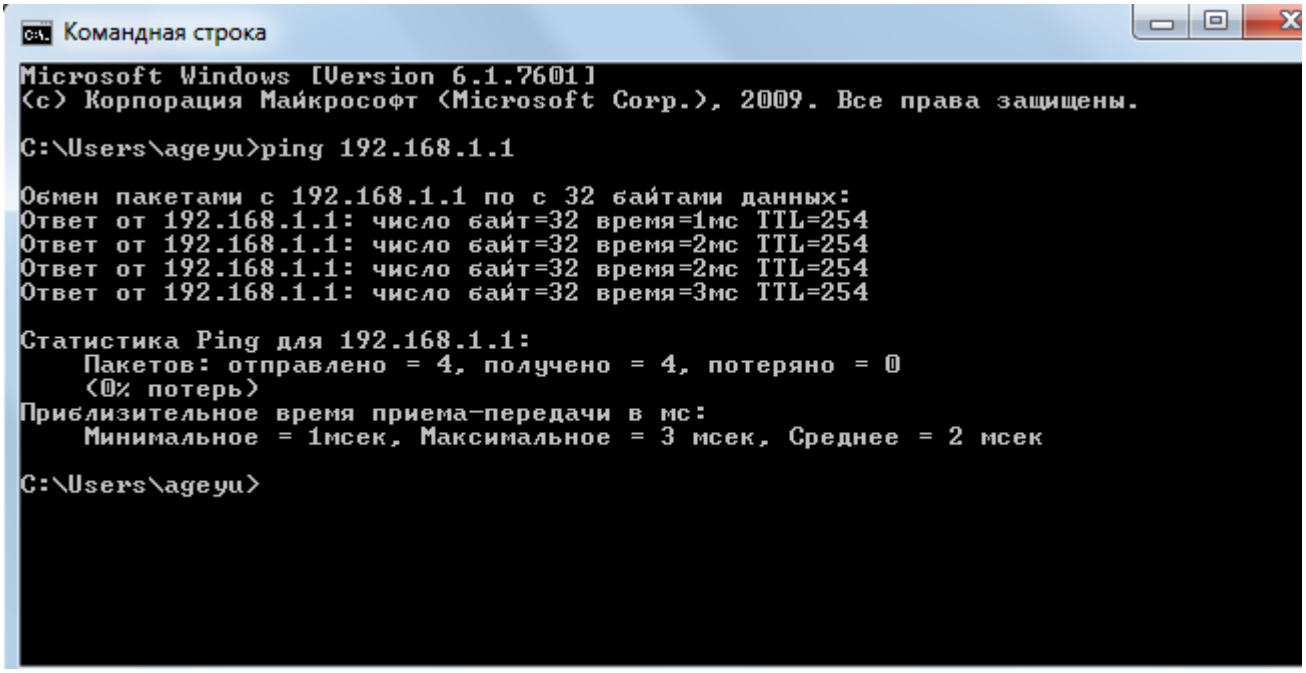


Рис. 5. Проверка состояния сетевого соединения.

Лабораторная работа №4 Сервисы совместного доступа, разрешения имен и обмена файлами

Часть 1. Использование сервиса совместного доступа к файлам Microsoft Windows

Задачи

С помощью операционной системы Windows выполнить следующие задачи:

- открыть общий доступ к файлам и папкам;
- подключить сетевые диски.

Исходные данные / подготовка

Одно из ключевых преимуществ взаимодействующих по сети компьютеров – предоставление возможности совместного использования информации с другими подключенными пользователями. Это может быть музыкальная композиция, предложение или праздничные рисунки, существует много ситуаций, в которых требуется предоставить общий доступ к данным друзьям и коллегам по работе.

Подключение дисков сопутствует предоставлению общего доступа к папкам, так как при этом предоставляется быстрый доступ к часто используемым папкам. Подключенные диски также обеспечивают пользователям самый простой способ перемещения по каталогам и поиска нужных файлов и/или папок. При подключении дисков локальный ресурс (буква диска) сопоставляется общему сетевому ресурсу (жесткому диску или папке в сети).

Требуются следующие ресурсы:
- две настроенные рабочие станции Windows XP Professional, связанные через локальную сеть.

Примечание. Воспользуйтесь сетью, ранее настроенной на лабораторном занятии 3.6.5.

Шаг 1. Предоставление общего доступа к папке
а. Нажмите кнопку «Пуск» и выберите «Все программы», «Стандартные», а затем – «Проводник».
б. В панели «Папки» щелкните знак плюса (+) рядом с элементом «Мой компьютер». Выберите диск C:. В меню «Файл» откройте подменю «Создать» и выберите пункт «Папку». Введите «Share» в качестве имени папки.

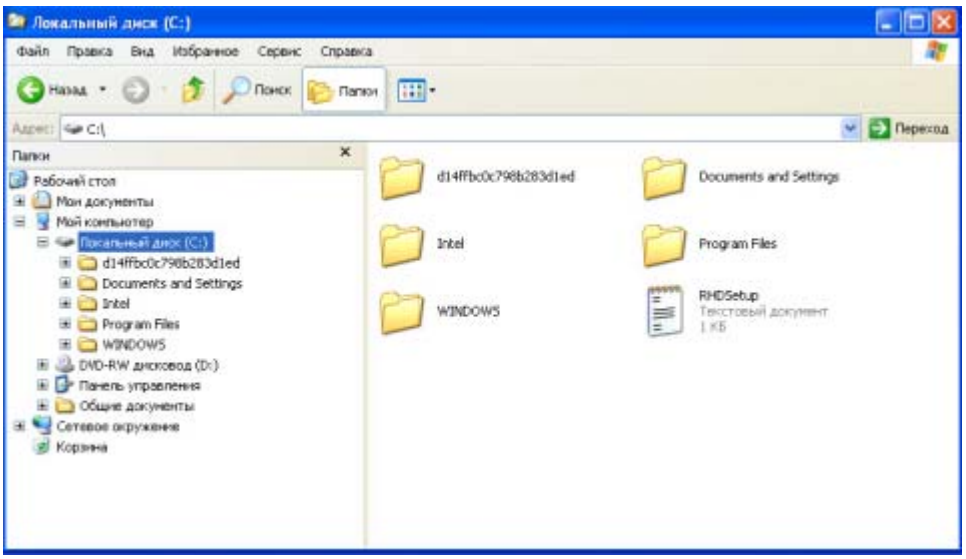


Рис. 1. Выбор папки для предоставления в общий доступ.

в. Правой кнопкой мыши щелкните имя новой папки «Share» и выберите пункт «Свойства».
ПРИМЕЧАНИЕ. Возможность совместного использования недоступна для каталогов «Documents and Settings», «Program Files» и системных папок Windows.
г. Перейдите на вкладку «Доступ». В диалоговом окне «Свойства: Share» установите переключатель «Открыть общий доступ к этой папке», чтобы открыть общий доступ к данной папке другим пользователям локальной сети. По умолчанию у общей папки такое же имя, что и у исходной папки.
ПРИМЕЧАНИЕ. Чтобы изменить имя папки в сети, введите новое имя папки в текстовом поле «Общий ресурс». Это не меняет имя папки на компьютере.

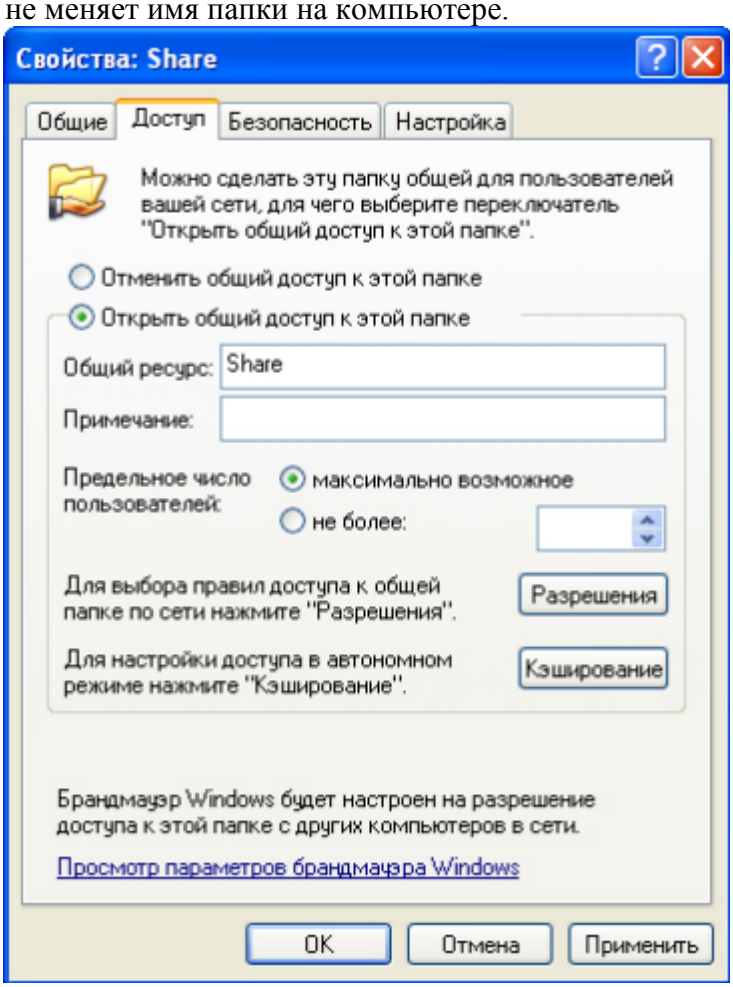


Рис. 2. Разрешение общего доступа к выбранной папке по сети.

д. Нажмите кнопку «Применить», а затем – «ОК».
е. Создайте текстовый файл с помощью программы «Блокнот» и сохраните его в папке «Share».

На рабочем столе Windows XP нажмите кнопку «Пуск» и выберите «Все программы», «Стандартные», а затем – «Блокнот».
В приложении «Блокнот» введите сообщение «Hello World!».
В меню «Файл» выберите команду «Сохранить». В поле «Имя файла» введите «Пробное сообщение». Щелкните значок с папкой и со стрелкой, как показано на следующем рисунке.

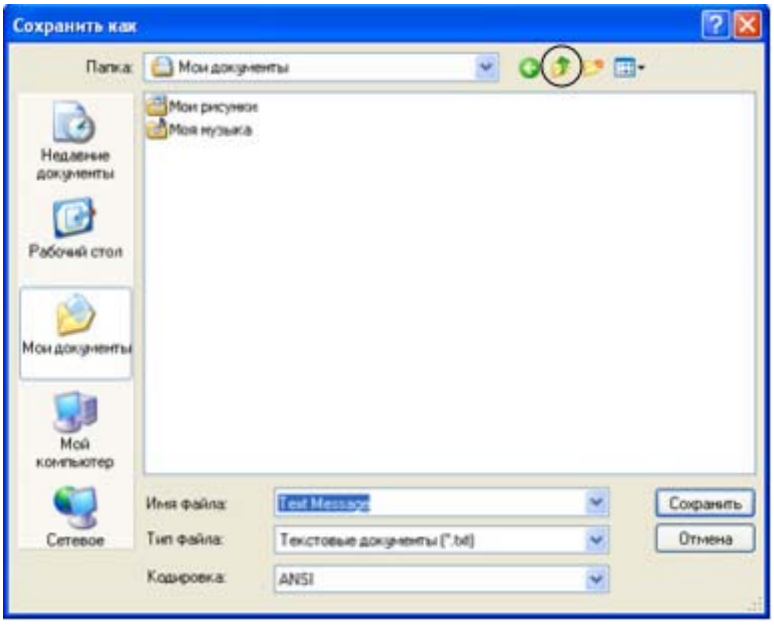


Рис. 3. Создание текстового файла и сохранение его в папке, открытой для совместного доступа.

ж. Дважды щелкните «Мой компьютер», а затем – букву диска «C:». Найдите и дважды щелкните значок папки «Share», а затем нажмите кнопку «Сохранить».
з. Закройте приложение «Блокнот».
и. Повторите шаги 1 – 5 на втором компьютере Windows XP Professional со следующими исключениями:
Имя общей папки: Share2
Содержимое текстового файла: Hello planet!
Имя текстового файла: Пробное сообщение 2

Шаг 2. Подключение сетевых дисков для предоставления быстрого и простого доступа к общим папкам
а. На первой рабочей станции Windows XP нажмите кнопку «Пуск» и выберите «Все программы»,
«Стандартные», а затем – «Проводник».
б. На панели «Папки» выберите элемент «Мой компьютер». В меню «Сервис» выберите команду
«Подключить сетевой диск…».
в. В текстовом поле «Диск» выберите неиспользованную букву диска в раскрывающемся меню.
г. Вопрос: Какая буква диска выбрана? _____
д. В поле «Папка» введите IP-адрес удаленного ПК и имя удаленного общего ресурса в следующем формате: \\ip-адрес\имя_общего_ресурса

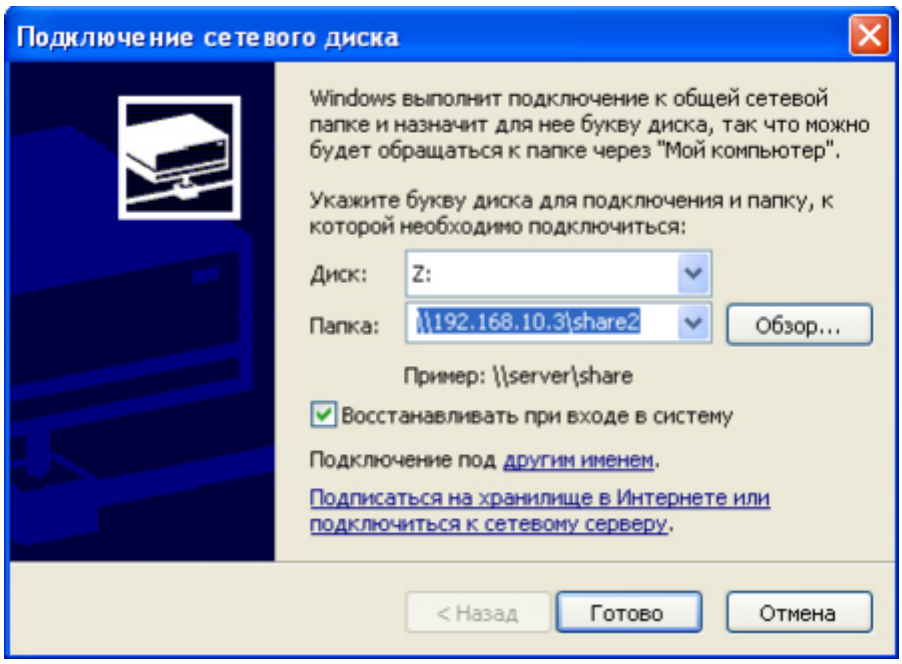


Рис. 4 Создание сетевого ресурса, доступного как локальный логический диск.

е. Нажмите кнопку «Готово».
Откроется окно с сообщением: «Попытка подключения к \\192.168.10.3\share2». Откроется окно с содержимым общей папки «Share2», которой теперь назначена буква диска.
ПРИМЕЧАНИЕ. IP-адрес можно заменить именем компьютера.
ж. Дважды щелкните имя текстового документа «Пробное сообщение 2». Добавьте в документ слова «Техническое правило». В меню «Файл» выберите команду «Сохранить».
Вопрос: Какое сообщение отображается? Как вы думаете, почему это произошло?

_____

_____

з. В версии Windows XP Professional файлы в общей папке автоматически защищены. Нажмите кнопку «ОК» в окне сообщения. Нажмите кнопку «Отмена», а затем – кнопку «Закрыть» для документа «Пробное сообщение 2».
и. В окне сообщения нажмите кнопку «Нет», чтобы закрыть документ без сохранения изменений.
к. Повторите процедуру а-е на шаге 2, чтобы подключить диск на второй рабочей станции Windows XP. Этот диск должен быть сопоставлен общему ресурсу, настроенному на шаге 1.

Шаг 3. Проверка работы
а. На первом компьютере Windows XP нажмите кнопку «Пуск» и выберите «Все программы», «Стандартные», а затем – «Проводник»
б. Раскройте ветку «Мой компьютер», щелкнув знак плюса (+) рядом с именем.
в. В списке проводника должен отображаться диск с буквой диска, выбранной для удаленного общего ресурса.

г. Повторите процедуру а-с на втором компьютере Windows XP Professional.
Если данная буква диска отображается на обоих компьютерах, то общий доступ к папкам и подключение выполнены правильно на обеих рабочих станциях Windows XP. Те же действия можно выполнять для любой папки. При правильном сопоставлении диска общей папке все содержащиеся в ней файлы и папки будут доступны из других рабочих станций локальной сети.

Вопросы для обсуждения
1. Приведите некоторые из преимуществ подключения дисков и общих папок в домашних сетях или в сетях малых офисов.

_____
_____
_____

2. К каким папкам нельзя предоставить общий доступ? Попытайтесь привести причины, почему операционная система может не предоставлять общий доступ к определенным видам папок.

_____
_____
_____

3. Подключенный диск предоставляет указатель на сетевой ресурс, однако буква подключенного файла имеет только локальное значение. Как вы думаете, что такое локальное значение?

_____
_____

Часть 2. **Сервис разрешения имен - DNS**

Задачи

- Отследить преобразование URL-адреса в IP-адрес.
- Отследить поиск в DNS с помощью команды nslookup.

Исходные данные / подготовка

Система доменных имен (Domain Name System - DNS) используется при вводе унифицированного указателя ресурса (URL-адрес), например, http://www.cisco.com, в поле адреса веб-обозревателя.

В первой части URL-адреса указывается используемый протокол. Из них наиболее распространены HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) и FTP (File Transfer Protocol).

Система DNS использует вторую часть URL-адреса, так в приведенном примере это www.cisco.com. Система DNS преобразует доменное имя (подобное www.cisco.com) в IP-адрес, чтобы позволить исходному узлу достичь узла назначения. На данной лабораторной работе работайте в парах.

Требуются следующие ресурсы:

- компьютер под управление Windows с подключением к Интернету;
- доступ к команде Run.

Шаг 1. Отслеживание преобразований DNS

а. Нажмите кнопку «Пуск», выберите команду «Выполнить», введите команду cmd, а затем нажмите кнопку «ОК». Откроется окно командной строки.

б. В командной строке введите ping www.cisco.com. Компьютеру необходимо преобразовать www.cisco.com в IP-адрес, чтобы знать, куда отправлять ICMP-пакеты типа «эхо». Команда ping отправляет пакеты этого типа.

в. В первой строке выходных данных показано имя www.cisco.com, преобразованное в IP-адрес системой DNS. Результаты работы системы DNS должны быть видны, даже если в учебном учреждении есть межсетевой экран, блокирующий обмен пакетами, или если компания Cisco не поддерживает обмен пакетами со своими веб-серверами.

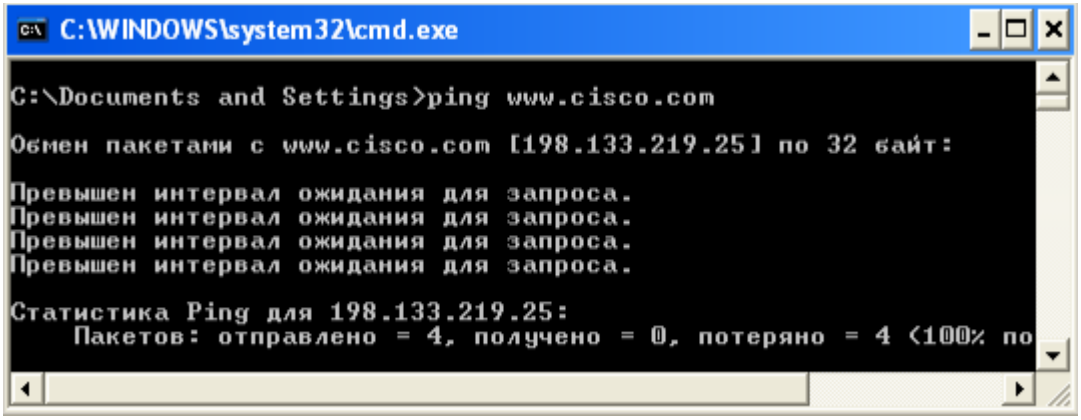


Рис. 5. Разрешение доменного имени, выполняемое в процессе работы программы ping.

г. Какой IP-адрес показан на экране? _____
д. Совпадает ли он с адресом, показанным на представленном выше рисунке? _____
Как думаете, почему это произошло?

_____

е. Обсудите с другими учащимися один или два других случая (кроме команды ping) использования системы DNS.

_____

Шаг 2. Проверка работы системы DNS с помощью команды nslookup

а. В командной строке введите команду nslookup.
б. Какой DNS-сервер используется по умолчанию? _____
в. Обратите внимание на изменение командной строки. Это командная строка NSLOOKUP.
В данной командной строке можно вводить команды, относящиеся к системе DNS.
г. В командной строке введите ?, чтобы просмотреть список всех команд, доступных в режиме NSLOOKUP.
д. Запишите три команды, которые можно использовать в режиме NSLOOKUP.

_____

_____

_____

е. В командной строке NSLOOKUP введите www.cisco.com.
ж. Каков преобразованный IP-адрес? _____
з. Совпадает ли он с адресом из выходных данных команды ping? _____
и. В командной строке введите IP-адрес только что обнаруженного веб-сервера Cisco.
С помощью команды NSLOOKUP можно узнать доменное имя IP-адреса, если URL-адрес не известен.
Используя описанные выше процедуры, найдите IP-адрес, соответствующий имени www.google.com.

_____

Шаг 3. Определение почтовых серверов с помощью команды nslookup
а. В командной строке введите set type=mx, чтобы с помощью команды NSLOOKUP определить почтовые серверы.
б. В командной строке введите www.cisco.com.
в. Какие у данного сервера основное имя, ответственный почтовый адрес и время жизни (TTL) по умолчанию?

_____

_____

г. В командной строке ведите команду exit, чтобы вернуться к обычной командной строке.
д. В этой командной строке введите ipconfig /all.

е. Запишите IP-адреса всех используемых в локальной сети DNS-серверов.

_____

ж. Введите команду exit, чтобы закрыть окно командной строки.

Вопросы для обсуждения

1. Если бы в университете не было DNS-сервера, как бы это сказалось на использовании Интернета?

_____

_____

_____

2. В некоторых компаниях не выделяется отдельный сервер для службы DNS. Вместо этого компьютер, на котором работает DNS-сервер также выполняет и другие функции. Как вы думаете, какие еще функции может выполнять специализированный сервер? В этом случае полезна команда ipconfig /all.

_____

Часть 3. **Изучение протокола FTP**

Задачи

- Продемонстрировать использование протокола FTP из командной строки и графического интерфейса.

Исходные данные / подготовка

Протокол FTP (File Transfer Protocol) является частью набора протоколов TCP/IP. Протокол FTP используется для передачи файлов от одного сетевого устройства к другому. ОС Windows включает FTP-приложение, которое можно запустить из командной строки. Также для загрузки доступно много бесплатных FTP-приложений с графическим интерфейсом пользователя. Такие приложения проще использовать, чем набирать команды в командной строке.

При использовании протокола FTP один компьютер обычно является сервером, а другой – клиентом. При доступе к серверу со стороны клиента необходимо указать имя пользователя и пароль. На некоторых FTP-серверах есть идентификатор пользователя anonymous. Для доступа к таким узлам необходимо просто указать «anonymous» в качестве имени пользователя без пароля. Обычно у администратора узла есть файлы, которые пользователь с идентификатором anonymous может копировать, но не может записывать.

Если в данном классе нет доступного FTP-сервера, можно загрузить и установить свободно распространяемую версию сервера, например, Home FTP Server или Cerberus FTP Server. Также можно воспользоваться FTP-сервером, запускаемым на компьютере с компакт-диска CCNA Discovery Live.

Другой компьютер будут действовать как FTP-клиент, используя команды FTP в командной строке, веб-обозревателе или загрузив бесплатно распространяемую версию FTP-клиента, например, SmartFTP Client или Core FTP LE Client. Над выполнением этой лабораторной работы требуется работать в парах.

Требуются следующие ресурсы:

- компьютер под управлением Windows с FTP-клиентом;
- FTP-сервер (существующий FTP-сервер, загруженное свободно распространяемое программное обеспечение или компакт-диск Live).

Шаг 1. Работа с протоколом FTP из командной строки

а. Нажмите кнопку «Пуск», выберите пункт «Выполнить», введите в командной строке cmd, а затем нажмите кнопку «ОК».

б. В командной строке введите ftp, чтобы запустить FTP-приложение. Командная строка изменится.

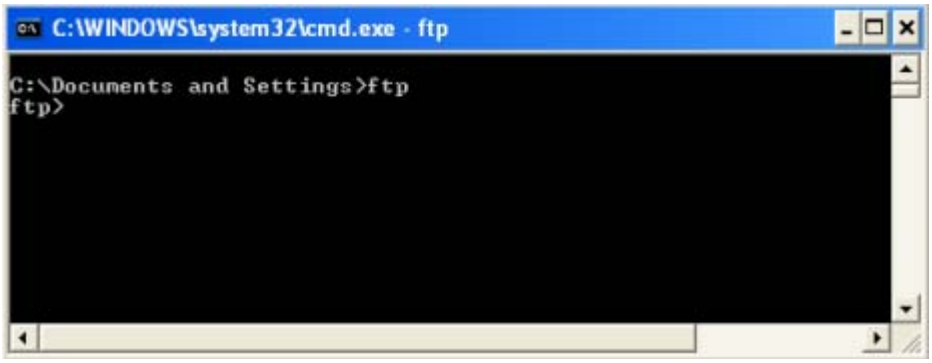


Рис. 6. FTP-клиент, встроенный в ОС Windows.

в. В командной строке ftp введите ?, чтобы просмотреть список всех команд, доступных в данном режиме.

г. Список трех FTP-команд. _____

д. В командной строке введите help put, чтобы просмотреть краткое описание команды put.

е. Какое назначение у команды put? _____

ж. Еще раз воспользуйтесь командой help, чтобы узнать назначение команд get, send и recv.

get _____

send _____

recv _____

ПРИМЕЧАНИЕ. Исходными командами FTP были PUT (для отправки файла FTP-северу) и GET (для загрузки файла с FTP-сервера). Также требуется выбрать режим передачи файлов: ASCII или binary (двоичный). При загрузке двоичного файла в режиме ASCII он окажется поврежденным. Некоторые более новые программы с графическим интерфейсом самостоятельно определяют режим пересылки.

з. Возьмите в партнеры другого учащегося. С помощью процедур, изученных на предыдущих лабораторных занятиях, запишите имя и IP-адрес каждого партнерского компьютера. Очень важно получить правильные имена. Некоторые FTP-приложения позволяют использовать либо IP-адреса, либо имена компьютеров.

Компьютер 1: _____

Компьютер 2: _____

Шаг 2. Использование FTP-клиента с графическим интерфейсом пользователя или веб-обозревателя

а. При использовании веб-обозревателя в качестве FTP-клиента откройте окно веб-обозревателя и введите ftp://ip_адрес_FTP-сервера. Если FTP-сервер настроен на использование идентификатора пользователя «anonymous», подключайтесь прямо к данному FTP-серверу. С помощью FTP-клиента загрузите с сервера любой доступный файл.

б. При использовании FTP-клиента с графическим интерфейсом пользователя откройте данное приложение. Для большинства FTP-клиентов требуется настроить новое соединение, введя его имя, IP-адрес требуемого FTP-сервера, а также имя пользователя и пароль. Можно ввести anonymous, если FTP-сервер поддерживает этот тип соединения. В некоторых приложениях для разрешения анонимного входа используются флажки. После завершения настройки соединения подключитесь к FTP-серверу и загрузите любой файл.

в. Как называется файл, загруженный с данного FTP-сервера? _____

г. Приведите пример, когда протокол FTP может быть полезен специалисту по компьютерам.

_____

_____

_____

Шаг 3. Использование FTP-сервера и FTP-клиента (необязательный)

а. Если для управления доступны FTP-сервер и FTP-клиент, попрактикуйтесь в двухсторонней пересылке файлов между клиентом и сервером.

б. Продемонстрируйте свои переданные файлы другой группе учащихся.

в. Завершите работу FTP-сервера и клиентских приложений.

Лабораторная работа №5 Настройка беспроводного подключения.

Часть 1. Настройка точки беспроводного доступа

Задача
- Настроить точку беспроводного доступа, являющуюся компонентом многофункционального устройства, чтобы разрешить доступ беспроводным клиентам.

Исходные данные / подготовка

Устройство Linksys WRT54G2 совмещает в себе встроенный коммутатор на 4 порта, маршрутизатор и точку беспроводного доступа. В этой лабораторной работе необходимо настроить один из компонентов этого многофункционального устройства, а именно точку беспроводного доступа, чтобы разрешить доступ беспроводным клиентам. Будут настроены основные беспроводные возможности многофункционального устройства, но это не будет безопасная беспроводная сеть. Настройка безопасной беспроводной сети будет выполнена в следующей лабораторной работе.

Требуются следующие ресурсы:
- компьютер с ОС Windows XP, подключенный через кабель к многофункциональному устройству;
- устройство Linksys WRT54G2.

Шаг 1. Проверка соединения между компьютером и многофункциональным устройством
а. Компьютер, используемый для настройки точки доступа, должен быть подключен к одному из портов коммутатора многофункционального устройства.
б. На компьютере щелкните кнопку «Пуск» и выберите «Выполнить». Введите команду cmd и нажмите кнопку «ОК» или клавишу ВВОД.
в. Используя командную строку, отправьте эхо-запрос на многофункциональное устройство, используя IP-адрес по умолчанию (192.168.1.1) или IP-адрес, настроенный для порта многофункционального устройства. Ничего не предпринимайте, пока эхо-запрос не будет успешным.
г. Запишите команду, использованную для отправки эхо-запроса на многофункциональное устройство.

_____

ПРИМЕЧАНИЕ. Если эхо-запрос выполнить не удалось, попробуйте следующие способы устранения неполадок.
- Убедитесь, что IP-адрес компьютера находится в сети 192.168.1.0. Для успешного выполнения эхо-запроса компьютер должен находиться в той же сети, что и многофункциональное
устройство. Служба DHCP многофункционального устройства включена по умолчанию. Если компьютер настроен как клиент DHCP, он должен иметь правильный IP-адрес и маску подсети. Если компьютер использует статический IP-адрес, он должен находиться в сети 192.168.1.0, а его маска подсети должна быть 255.255.255.0.
- Убедитесь, что используется гарантированно работоспособный прямой кабель. Протестируйте его, чтобы убедиться в этом.
- Проверьте, что индикатор связи порта, к которому подключен компьютер, горит.
- Проверьте, подается ли на многофункциональное устройство электропитание.

Если эти шаги не помогли решить проблему, обратитесь к преподавателю.

Шаг 2. Вход в систему многофункционального устройства и настройка беспроводной сети

а. Откройте веб-обозреватель. В строке адреса наберите http://ip_address, где ip_address – IP-адрес беспроводного маршрутизатора (по умолчанию 192.168.1.1). В запросе оставьте поле ввода имени пользователя пустым, но введите пароль, назначенный маршрутизатору. Пароль по умолчанию: admin. Щелкните кнопку «OK».
б. В главном меню щелкните параметр «Wireless» (беспроводная сеть).

Рис. 1. Интерфейс окна настроек многофункционального устройства Linksys.

в. В окне «Basic Wireless Settings» (основные настройки беспроводной сети) в списке «Network Mode» (сетевой режим) по умолчанию выбрано значение «Mixed» (смешанный), поскольку точка доступа поддерживает беспроводные устройства 802.11b, g, и n. Можно использовать любой из этих стандартов для подключения к точке доступа. Если беспроводная часть многофункционального устройства НЕ используется, в качестве сетевого режима можно установить «Disabled» (отключено). Оставьте выбранным значение по умолчанию «Mixed» (смешанный).
г. Удалите SSID по умолчанию (linksys) из поля ввода «Network Name (SSID)» (сетевое Имя (SSID)). Введите новый SSID, используя свою фамилию или имя, указанное преподавателем. SSID задаются с учетом регистра.
д. Запишите точное имя SSID, которое будет использоваться. _____
_____
е. Щелкните по раскрывающемуся меню «Radio Band» (радиодиапазон) и запишите два предлагаемых параметра.
_____
ж. Для беспроводной сети, в которой можно использовать клиентские устройства 802.11b, g или n, значение по умолчанию – «Auto» (автоматически). Значение «Auto» (автоматически)» позволяет выбрать параметр «Wide Channel» (широкий канал) и обеспечивает наилучшие параметры работы. Параметр «Standard Channel» (стандартный канал) используется, если устройства беспроводных клиентов имеют типы 802.11b или/и g. Параметр «Wide Channel» (широкий канал) используется, если используются только клиентские устройства 802.11n. Оставьте выбор значения по умолчанию «Auto» (авто).

з. Для параметра «SSID Broadcast» (широковещательная рассылка SSID) по умолчанию выбрано значение «Enabled» (включить), это позволяет точке доступа регулярно посылать SSID, используя беспроводную антенну. Все беспроводные устройства поблизости могут обнаружить этот сигнал. Таким способом клиенты обнаруживают находящуюся поблизости беспроводную сеть.

и. Щелкните кнопку «Save Settings» (сохранить настройки), находящуюся в самом низу веб-страницы. После успешного сохранения настоек щелкните «Continue» (продолжить).
к. Теперь точка доступа настроена для беспроводной сети с присвоенным ей именем (SSID). Необходимо записать эту информацию до начала следующей лабораторной работы или до подключения любых беспроводных сетевых интерфейсных плат к беспроводной сети.

Вопросы для обсуждения
1. Сколько беспроводных устройств по вашему мнению можно настроить в одном помещении? Что может ограничить это число?

_____
_____
_____

2. Какую потенциальную угрозу безопасности при широковещательной рассылке вашего SSID с точки доступа вы можете назвать?

_____
_____

Часть 2. Настройка беспроводного клиента

Задачи
- Установите и настройте на клиентском компьютере драйвер для беспроводной сетевой интерфейсной платы, подключаемой к USB.
- Определите версию установленного драйвера и проверьте обновления в Интернете.

Исходные данные / подготовка

В этой лабораторной работе необходимо установить на компьютере драйвер для беспроводной сетевой интерфейсной платы, подключаемой к USB. Драйвер – это вид программного обеспечения, который управляет беспроводной сетевой интерфейсной платой. Драйвер можно найти на CD-диске, поставляемом вместе с сетевой интерфейсной платой, или он может быть загружен из Интернета.
Многие производители требуют установить драйвер до подключения адаптера. Процедура, описанная в этой лабораторной работе, предназначена для беспроводной сетевой интерфейсной платы Linksys USB 802.11g, но она будет аналогична и для других плат. Всегда выполняйте процедуру, рекомендованную производителем беспроводной сетевой интерфейсной платы.

Требуются следующие ресурсы:
- компьютер с ОС Windows XP и со свободным USB портом;
- беспроводная сетевая интерфейсная плата и соответствующий драйвер;
- права администратора для установки драйвера;
- устройство Linksys WRT54G2 с беспроводным доступом, настроенное в предыдущей лабораторной работе.

Шаг 1. Установка драйвера беспроводной сетевой интерфейсной платы
а. Вставьте компакт-диск, на котором находится драйвер беспроводной сетевой интерфейсной платы, в дисковод CD/DVD и установите драйвер в соответствии с рекомендациями производителя. Для большинства USB-устройств необходимо установить драйвер до физического подключения самого устройства. Обратите внимание, что можно выполнить часть процесса установки сейчас, а закончить после установки беспроводной сетевой интерфейсной платы.

Рис. 2. Окно программы настройки беспроводного USB-интерфейса.

б. Кто производитель беспроводной сетевой интерфейсной платы? _____

в. Опишите процесс установки драйвера беспроводной сетевой интерфейсной платы.

_____

_____

Шаг 2. Установка беспроводной сетевой интерфейсной платы

а. При запросе подсоедините USB-кабель беспроводной сетевой интерфейсной платы к свободному USB-порту. Для продолжения нажмите кнопку «Next» (далее).

Рис. 3. Подключение беспроводного USB-адаптера.

Шаг 3. Выполнение подключения к беспроводной сети

а. Большинство адаптеров беспроводных сетевых интерфейсных плат имеют клиентское программное обеспечение для управления сетевой интерфейсной платой. Это программное обеспечение отображает все обнаруженные беспроводные сети. Выберите SSID беспроводной сети, настроенной на точке доступа в предыдущей лабораторной работе.

Рис. 4. Обнаружение беспроводных сетей в радиусе действия адаптера.

б. Какой SSID вы используете? _____

в. Если беспроводная сетевая интерфейсная плата не подключилась к беспроводной сети, выполните соответствующие действия по поиску и устранению неполадок.

г. Укажите силу сигнала для беспроводной сетевой интерфейсной платы. _____

д. Обнаружила ли беспроводная сетевая интерфейсная плата другие беспроводные сети? _____ Почему? _____

е. Покажите свое активное сетевое подключение другому учащемуся или лаборанту.

ж. Как по-другому называется беспроводной узел? _____

з. Что лучше: использовать клиентское программное обеспечение от производителя беспроводной сетевой интерфейсной платы или разрешить управлять беспроводной сетевой интерфейсной платой Windows XP?

_____

Шаг 4. Определение версии драйвера сетевой платы

а. Производители оборудования постоянно обновляют драйверы. Драйвер, поставляемый в комплекте с сетевой интерфейсной платой или другим оборудованием, часто является не самым последним.

б. Чтобы узнать версию установленного вами драйвера сетевой интерфейсной платы, щелкните «Пуск», выберите «Панель управления» и далее «Сетевые подключения». Щелкните правой кнопкой мыши по беспроводному соединению и выберите пункт «Свойства». Щелкните кнопку «Настройка» для сетевой интерфейсной платы, а затем вкладку «Драйвер». Как называется установленный драйвер и какая его версия установлена?

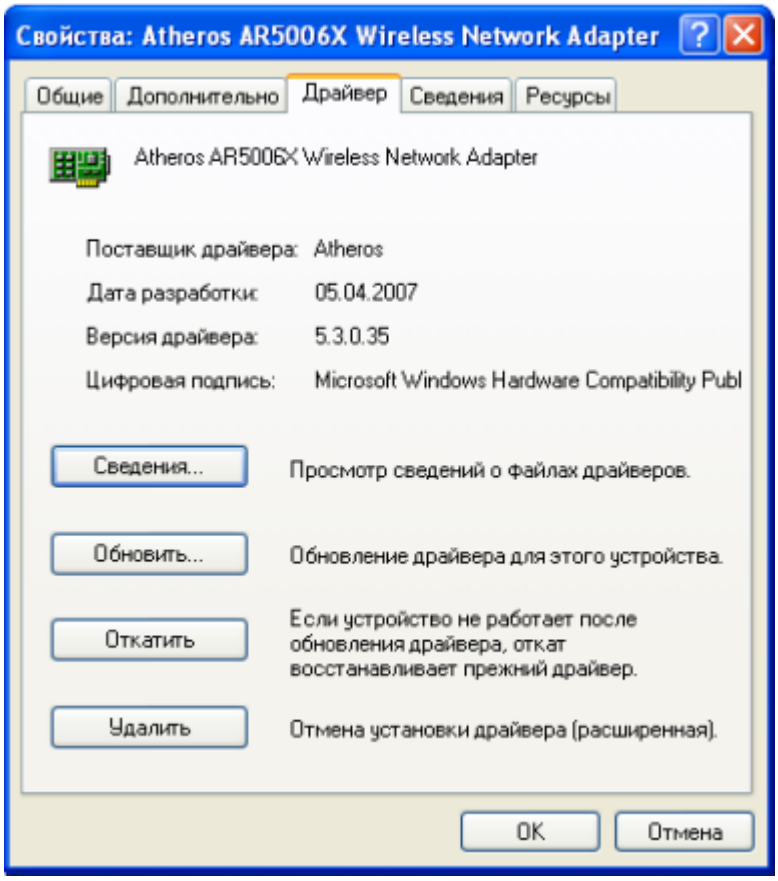


Рис. 5. Определение версии драйвера для установленной беспроводной сетевой карты.

Шаг 5. Определение текущей версии драйвера сетевой интерфейсной платы

а. Выполните поиск драйверов, поддерживающих вашу беспроводную сетевую интерфейсную плату, на веб-узле производителя. Предлагает ли производитель более новые версии драйвера?

_____

б. Какая из перечисленных версий самая новая? _____

в. Если есть более новый драйвер, что с ним следует сделать? _____

_____

Шаг 6. Проверка подключения.

а. После установки сетевой интерфейсной платы необходимо проверить возможность соединения с Linksys WRT300N.

б. Откройте веб-обозреватель (например, Windows Internet Explorer или Mozilla Firefox).

в. В строке адреса введите http://192.168.1.1. Это адрес по умолчанию точки доступа.

г. В диалоговом окне «Подключение к 192.168.1.1» ничего не вводите в поле ввода имени пользователя, а в поле ввода пароля введите admin. Не устанавливайте флажок «Сохранить пароль». Нажмите кнопку «ОК».

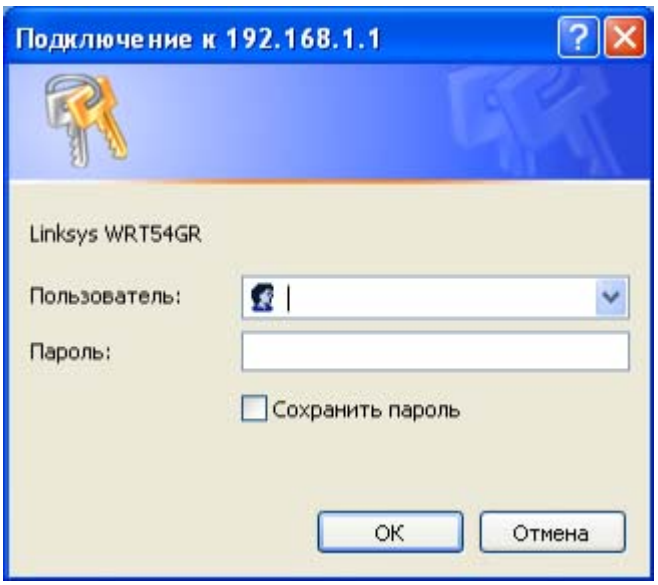


Рис. 6. Подключение к многофункциональному устройству по беспроводной сети.

д. Если вы увидите экран настройки Linksys, то вы успешно соединились с точкой доступа. Если соединение не установлено, следует устранить неполадки в соединении, убедившись что устройства включены и IP-адреса всех устройств верны. Какой IP-адрес должен быть настроен для беспроводной сетевой интерфейсной платы?

Вопросы для обсуждения

1. Будет ли, по вашему мнению, отличаться процесс установки беспроводной сети в продуктовом или книжном магазине от только что выполненного? _____ Почему?

_____

_____

_____

б. Будет ли, по вашему мнению, использованная модель точки доступа достаточна для продуктового магазина в вашем районе? Поясните свой ответ. _____

Часть 3. Настройка безопасности беспроводной сети

Задачи

- Разработать план обеспечения безопасности для домашней сети.
- Настроить точку беспроводного доступа, являющуюся компонентом многофункционального устройства, используя лучшие методы обеспечения безопасности.

Исходные данные / подготовка

Хорошо продуманная реализация системы безопасности крайне важна для безопасной работы беспроводной сети. В этой лабораторной работе демонстрируются действия, которые необходимо предпринять, чтобы гарантировать безопасность сети, используя следующий сценарий:
Вы только что приобрели беспроводной маршрутизатор Linksys WRT54G2 и хотите настроить небольшую сеть у себя дома. Вы выбрали этот маршрутизатор, поскольку согласно спецификации IEEE 802.11n он в 12 раз превосходит 802.11g по скорости и в 4 раза по дальности. Поскольку в стандарте 802.11n используется частота 2,4 ГГц, он обратно совместим как с 802.11b, так и с 802.11g и использует технологию MIMO (много входов, много выходов).

Механизмы безопасности следует включить перед подключением беспроводного устройства к Интернету или проводной сети. Также следует изменить значения по умолчанию, поскольку они широко известны и могут быть получены из Интернета.

Требуются следующие ресурсы:
- компьютер с ОС Windows;
- устройство Linksys WRT54G2;
- прямой кабель Ethernet.

Шаг 1. Разработка плана обеспечения безопасности для домашней сети

а. Укажите как минимум шесть лучших методов, которые следует использовать, чтобы защитить многофункциональное устройство и беспроводную сеть.

1) _____
2) _____
3) _____
4) _____
5) _____
6) _____

б. Укажите, какие существуют угрозы безопасности для каждого из элементов.

1) _____
2) _____
3) _____
4) _____
5) _____
6) _____

Шаг 2. Подключение компьютера к многофункциональному устройству и вход на веб-утилиту

а. Подключите ваш компьютер (сетевую интерфейсную плату Ethernet) к многофункциональному устройству (порт 1 на Linksys WRT54G2), используя прямой кабель.

б. IP-адрес Linksys WRT54G2 по умолчанию: 192.168.1.1, маска подсети по умолчанию: 255.255.255.0. Для возможности обмена данными компьютер и устройство Linksys должны находиться в одной сети. Измените IP-адрес компьютера на 192.168.1.2 и убедитесь, что в качестве маски подсети указано 255.255.255.0. Введите в качестве основного шлюза внутренний адрес устройства Linksys (192.168.1.1). Для этого щелкните «Пуск» > «Панель управления» > «Сетевые подключения». Щелкните правой кнопкой мыши по беспроводному подключению и выберите пункт «Свойства». Выберите протокол Интернета (TCP/IP) и введите адреса, как указано ниже.

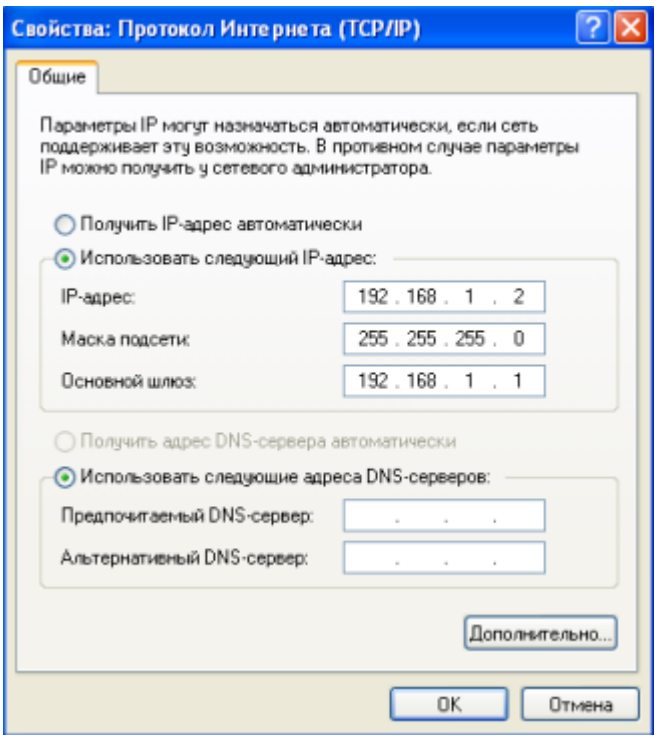


Рис. 7. Настройка сетевого адреса на компьютере клиента сети.

в. Откройте веб-обозреватель (например, Internet Explorer, Netscape или Firefox), введите в поле адреса IP-адрес по умолчанию устройства Linksys (192.168.1.1) и нажмите клавишу ВВОД.

г. Отображается экран с запросом имени пользователя и пароля.

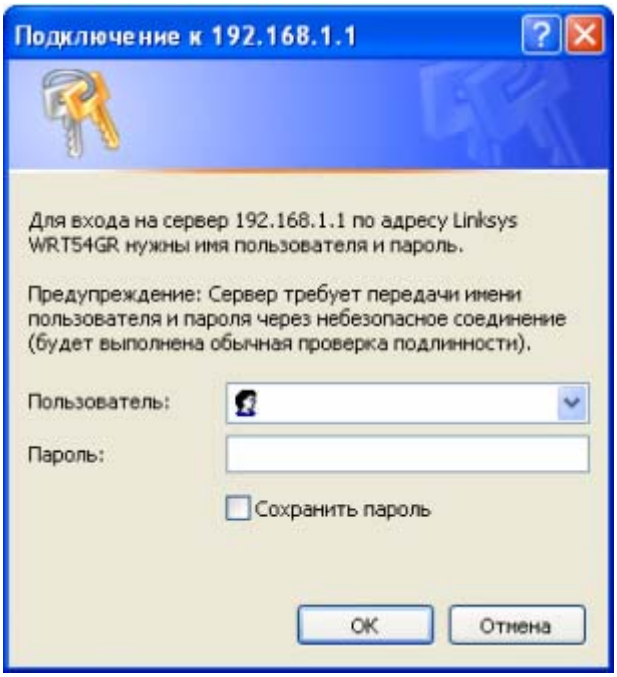


Рис. 8. Проверка пользователя при попытке доступа к устройству.

д. Оставьте поле имени пользователя пустым, а в поле пароля введите admin. Это пароль по умолчанию для устройства Linksys. Щелкните кнопку «ОК». Пароли задаются с учетом регистра.

е. После выполнения всех необходимых изменений в устройстве Linksys нажмите «Save Settings» (сохранить настройки) на каждом экране, чтобы сохранить изменения, или «Cancel Changes» (отменить изменения) для сохранения значений по умолчанию.

Шаг 3. Изменение пароля устройства Linksys

а. Изображенный здесь начальный экран – это экран «Setup» (настройки) > «Basic Setup» (основные настройки).

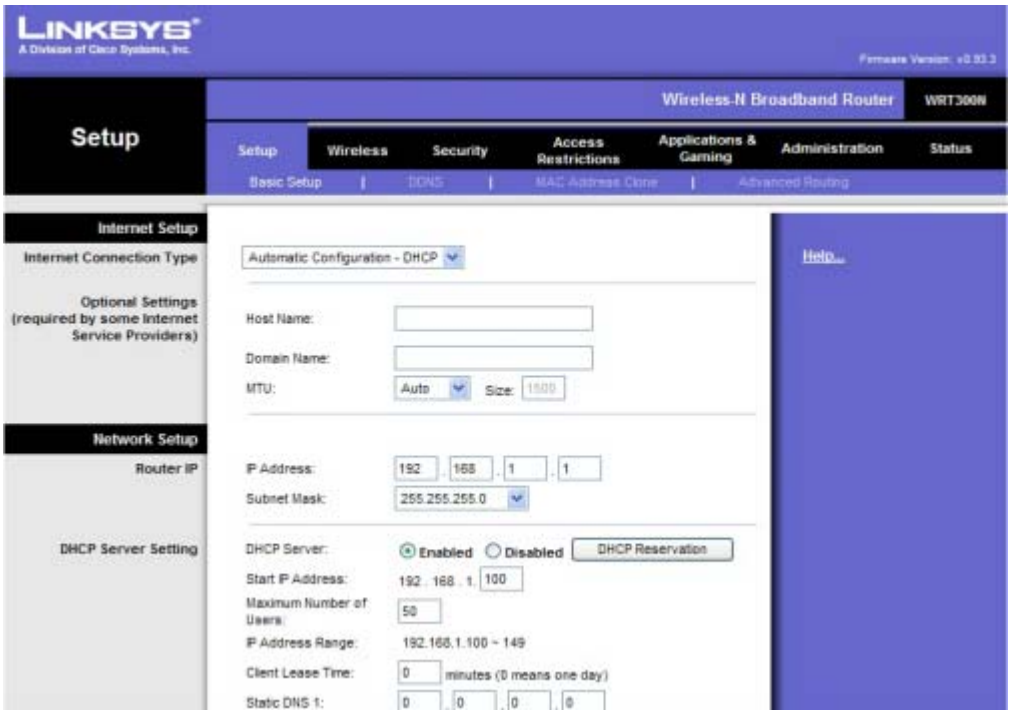


Рис. 9. Изменение пароля доступа к устройству.

б. Щелкните вкладку «Administration» (администрирование). Вкладка «Management» (управление) выбрана по умолчанию.

в. Введите новый пароль для устройства Linksys, а затем подтвердите его. Новый пароль должен состоять не более чем из 32 символов и не должен содержать пробелов. Пароль необходим для доступа к веб-утилите устройства Linksys и к мастеру установки.

г. Возможность доступа к веб-утилите через беспроводную сеть включена по умолчанию. Эту функцию можно отключить для повышения уровня безопасности.

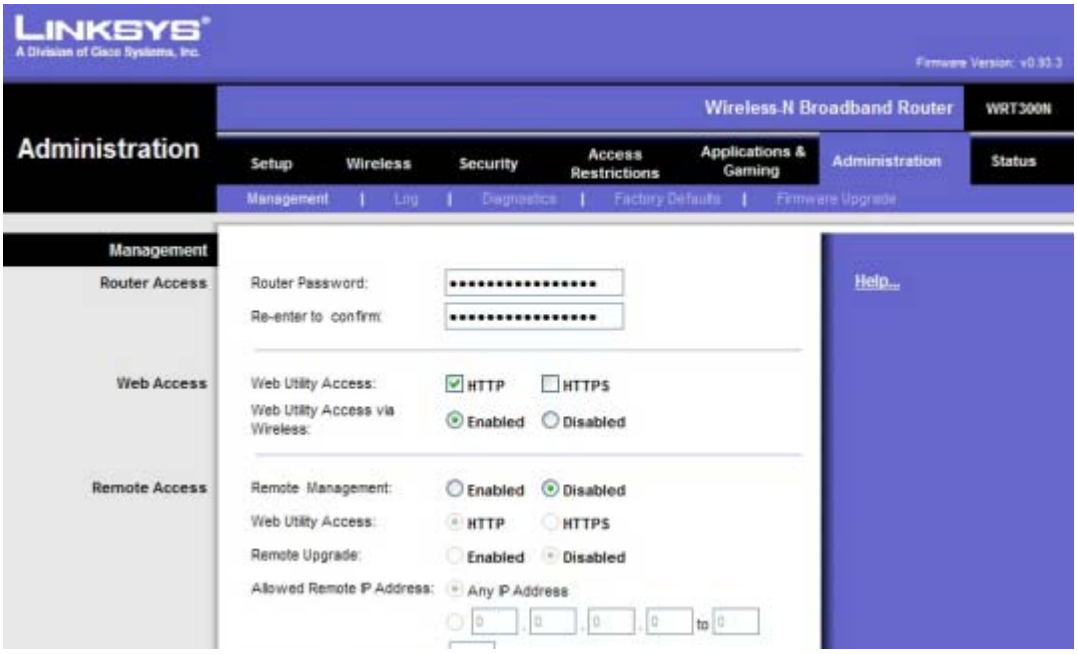


Рис. 10. Настройка ограничений доступа.

д. Щелкните кнопку «Save Settings» (сохранить настройки), чтобы сохранить информацию.
ПРИМЕЧАНИЕ. Если вы забудете свой пароль, можно восстановить заводские настройки устройства Linksys по умолчанию, нажав кнопку RESET и удерживая ее в течение 5 секунд. Пароль по умолчанию: admin.

Шаг 4. Настройка параметров безопасности беспроводной сети
а. Щелкните вкладку «Wireless» (беспроводная). Вкладка «Basic Wireless Settings» (основные настройки беспроводной сети) выбрана по умолчанию. «Network Name» (сетевое имя) – это SSID, общее для всех устройств сети. Оно должен быть одинаковым для всех устройств в беспроводной сети. Оно задается с учетом регистра, и его длина не может превышать 32 символов.

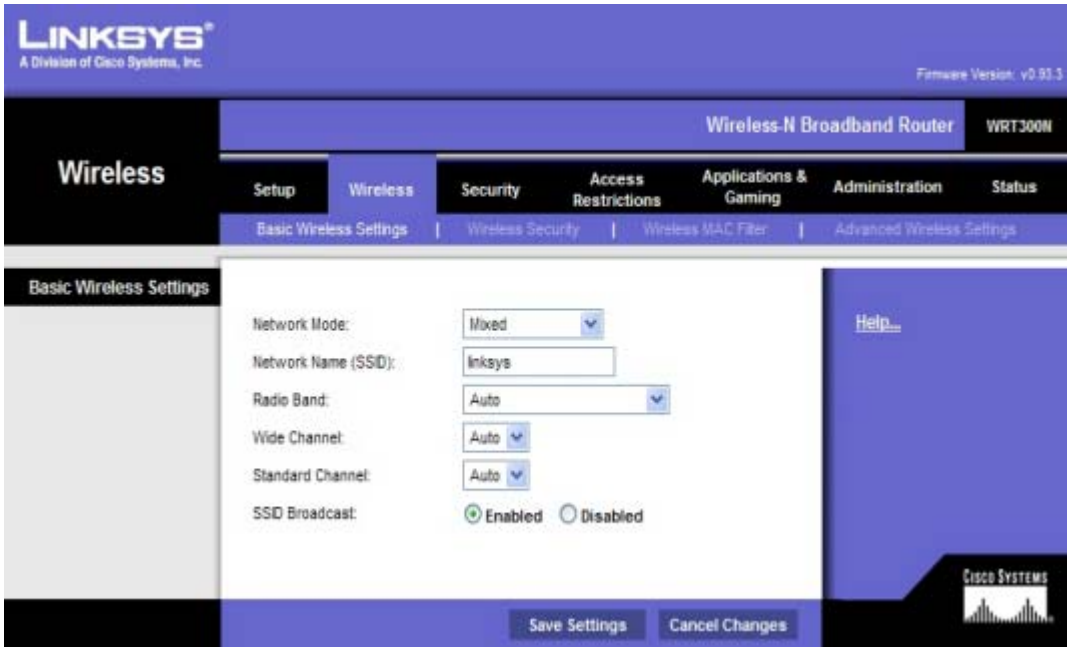


Рис. 11. Настройка параметров защиты беспроводной сети.

б. Измените значение SSID с linksys на уникальное имя. Запишите выбранное имя.

_____

в. Оставьте в качестве значения параметра «Radio Band (Радиодиапазон)» – «Auto» (автоматически). Это позволяет сети использовать все устройства: 802.11n, g и b.
г. Для параметра «SSID Broadcast» (широковещательная рассылка SSID) выберите переключатель «Disabled» (отключить), чтобы отключить широковещательную рассылку SSID. Беспроводные клиенты выполняют поиск сети в зоне своего доступа и обнаруживают широковещательную рассылку SSID устройства Linksys. Для большей безопасности отключите широковещательную рассылку SSID.
д. Сохраните изменения перед переходом на следующий экран.

Шаг 5. Настройка шифрования и аутентификации
а. Выберите вкладку «Wireless Security» (безопасность беспроводной сети) на экране «Wireless» (беспроводная сеть).
б. Этот маршрутизатор поддерживает четыре типа настроек режима безопасности:
- WEP (обеспечение конфиденциальности, сопоставимой с проводными сетями);
- WPA (защищенный доступ к Wi-Fi), использующий предварительно согласованный ключ (PSK);
- WPA Enterprise, использующий службу удаленной аутентификации пользователей с коммутируемым доступом (RADIUS);
- RADIUS.

в. Выберите Security Mode (режим безопасности) WPA Personal.

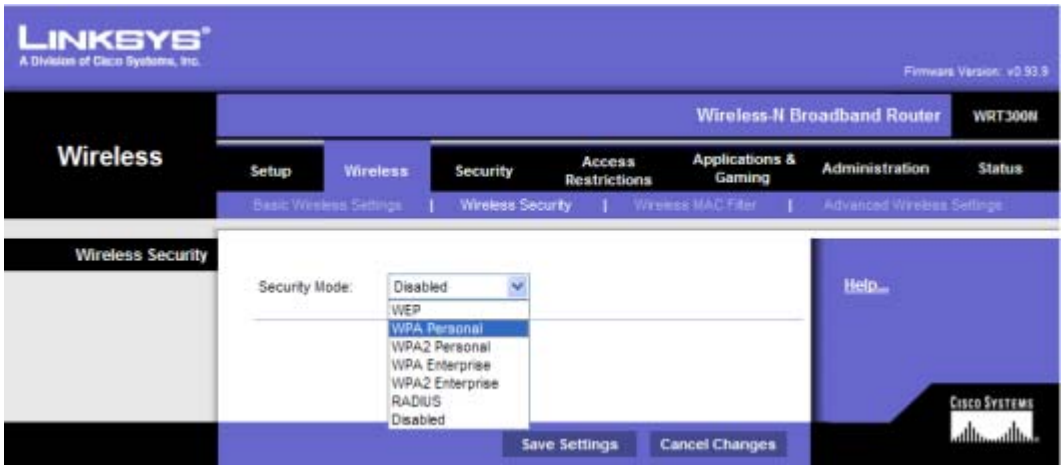


Рис. 12. Выбор криптографического протокола для беспроводной сети.

г. На следующем экране выберите алгоритм шифрования (строка Encryption).
Чтобы защитить сеть, используйте самый высокий уровень шифрования из предложенных для выбранного режима безопасности. Далее перечислены режимы безопасности и уровни шифрования от наименее защищенного (WEP) к наиболее защищенному (WPA2 с AES)

- WEP;
- WPA
- WPA2

o TKIP (Temporal Key Integrity Protocol);
o AES (Advanced Encryption System - расширенный стандарт шифрования); ;

AES поддерживается только новыми устройствами, содержащими специальный криптографический сопроцессор. Чтобы обеспечить совместимость со всеми устройствами, выберите протокол TKIP.

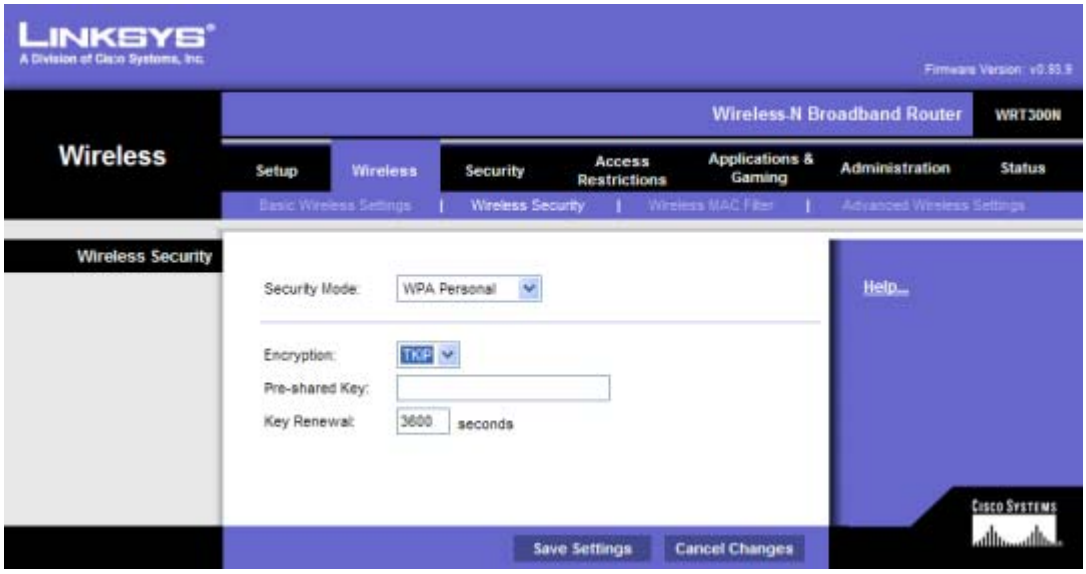


Рис. 13. Выбор алгоритма шифрования.

д. Для аутентификации введите предварительно согласованный ключ длиной от 8 до 63 символов. Этот ключ является общим для устройства Linksys и всех подключенных устройств.
е. Выберите период обновления ключа от 600 до 7 200 секунд. Период обновления – время, через которое устройство Linksys изменяет ключ шифрования.

ж. Сохраните настройки до выхода из этого экрана.

Шаг 6. Настройка фильтрации по MAC-адресам

а. Выберите вкладку «Wireless MAC Filter» (фильтр беспроводных MAC-адресов) на экране «Wireless» (беспроводная).

б. Фильтрация по MAC-адресам позволяет только беспроводным клиентам с указанными MAC-адресами подключаться к сети. Установите переключатель «Permit PCs listed below to access the wireless network» (разрешить указанным ниже ПК получать доступ к беспроводной сети). Щелкните кнопку «Wireless Client List» (список беспроводных клиентов), чтобы отобразить список всех беспроводных клиентских компьютеров в сети.

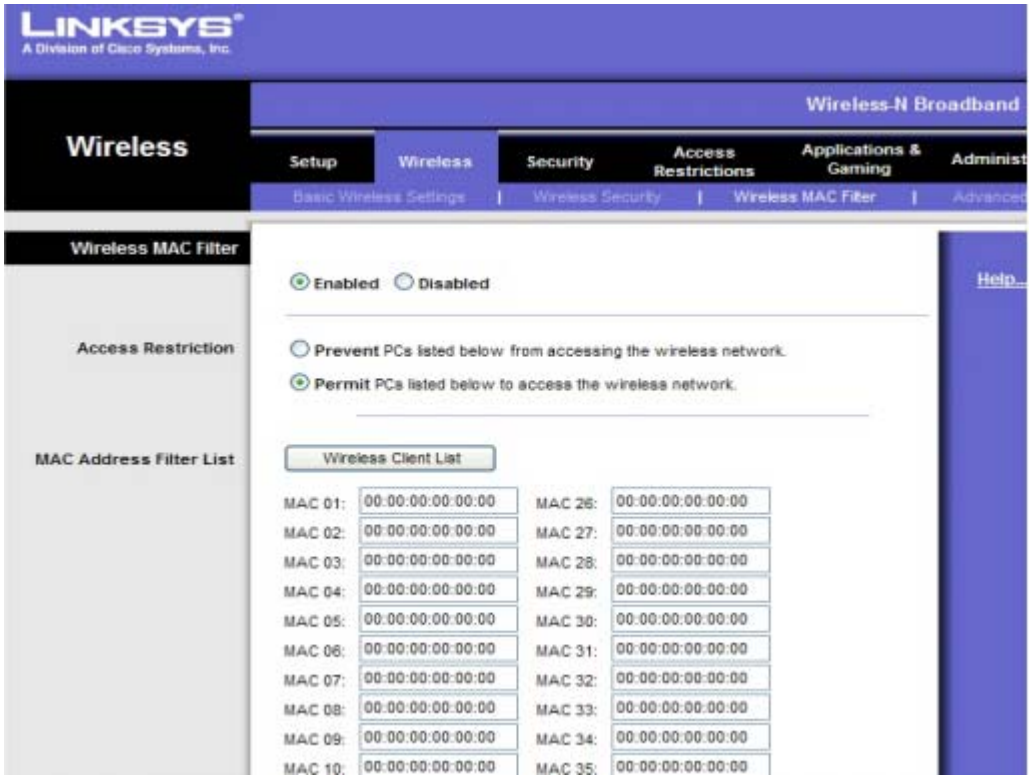


Рис. 14. Настройка фильтрации клиентских подключений по MAC-адресам.

в. На следующем экране можно указать, какие MAC-адреса могут иметь доступ к беспроводной сети. Установите флажок «Save to MAC Address Filter List» (сохранить в списке фильтра по MAC-адресам) для всех клиентских устройств, которые следует добавить, а затем щелкните кнопку «Add» (добавить). Все беспроводные клиенты, не указанные в списке, не смогут подключиться к беспроводной сети. Сохраните настройки до выхода из этого экрана.

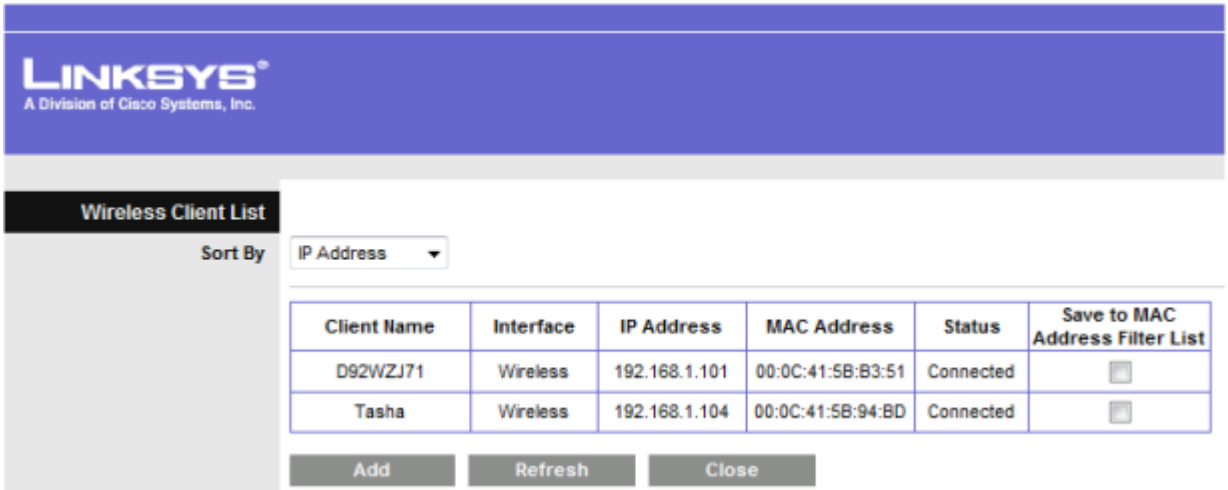


Рис. 15. Отображение подключенных клиентов.

Вопросы для обсуждения

1. Какая функция, настроенная на Linksys WRT54G2, по вашему мнению, наиболее важна для обеспечения безопасности и почему?

_____
_____
_____

2. Напишите, что еще можно сделать, чтобы повысить безопасность сети.

_____
_____

Лабораторная работа №6 Настройка средств обеспечения безопасности

Часть 1. Настройка политик доступа и DMZ на многофункциональном устройстве

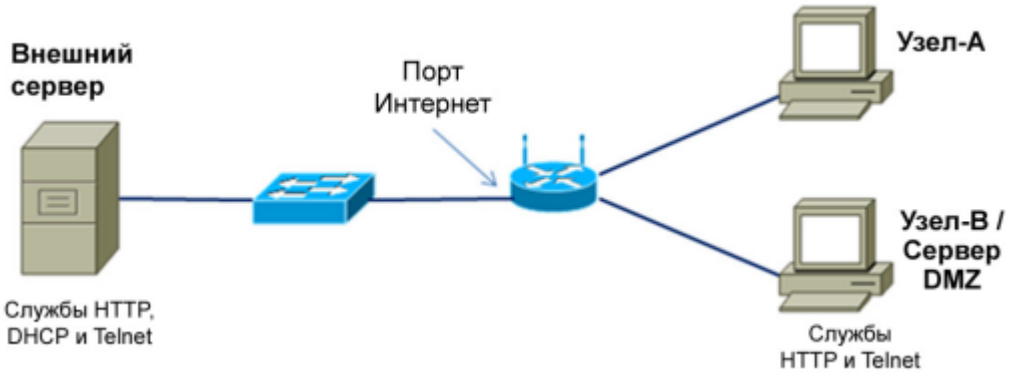


Рис. 1. Топология сети в которой установлено многофункциональное устройство.

Задачи

- Войти в систему многофункционального устройства и просмотреть настройки безопасности.
- Настроить политики доступа в Интернет на основе IP-адреса и приложения.
- Настроить DMZ для сервера открытого доступа со статическим IP-адресом.
- Настроить переадресацию портов, чтобы разрешить доступ только к портам HTTP.
- Использовать возможности справки Linksys WRT54G2.

Исходные данные / подготовка

В этой лабораторной работе содержатся инструкции по настройке параметров безопасности на Linksys WRT54G2. Linksys содержит программный межсетевой экран для защиты внутренних (принадлежащих к локальной сети) клиентов от атак с внешних узлов. Подключения внутренних узлов к внешним адресатам могут фильтроваться в зависимости от IP-адреса, веб-узла назначения и приложения.

Устройство Linksys также можно настроить на создание демилитаризованной зоны (DMZ) для контроля доступа к серверу с внешних узлов. Эта лабораторная работа выполняется в группах по двое, при этом две группы могут работать вместе для взаимного тестирования настроек ограничения доступа и функциональности DMZ. Работа делится на 2 части:

- Часть 1. Настройка политик доступа.
- Часть 2. Настройка DMZ.

Для выполнения работы требуются следующие ресурсы:

- Linksys WRT54G2 или другое многофункциональное устройство с настройками по умолчанию;
- идентификатор пользователя и пароль для устройства Linksys, если они отличаются от значений по умолчанию;
- компьютер с Windows XP Professional для доступа к графическому интерфейсу пользователя Linksys;
- внутренний ПК в качестве сервера в DMZ со службами HTTP и Telnet (заранее настроенный или сервер Discovery Live CD);
- внешний сервер, используемый в качестве «Интернета» и поставщика услуг Интернета, на котором заранее настроены службы DHCP, HTTP и Telnet (это может быть реальный сервер или сервер Discovery Live CD);

- кабели для соединения ПК, Linksys WRT54G2 или другого многофункционального устройства и коммутаторов.

Часть 1. Настройка политик доступа

Шаг 1. Создание сети и настройка узлов

а. Присоедините узлы к портам коммутатора многофункционального устройства, как показано на схеме топологии рис. 1. Узел-А – это консоль, используемая для доступа к графическому интерфейсу пользователя Linksys. Узел-В сначала выполняет роль тестовой машины, а затем используется как сервер DMZ.
б. Настройте IP-конфигурацию для обоих узлов, используя сетевые подключения Windows XP и свойства TCP/IP. Убедитесь, что узел-А настроен как клиент DHCP. Присвойте узлу-В статический IP-адрес в диапазоне 192.168.1.x с маской подсети 255.255.255.0. В качестве основного шлюза следует задать внутренний локальный сетевой адрес устройства Linksys.

ПРИМЕЧАНИЕ. Если узел-В уже является клиентом DHCP, можно сохранить его текущий адрес и сделать его статическим, используя возможность сохранения DHCP на экране основных настроек Linksys.
в. Используйте команду ipconfig для отображения IP-адреса, маски подсети и основного шлюза для узла-А и узла-В и запишите их в таблицу. Узнайте у преподавателя IP-адрес и маску подсети внешнего сервера и запишите их в таблицу.

Табл. 1

Узел	IP-адрес	Маска подсети	Основной шлюз
Узел А			
Узел В/Сервер DMZ			
Внешний сервер			

Шаг 2. Вход в интерфейс пользователя

а. Для доступа к веб-интерфейсу пользователя устройства Linksys откройте обозреватель и введите IP-адрес устройства по умолчанию 192.168.1.1.
б. Войдите в систему, используя идентификатор пользователя и пароль по умолчанию admin. На рис. 2 показано окно аутентификации.

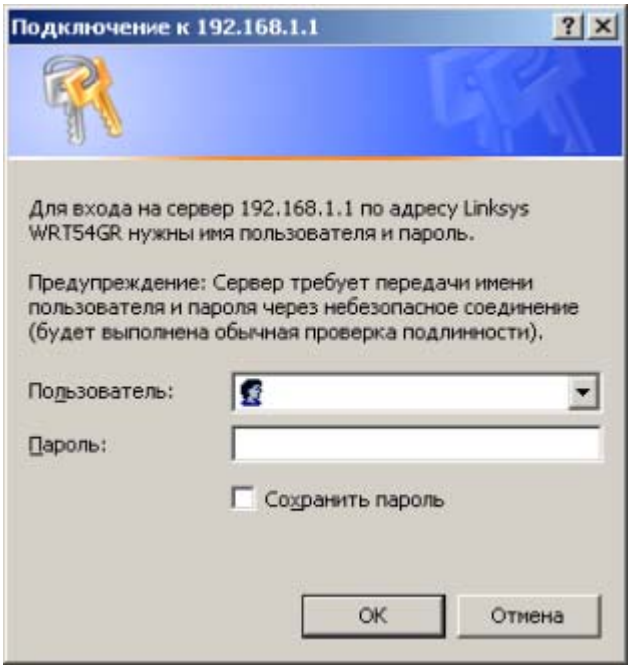


Рис. 2. Окно аутентификации на многофункциональном устройстве.

в. Многофункциональное устройство должно быть настроено для получения IP-адреса с внешнего сервера DHCP. При входе на устройство Экран по умолчанию после входа в систему многофункционального устройства:
«Setup» (настройки) > «Basic Setup» (основные настройки), как показано на рис. 3.

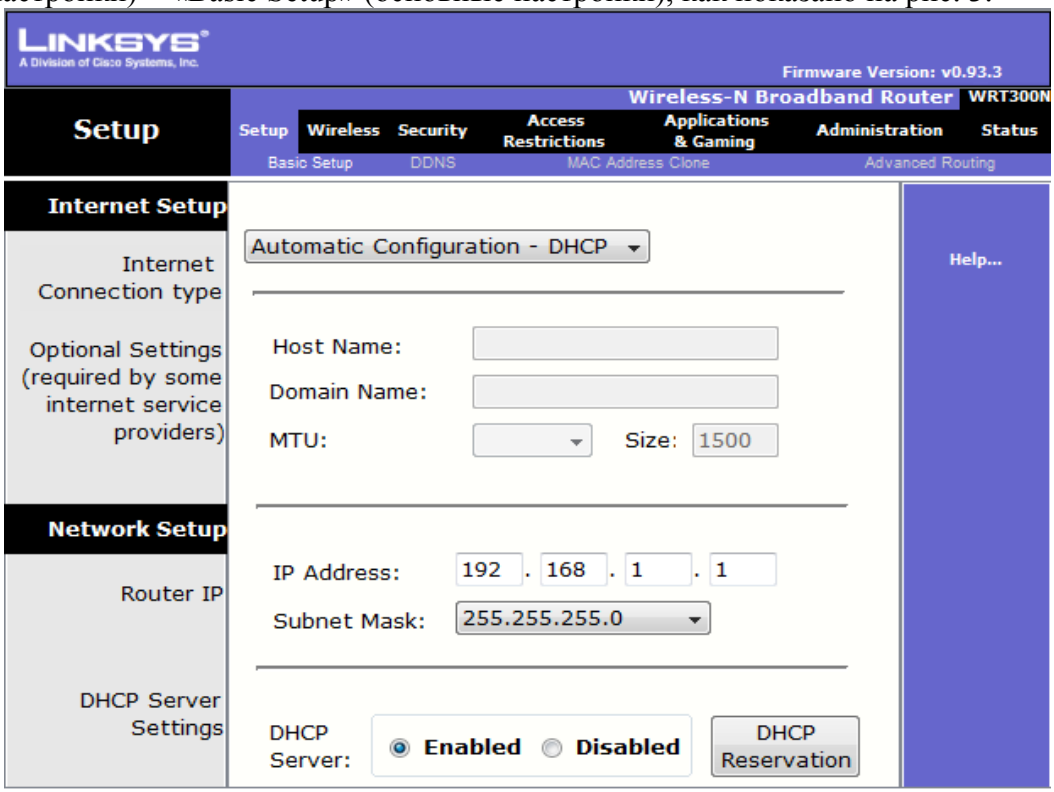


Рис. 3. Окно базовых настроек многофункционального устройства

Ответьте на следующие вопросы:
Какой используется тип подключения к Интернету?

_____

г. Какой IP-адрес и маска подсети маршрутизатора по умолчанию (внутреннего) используется для многофункционального устройства?

_____

д. Убедитесь, что многофункциональное устройство получило внешний IP-адрес с сервера DHCP. Для этого щелкните «Status» (статус) > вкладка «Router» (маршрутизатор).
е. Какой внешний IP-адрес и маска подсети присвоены многофункциональному устройству?

_____

Шаг 3. Просмотр настроек межсетевого экрана многофункционального устройства

а. Linksys WRT54G2 содержит простой межсетевой экран (рис. 4), который использует преобразование сетевых адресов (NAT). Кроме того, он имеет дополнительные возможности межсетевого экрана с использованием функции динамического анализа пакетов (SPI) для обнаружения и блокирования запросов, поступающих из Интернета.
б. На главном экране щелкните вкладку «Security» (безопасность) для просмотра состояния параметров «Firewall» (межсетевой экран) и «Internet Filter» (интернет-фильтр). Укажите статус защиты межсетевого экрана SPI. _____
в. Какие флажки установлены для «Internet Filter» (интернет-фильтр)?

_____

г. Щелкните «Help» (справка), чтобы больше узнать об этих настройках. Какие преимущества дает фильтрация IDENT?

_____

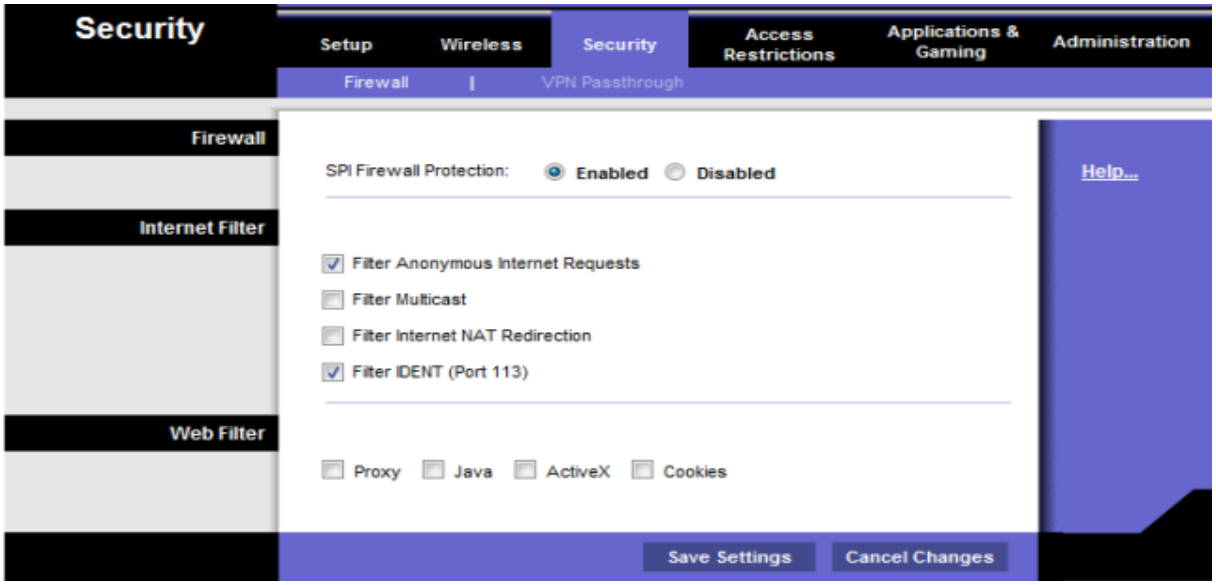


Рис. 4. Настройки межсетевого экрана многофункционального устройства.

Шаг 4. Настройка ограничений доступа в Интернет на основе IP-адреса

В лабораторной работе №5 было продемонстрировано, что для указания того, какие клиентские компьютеры могут получать доступ к многофункциональному устройству в зависимости от их MAC-адреса, можно использовать возможности беспроводной безопасности. Это предотвращает подключение не авторизованных компьютеров к точке беспроводного доступа и получение ими доступа к внутренней локальной сети и Интернету.

Многофункциональное устройство также позволяет указать, какие внутренние пользователи могут выйти в Интернет из локальной сети. Можно создать политику доступа в Интернет, разрешающую или запрещающую определенным внутренним компьютерам доступ в Интернет в зависимости от их IP-адреса, MAC-адреса и других критериев.

а. На главном экране многофункционального устройства щелкните вкладку «Access Restrictions» (ограничения доступа) и задайте параметр «Access Policy 1» (политика доступа 1).
б. Введите в качестве названия политики «Block-IP» (блокировка IP). Выберите «Enabled» (включено), чтобы включить политику, а затем выберите «Deny» (запретить), чтобы предотвратить доступ в Интернет с указанного IP-адреса (рис. 5).

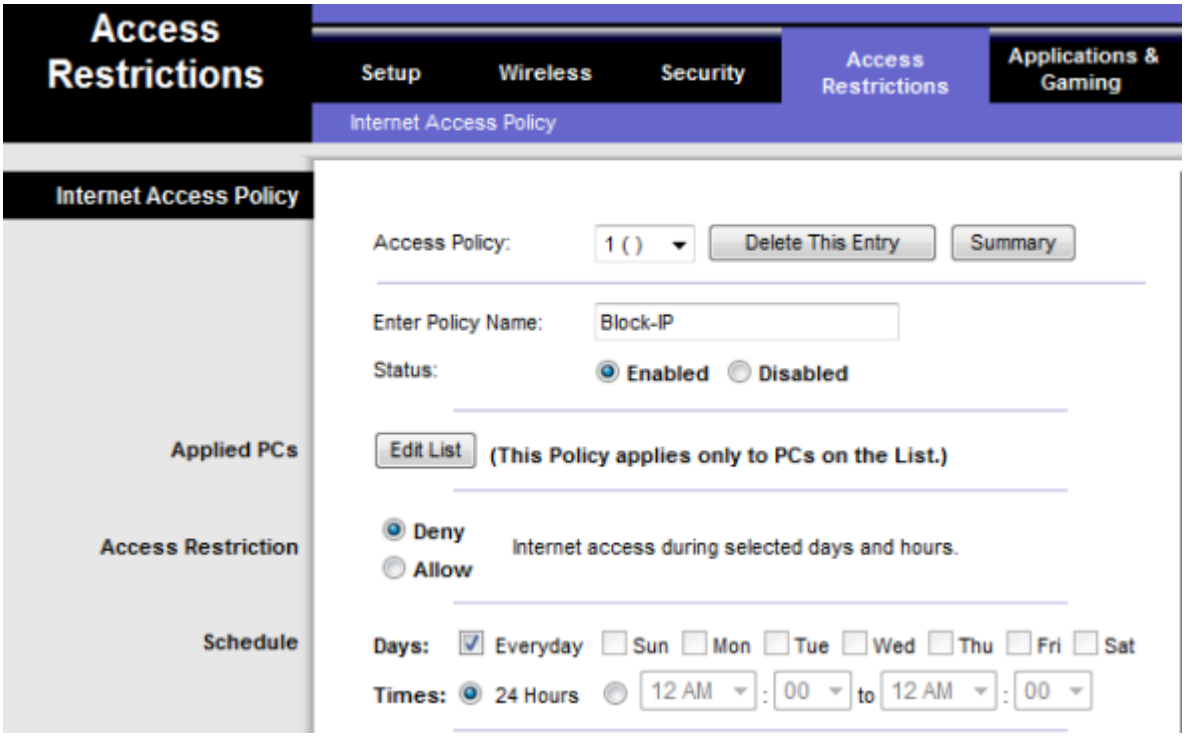


Рис. 5. Настройка политики ограничения доступа в Интернет.

в. Щелкните кнопку «Edit List» (редактировать список) и введите IP-адрес узла-B. Щелкните «Save Settings» (сохранить настройки), а затем «Close» (закрыть)». Щелкните «Save Settings» (сохранить настройки)» для сохранения политики доступа в Интернет 1 – «Блокировка IP».
г. Протестируйте политику, попробовав подключиться к внешнему веб-серверу с узла-B. Откройте обозреватель и введите IP-адрес внешнего сервера в поле адреса. Можете ли вы подключиться к серверу? _____
д. Измените статус политики «Block-IP» (блокировка IP) на «Disabled» (выключено) и щелкните «Save Settings» (сохранить настройки). Можете ли вы теперь подключиться к серверу?_____
__
е. Какие еще можно использовать политики доступа для блокировки доступа в Интернет?
_____

Шаг 5. Настройка политики доступа в Интернет на основе приложений

Можно создать политику доступа в Интернет, не позволяющую некоторым компьютерам использовать определенные приложения или протоколы Интернета.
а. На главном экране графического интерфейса пользователя Linksys щелкните вкладку «Access Restrictions» (ограничение доступа) и определите политику доступа в Интернет.
б. Введите в качестве названия политики «Block-Telnet» (блокировка Telnet). Выберите «Enabled» (включено) для включения политики, а затем щелкните «Allow to permit Internet access from a specified IP address as long as it is not one of the applications that is blocked» (разрешить доступ в Интернет с заданного IP-адреса, если это не одно из заблокированных приложений).

в. Щелкните кнопку «Edit List» (редактировать список) и введите IP-адрес узла-B. Щелкните «Save Settings» (сохранить настройки), а затем «Close» (закрыть). Какие другие интернет-приложения и протоколы можно заблокировать?

_____

г. Выберите приложение Telnet из списка приложений, которые можно заблокировать, а затем щелкните двойную стрелку вправо, чтобы добавить его к списку «Blocked List» (список заблокированных), как показано на рисунке 6. Щелкните «Save Settings» (сохранить настройки).

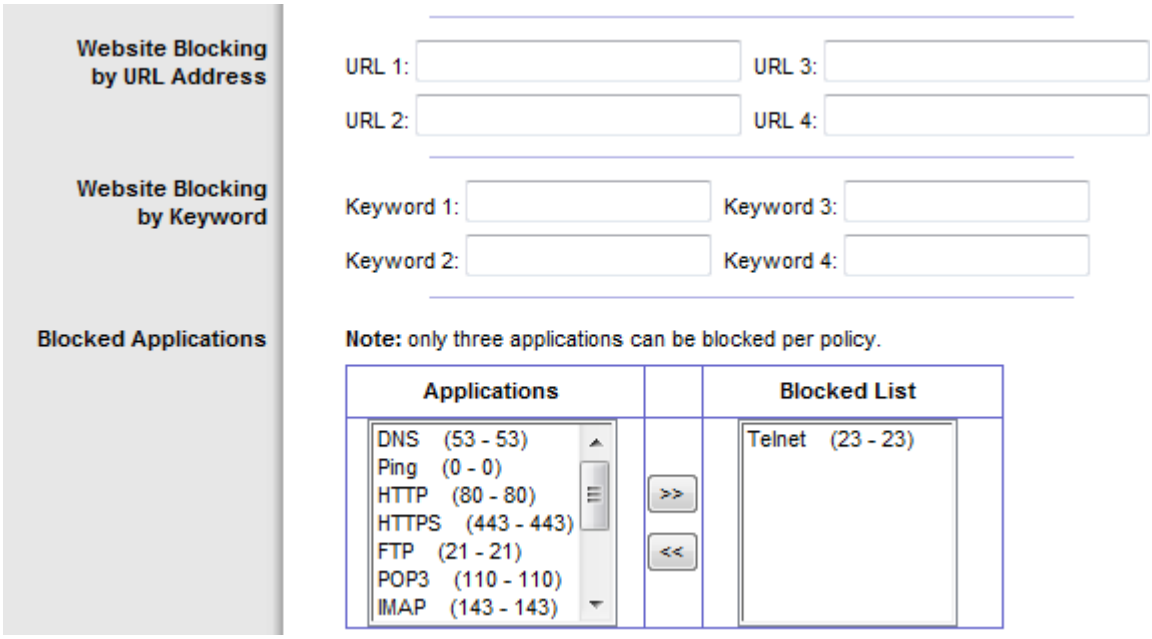


Рис. 6. Ограничение доступа для заданного приложения.

д. Протестируйте политику: откройте командную строку, используя «Пуск» > «Все программы» > «Стандартные» > «Командная строка».
е. Отправьте эхо-запрос на IP-адрес внешнего сервера с узла-B, используя команду ping. Можете ли вы получить эхо-запрос с сервера? _____
ж. Подключитесь по протоколу Telnet на IP-адрес внешнего сервера с узла-B, используя команду telnet A.B.C.D (где A.B.C.D – IP-адрес сервера).
Можете ли вы получить доступ к серверу? _____

Часть 2. Настройка DMZ на многофункциональном устройстве

Шаг 1. Настройка простой зоны DMZ

Иногда требуется разрешить доступ к компьютеру из Интернета, но защитить остальные компьютеры внутренней локальной сети. Для этого можно создать демилитаризованную зону (DMZ), которая позволяет получать доступ к любым портам и службам на указанном сервере. Любые запросы к службам по внешнему адресу многофункционального устройства будут перенаправлены указанному серверу.
а. Узел-B будет выполнять функцию сервера DMZ, и на нем необходимо запустить службы HTTP и Telnet. Убедитесь, что узел-B имеет статический IP-адрес, или, если узел-B является клиентом DHCP, можно зарезервировать его текущий адрес и сделать его статическим, используя функцию «DHCP Reservation» (резервирование DHCP) устройства Linksys на экране «Basic Setup» (основные настройки).
б. На главном экране графического интерфейса пользователя Linksys щелкните вкладку «Applications & Gaming» (приложения и игры), а затем щелкните «DMZ», рис. 7.
в. Щелкните ссылку «Help» (справка) для получения дополнительных сведений о DMZ. Для каких других целей может понадобиться настройка узла в DMZ?

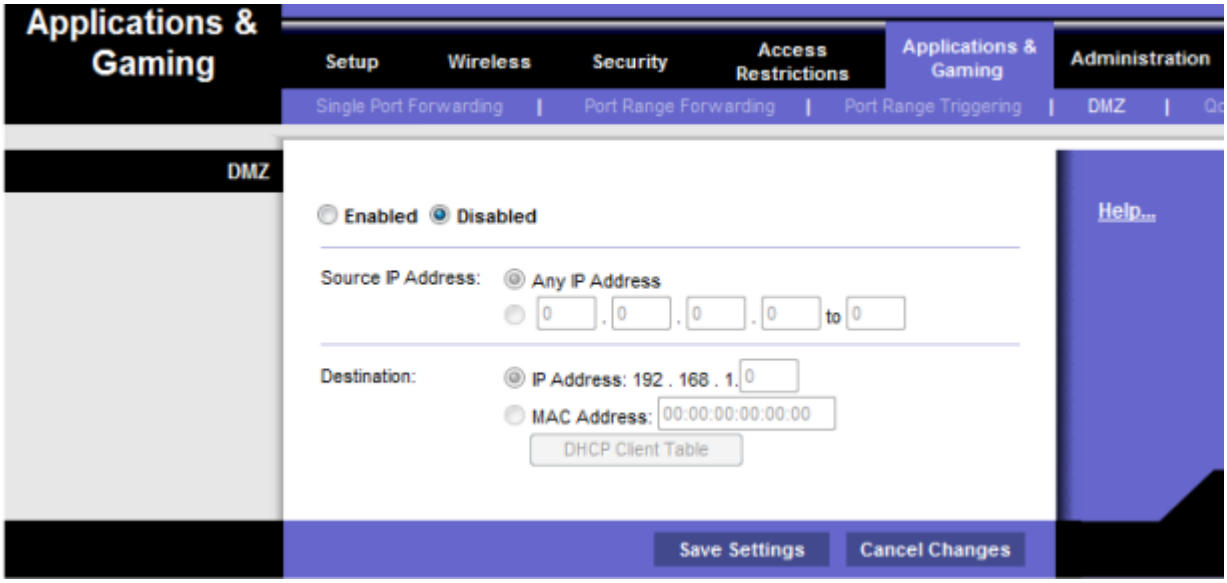


Рис. 7. Окно настроек DMZ.

г. Функция DMZ отключена по умолчанию. Выберите «Enabled» (включено), чтобы включить DMZ. Переключатель «Any IP Address» (любой IP-адрес) в поле «Source IP Address» (IP-адрес источника) должен быть выбран, а в поле в поле «Destination IP Address» (IP-адрес назначения)» введите IP-адрес узла-B. Щелкните «Save Settings» (сохранить настройки) и «Continue» (продолжить) при получении запроса.

д. Проверьте базовый доступ к серверу DMZ, отправив эхо-запрос с внешнего сервера на внешний адрес многофункционального устройства. Используйте команду ping –a, чтобы убедиться, что на запросы в действительности отвечает сервер DMZ, а не многофункциональное устройство. Можно ли получить эхо-запрос с DMZ-сервера?

_____

е. Протестируйте HTTP-доступ к серверу DMZ: откройте обозреватель на внешнем сервере и введите внешний IP-адрес многофункционального устройства. Попробуйте сделать то же самое из обозревателя на узле-A, используя внутренние адреса. Можно ли получить доступ к веб-странице? _____

ж. Протестируйте подключение по протоколу Telnet: откройте командную строку (см. шаг 5). Подключитесь по протоколу Telnet к внешнему IP-адресу многофункционального устройства, используя команду telnet A.B.C.D (где A.B.C.D – внешний IP-адрес многофункционального устройства). Можете ли вы получить доступ к серверу?_____

Шаг 2. Настройка узла с переадресацией одного порта

Базовые функции хостинга DMZ, настроенные на шаге 6, позволяют открыть доступ ко всем портам и службам на сервере, например, HTTP, FTP и Telnet. Если узел используется для конкретной цели (например, для служб FTP или для веб-служб), доступ должен быть ограничен указанной службой. Это можно сделать за счет переадресации одного порта. Эта функция более безопасна, чем основные функции DMZ, поскольку она открывает доступ только к необходимым портам. Перед выполнением этого шага отключите настройки DMZ для шага 1. узел-B – это сервер, на который переадресуются порты, но доступ к нему ограничен веб-протоколом (HTTP).

а. На главном экране щелкните вкладку «Applications & Gaming» (приложения и игры), а затем щелкните «Single Port Forwarding» (переадресация одного порта), чтобы указать приложения и номера портов.

б. Щелкните первое раскрывающееся меню под заголовком «Application Name» (имя приложения) и выберите HTTP. Это порт 80 протокола веб-сервера.
в. В первое поле «To IP Address» (на IP-адрес) введите IP-адрес узла-B и установите флажок «Enabled» (включено). Щелкните кнопку «Save Settings» (сохранить настройки).

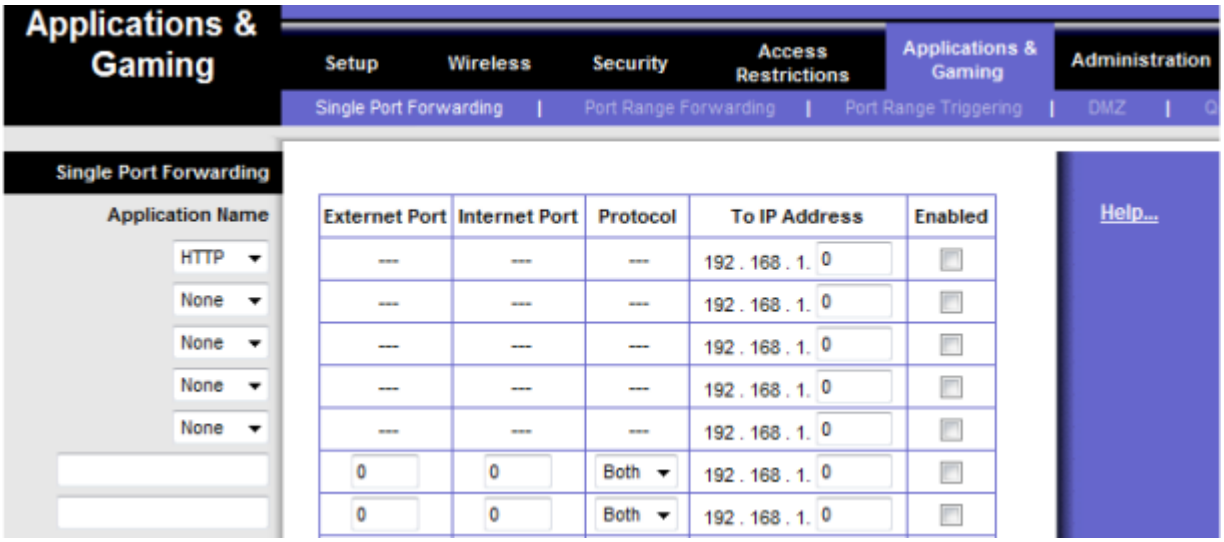


Рис. 8. Настройка перенаправления портов.

г. Протестируйте HTTP-доступ к узлу DMZ: откройте обозреватель на внешнем сервере и введите внешний IP-адрес многофункционального устройства. Попробуйте сделать то же самое из обозревателя на узле-A на узел-B. Можно ли получить доступ к веб-странице?_____
д. Протестируйте подключение по протоколу Telnet: откройте командную строку (см. шаг 5). Подключитесь по протоколу telnet к внешнему IP-адресу многофункционального устройства, используя команду A.B.C.D (где A.B.C.D – внешний IP-адрес многофункционального устройства). Можете ли вы получить доступ к серверу?_____

Шаг 3. Восстановление настроек по умолчанию многофункционального устройства

а. Чтобы восстановить заводские настройки по умолчанию устройства Linksys, щелкните вкладку «Administration» (администрирование) > «Factory Defaults» (заводские настройки по умолчанию).
б. Щелкните кнопку «Restore Factory Defaults» (восстановить заводские настройки по умолчанию), рис. 9. Все записи и изменения настроек будут потеряны.

ПРИМЕЧАНИЕ. Текущие настройки можно сохранять и загружать, используя вкладку «Administration» (администрирование) > «Management» (управление) и кнопки «Backup Configuration» (резервное копирование конфигурации) и «Restore Configuration» (восстановить конфигурацию).

Рис. 9. Восстановление заводских настроек.

Часть 2. Выполнение анализа уязвимости системы с помощью программы MBSA

ВНИМАНИЕ! При выполнении этой лабораторной работы могут оказаться нарушенными юридические и организационные политики безопасности. Анализатор системы безопасности, загружаемый в процессе выполнения этой лабораторной работы, необходимо использовать только в целях обучения в рамках этой лабораторной работы. До использования анализатора системы безопасности в реальной сети проконсультируйтесь с преподавателем и администрацией сети относительно внутренних правил по использованию таких инструментальных средств.

Рис. 10. Топология сети при выполнении анализа уязвимостей.

Задачи

- Загрузить и установить программный анализатор системы безопасности.
- Выполнить тестирование узла для определения потенциальных мест, уязвимых для атаки.

Исходные данные / подготовка

Анализаторы системы безопасности – ценные средства, используемые сетевыми администраторами и инспекторами для выявления уязвимых мест сети и узла. Для тестирования безопасности узла и сети разработано много инструментальных средств анализа уязвимости, также известные как сканеры безопасности. В этой лабораторной работе предлагается загрузить и установить анализатор основных элементов защиты Microsoft Baseline Security Analyzer (MBSA). Инструментальное средство MBSA специально разработано для выявления потенциальных проблем нарушения безопасности, связанных с операционными системами, обновлениями и приложениями корпорации Microsoft. Оно также выявляет ненужные службы, которые, возможно, запущены на компьютере, а также все открытые порты.

Средство MBSA запускается в системах Windows Server или Windows XP и используется для поиска распространенных ошибок при настройке системы безопасности или отсутствующих обновлений безопасности для операционной системы, а также для большинства версий Internet Information Server (IIS), SQL Server, Internet Explorer (IE) и продуктов MS Office. MBSA предлагает конкретные способы устранения потенциальных проблем.

Эту лабораторную работу можно выполнять индивидуально или в группах по двое.

Для выполнения работы требуются следующие ресурсы:

- компьютер, на котором запущена операционная система Windows XP Professional, выполняющий функцию тестируемой станции;
- высокоскоростное подключение к Интернету для загрузки средства MBSA (если оно предварительно не установлено);
- компьютер должен быть подсоединен к интегрированному коммутатору-маршрутизатору или автономному концентратору или коммутатору;
- дополнительно можно пользоваться сервером, на котором одновременно запущены DHCP, HTTP, FTP и Telnet (предварительно настроенные).

Шаг 1. Загрузка и установка MBSA

а. Откройте обозреватель и перейдите на веб-страницу MBSA по адресу:
http://technet.microsoft.com/en-us/security/cc184924.aspx
б. Какая последняя версия MBSA доступна? _____
в. Перечислите некоторые функции, предлагаемые средством MBSA. _____
_____
г. Прокрутите страницу вниз и выберите язык, чтобы начать процесс загрузки.
д. Щелкните «Continue» (продолжить) для проверки установленной на компьютере копии Microsoft Windows.
е. Щелкните кнопку «Download Files below» (загрузить следующие файлы) и выберите файл для загрузки. (Файл установки на английском языке: MBSASetup-EN.msi). Щелкните кнопку «Download» (загрузить) справа от этого файла. Укажите размер загружаемого файла в мегабайтах. _____
ж. При отображении диалогового окна «Загрузка файла – Предупреждении системы безопасности» щелкните «Сохранить» и загрузите файл в указанную папку или на рабочий стол. Можно также запустить его с веб-узла загрузки программ.
з. По завершении загрузки убедитесь, что все остальные приложения закрыты. Дважды щелкните загруженный файл. Для запуска программы установки щелкните «Выполнить», и еще раз щелкните «Выполнить» при появлении предупреждения системы безопасности. На экране установки MBSA щелкните «Next» (далее).
и. Выберите соответствующий переключатель для принятия условий лицензионного соглашения и щелкните «Next» (далее). По мере выполнения процесса установки принимайте все параметры по умолчанию, а затем щелкните «Finish» (готово). На последнем экране программы установки MBSA щелкните кнопку «OK» и закройте папку, чтобы вернуться к рабочему столу Windows.

Шаг 2. Создание сети и настройка узлов

а. Подсоедините узел (узлы) к интегрированному маршрутизатору, концентратору или коммутатору, как показано на схеме топологии. Узел Host-A – это тестируемая станция, где установлено средство MBSA. Сервер можно не использовать.
б. Задайте IP-конфигурацию узла (узлов), используя окно "Сетевые подключения" Windows XP и свойства TCP/IP. Если узел подсоединен к интегрированному маршрутизатору, настройте его как DHCP-клиент. В противном случае перейдите к шагу 2в.

в. Если узел подсоединен к концентратору или коммутатору, а DHCP-сервер не доступен, настройте его вручную, присвоив ему статический IP-адрес.
Какие IP-адрес и маску подсети имеет узел Host-A и сервер (не обязательно)?
_____

Шаг 3. Запуск на узле программы MBSA

а. Дважды щелкните значок MBSA на рабочем столе или запустите ее из меню «Пуск» > «Все программы». Какие параметры доступны при отображении главного экрана? _____
_____

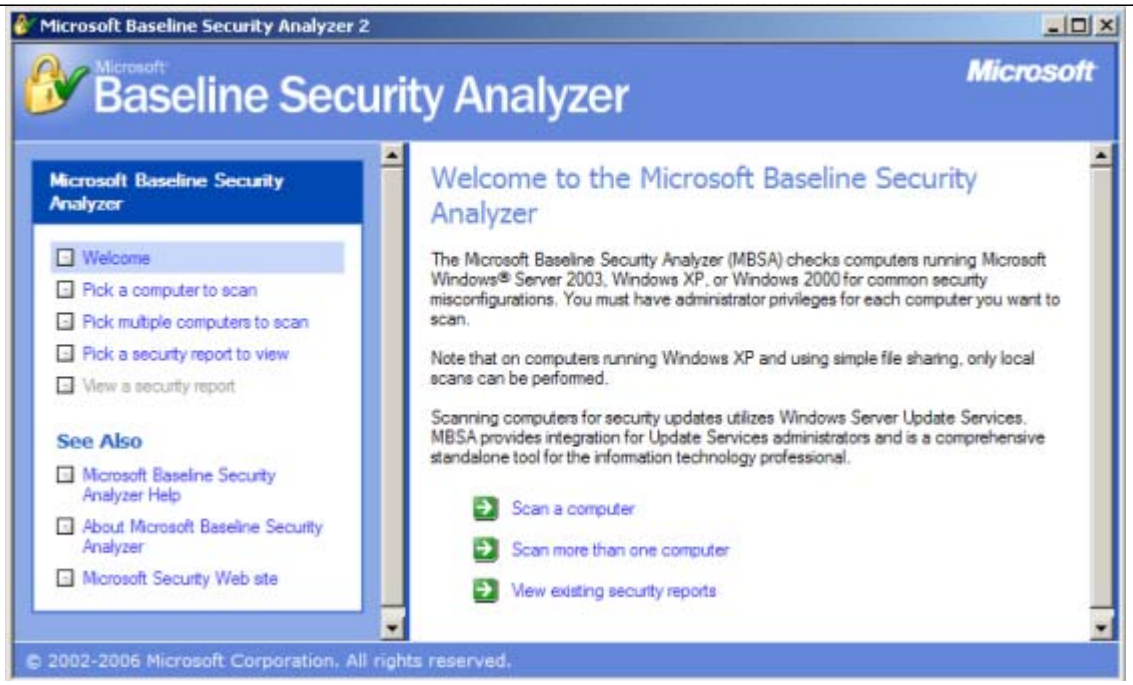


Рис. 11. Главное окно MBSA.

Шаг 4. Выбор компьютера для выполнения сканирования

а. В левой части экрана щелкните «Pick a computer to scan» (выберите компьютер для сканирования). По умолчанию отображается компьютер, на который установлена программа MBSA.
б. Какие два способа задания компьютера для сканирования существуют? _____
_____
в. Укажите для выполнения сканирования компьютер по умолчанию. Снимите флажки «Check for IIS administrative vulnerabilities» (поиск уязвимых мест IIS) и «Check for SQL administrative vulnerabilities» (поиск уязвимых мест SQL), поскольку маловероятно, что эти услуги установлены на сканируемом компьютере. Щелкните «Start Scan» (начать сканирование).

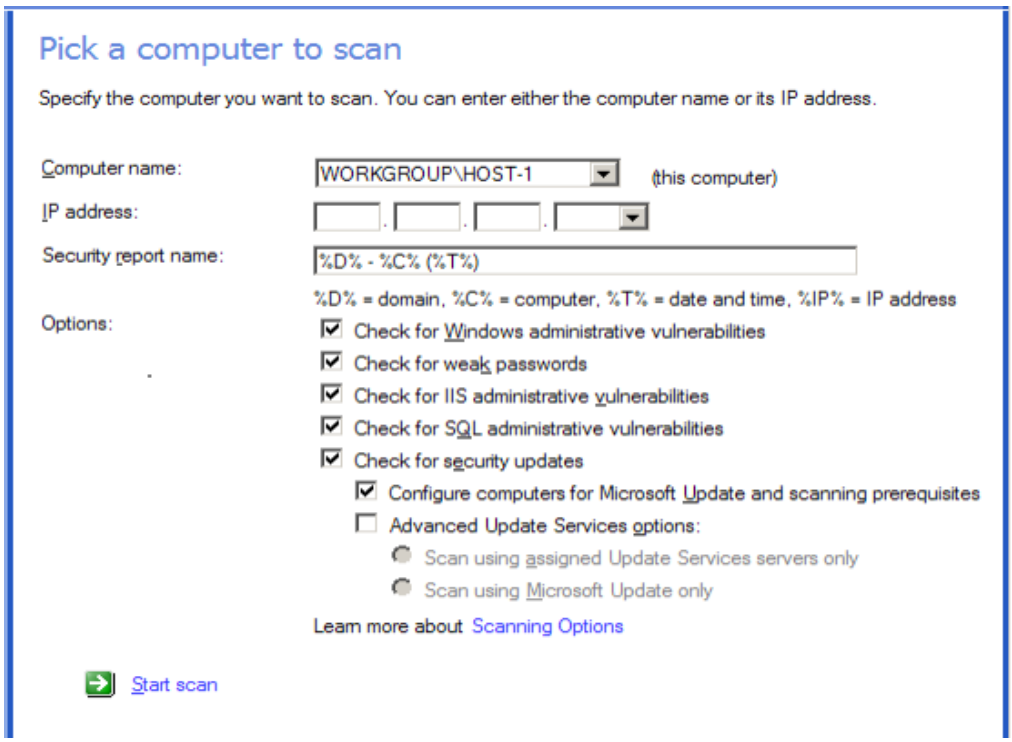


Рис. 12. Окно настройки параметров сканирования.

Шаг 5. Просмотр результатов поиска обновлений безопасности

а. Изучите отчет безопасности. Какие результаты получены в результате поиска обновлений безопасности? _____

_____

б. При наличии красных или желтых символов "X" щелкните «How to correct this» (как устранить эту проблему). Какое решение предлагается? _____

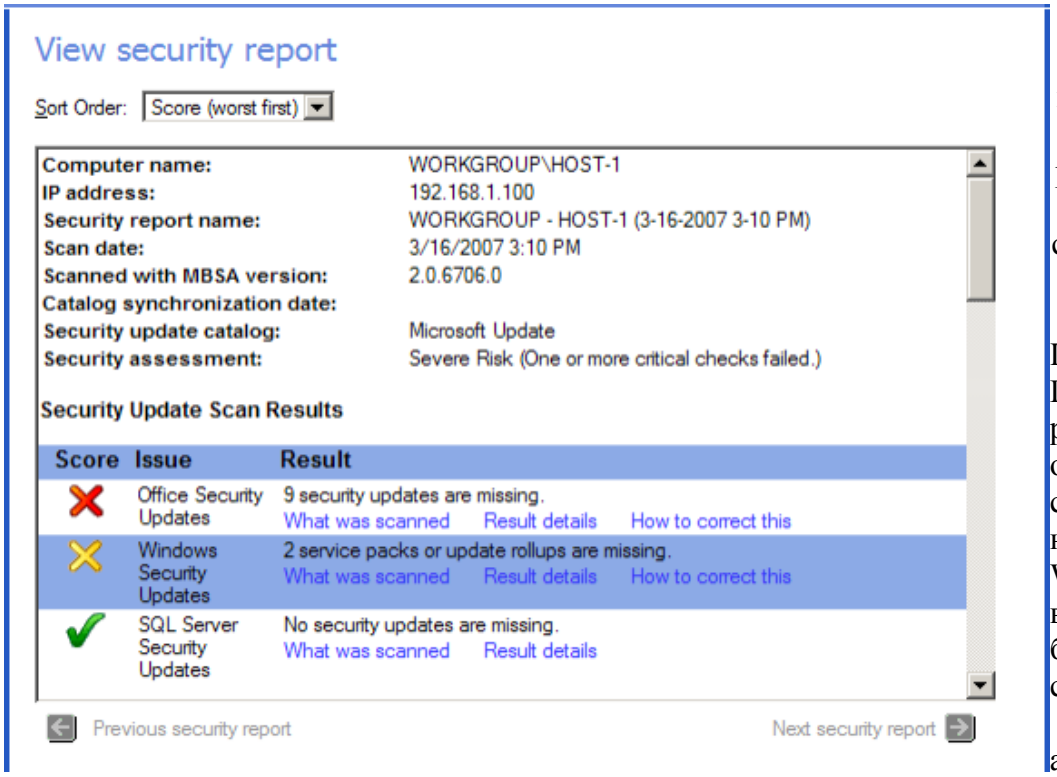


Рис. 13. Отчет, получаемый в результате сканирования.

Шаг 6. Просмотр результатов сканирования Windows в отчете безопасности

а.

Прокрутите отчет вниз и найдете второй раздел, содержащий результаты сканирования Windows («Windows Scan Results»). Были ли найдены какие-либо уязвимые места системы административной безопасности? _____

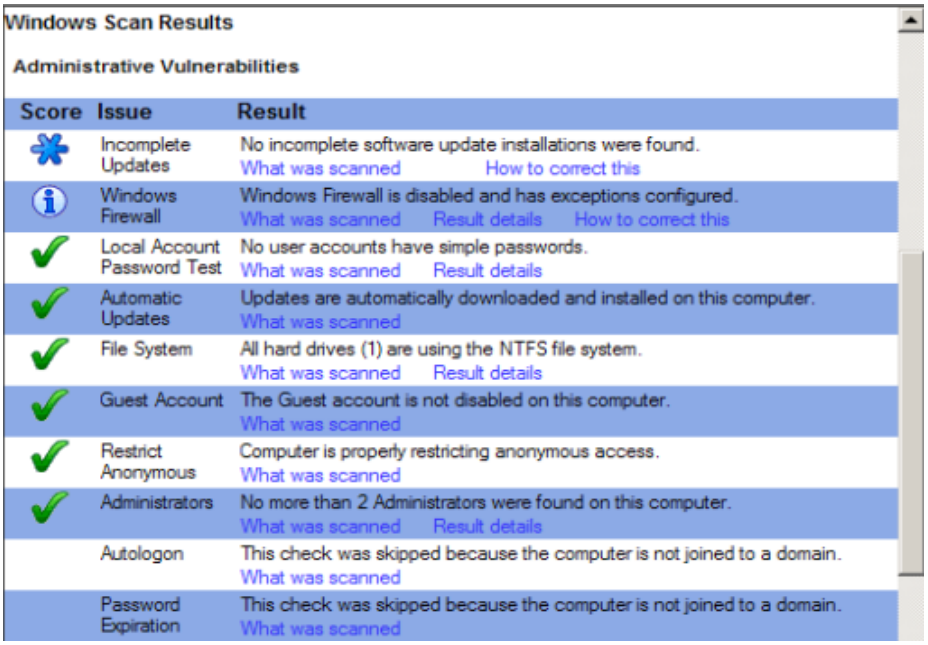


Рис. 14. Результат сканирования операционной системы.

б. В разделе «Additional System Information» (дополнительные сведения о системе) на экране (см. рис. 15) в столбце «Issue» (проблема) в строке «Services» (службы) щелкните «What was scanned» (что сканировалось) и «Result details» (подробные сведения) в столбце «Result» (результаты), чтобы прочесть описание выполненной проверки. Что вы обнаружили? По завершении закройте оба всплывающих окна и вернитесь к отчету безопасности.

_____

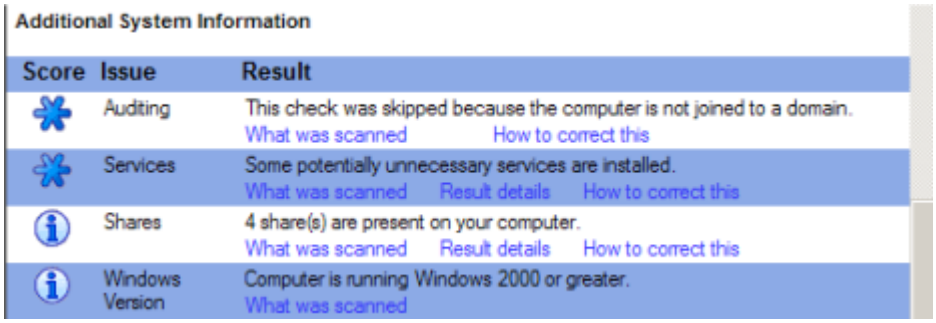


Рис. 15. Окно дополнительной информации.

Шаг 7. Просмотр результатов сканирования приложений для настольного компьютера в отчете безопасности

а. Прокрутите отчет вниз и найдите последний раздел, содержащий результаты сканирования приложений для настольного компьютера («Desktop Applications Scan Results», рис. 16). Были ли найдены какие-либо уязвимые места системы административной безопасности?

_____

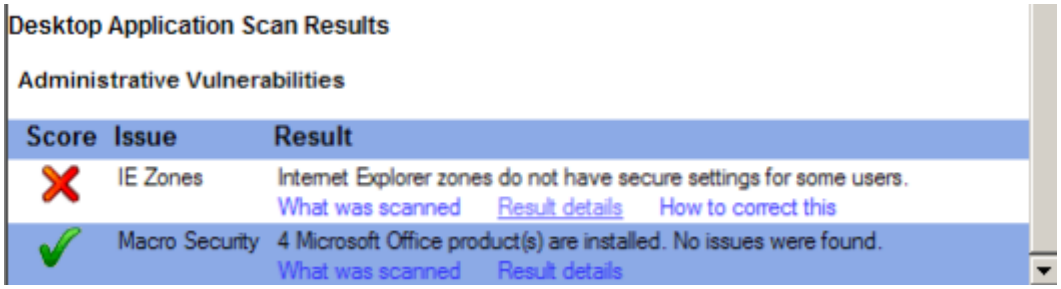


Рис. 16. Результат сканирования прикладных программ.

б. Сколько на компьютере установлено продуктов Microsoft Office? _____

в. Были ли для какого-либо из них выявлены проблемы безопасности (см. «Macro Security» [защита от макросов])?

_____

Шаг 8. Выполнение сканирования сервера, если он используется

а. Если в конфигурации доступен сервер с различными службами, на главном экране MBSA щелкните «Pick a computer to scan» (выберите компьютер для сканирования) и введите IP-адрес сервера, а затем щелкните «Start Scan» (начать сканирование). Какие уязвимые места в системе безопасности были выявлены?

_____

_____

_____

б. Установлены ли на нем потенциально бесполезные службы? Укажите номер порта, на котором они работают.

_____

_____

Шаг 9. Удаление MBSA с компьютера с использованием функции «Установка и удаление программ» на «Панели управления»

а. Этот шаг необязателен, и его выполнение зависит от того, выполняется ли в дальнейшем автоматическое восстановление узла в процессе работы сети.

б. Чтобы удалить MBSA с компьютера, щелкните «Пуск» > «Панель управления» > «Установка и удаление программ». Найдите приложение MBSA и удалите его. В списке оно отображается как Microsoft Baseline Security Analyzer 2.0.1 (или номер другой загруженной версии). Щелкните «Удалить», а затем щелкните «Да» для подтверждения удаления приложения MBSA. По завершении закройте все окна и вернитесь к рабочему столу.

Вопросы для обсуждения

а. Инструментальное средство MBSA предназначено для поиска уязвимых мест на компьютерах, на которых установлена ОС Windows. Найдите в Интернете другие аналогичные инструментальные средства. Перечислите некоторые из найденных инструментов.

_____

б. Какие инструментальные средства могут использоваться для компьютеров, на которых установлена операционная система, отличная от Windows? Найдите в Интернете другие инструментальные средства и перечислите некоторые из них.

_____

в. Какие другие шаги можно предпринять для повышения защищенности компьютера от атак из Интернета? _____

Литература

1. В. Г. Олифер, Н. А. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебное пособие для вузов /- 3-е изд. - СПб. : Питер, 2007. - 957 с. : ил. (27 экз. в библиотеке ТУСУР)
2. С. Г. Михальченко, Е. Ю. Агеев. Эксплуатация и развитие компьютерных систем и сетей: учебное пособие: В 2 разделах. Томск: ТУСУР, 2007. (27 экз. в библиотеке ТУСУР)
3. Официальный учебный курс CCNA Discovery корпорации Cisco [Электронный ресурс] – режим доступа: http://www.cisco.com/web/learning/netacad/index.html — зарегистрированные пользователи. (количество экз. соответствует числу обучающихся)
4. Э. С. Таненбаум. Компьютерные сети. /- 4-е изд. - СПб. : Питер, 2011. - 992 с. : ил.
5. TCP/IP Tutorial and Technical Overview. Из серии IBM Red Books. Язык англ. [Электронный ресурс] – режим доступа: http://www.redbooks.ibm.com/abstracts/gg243376.html - свободный. Книга доступна для бесплатного скачивания в формате pdf., 8-е изд., 2006, 1004 с. : ил.
6. М.В. Кульгин. Компьютерные сети. Практика построения. Для профессионалов. /- 2-е изд. - СПб. : Питер, 2003. - 462 с. : ил.
7. А.Ю. Филимонов. Построение мультисервисных сетей Ethernet. / СПб. : БХВ – Петербург, 2007. - 592 с. : ил.