**ЛАБОРАТОРНАЯ РАБОТА**

**СЕТЕВЫЕ СЕРВИСЫ**

**Цель работы: приобретение навыков безопасного использования сетевых сервисов**

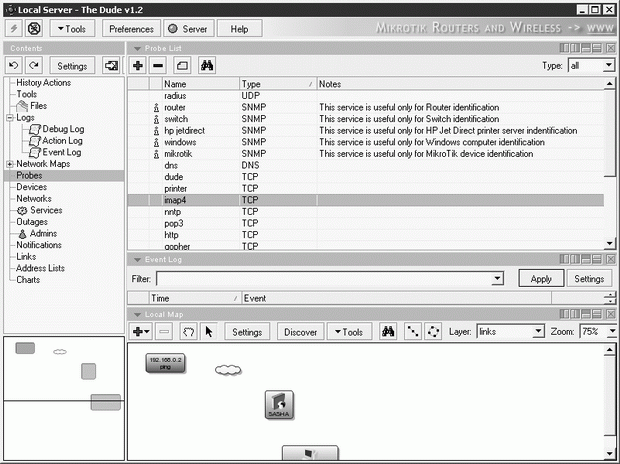
Рассмотрим несколько полезных программ, которые позволят вам использовать вашу локальную *сеть* с большей эффективностью.

Обращаем ваше внимание на то, что все описанные здесь программы представлены лишь в учебных целях. Мы считаем нужным предупредить о том, что используя описанное программное обеспечение для получения несанкционированного доступа к компьютерам других пользователей они совершают противоправные действия.

**TheDude**

Если в вашей локальной сети достаточно много компьютеров, вполне возможно, что вам захочется улучшить управление сетью с помощью специального программного обеспечения. В частности, существуют программы, которые умеют отслеживать состояние компьютеров сети и сообщать о нем администратору. Например, программа TheDude, которую мы сейчас рассмотрим, служит для мониторинга локальной сети. Основная ее особенность – автоматическое составление карты сети и отслеживание состояния устройств, входящих в сеть. Программу можно скачать на URL [http://www.mikrotik.com](http://www.mikrotik.com/) , дистрибутив занимает около 1,4 Мб.

Окно TheDude состоит из нескольких рабочих областей ( [рис. 3.4](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=2#image.3.4)).

[](http://www.intuit.ru/EDI/14_08_14_2/1407964674-31059/tutorial/532/objects/3/files/03_04.gif)

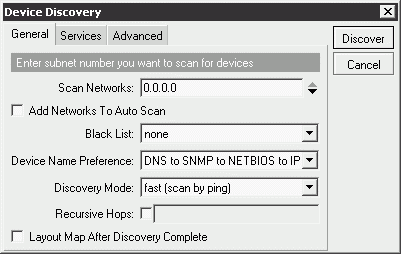
**Рис. 3.4.** Главное окно TheDude

В верхней левой части окна находится окно для перемещения по разделам программы, немного ниже – мини-карта сети. В правой же части отображаются выбранные разделы программы.

Например, раздел *NetworkMaps* \to LocalMap выводит карту сети. Карта строится автоматически на основе сканирования диапазона адресов вашей сети, который задается при первом запуске программы. Найденные устройства отображаются в виде квадратиков с информацией об именах устройств. Программа периодически пингует включенные в карту устройства, выясняя их доступность. Если устройство доступно – оно выделено на карте зеленым цветом, если нет – красным. Пользователь имеет возможность добавлять элементы на карту вручную, экспортировать карту в различные графические форматы.

Для того, чтобы TheDude просканировал определенный диапазон IP-адресов в поисках компьютеров и других устройств – нажмите кнопку Discover, которую можно найти в окошке LocalMap.

В появившемся после этого окне ( [рис. 3.5](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=2#image.3.5)) введите интересующий вас диапазон адресов и запустите сканирование. Так же вы можете сразу же установить галочки AddNetworkToAuto *Scan* для того, чтобы программа в дальнейшем автоматически сканировала выбранный диапазон адресов наряду с другими и LayoutMapAfter *Discovery* Complete – для обновления карты после завершения поиска устройств.



**Рис. 3.5.** Настройка поиска новых устройств

Вкладка этого окна Services служит для настройки *сетевых сервисов*, на которые должна реагировать программа, а Advanced содержит некоторые дополнительные параметры сканирования.

Пожалуй, карта сети – это основная и наиболее интересная возможность программы. Остальные ее инструменты имеют меньшую ценность, хотя, все равно, интересны так как предоставляют дополнительную информацию о сетевых устройствах, о ходе сканирования и так далее.

Следующая программа, которую мы рассмотрим, предназначена для перехвата и анализа пакетов, путешествующих по сети.

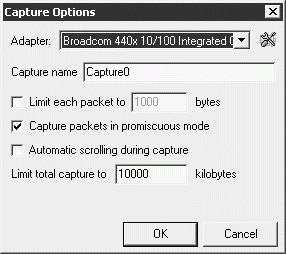
**Packetyzer**

**Packetyzer** – это мощная бесплатная программа для перехвата и анализа сетевых пакетов. Она поддерживает более чем 483 протокола, умеет работать с проводными и беспроводными сетями, легко настраивается.

**Packetyzer** можно скачать на <http://www.networkchemistry.com/products/packetyzer.php>

Размер дистрибутива составляет порядка 11,5 Мб.

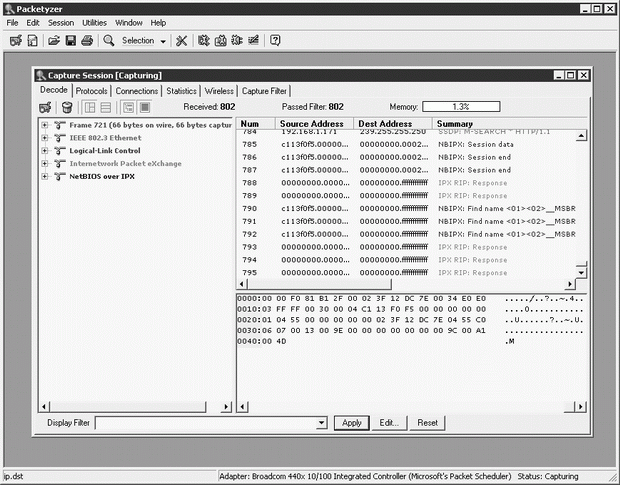
При запуске программа попросит вас указать сетевой адаптер, который будет использоваться для захвата пакетов ( [рис. 3.6](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=2#image.3.6)), здесь же можно ограничить общий размер захваченных пакетов (LimitTotalCaptureto) и максимальную длину одного пакета (LimiteachPacketto). Так же здесь можно включить автоматический скроллинг окна захвата пакетов в течение работы программы (Automaticscrollingduringcapture).



**Рис. 3.6.** Начальная настройка Packetyzer

После этого **Packetyzer** может начинать работу – для включения захвата пакетов надо нажать F5 или выбрать меню Session \to StartCapture. Соответственно, для остановки захвата надо также нажать F5, либо воспользоваться командой меню Session \to StopCapture.

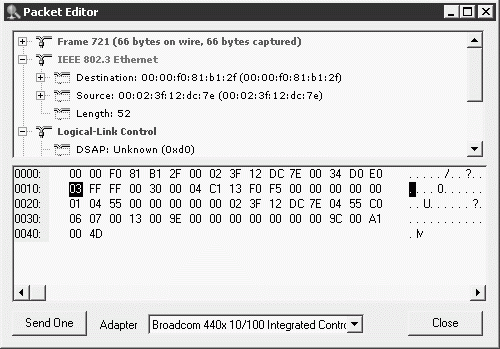
В ходе работы программы осуществляется перехват пакетов, проходящих через выбранный сетевой адаптер ( [рис. 3.7](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=2#image.3.7)).

[](http://www.intuit.ru/EDI/14_08_14_2/1407964674-31059/tutorial/532/objects/3/files/03_07.gif)

**Рис. 3.7.** Packetyzer в работе

На вкладке Deem, в верхней правой части окна программы расположена область, содержащая информацию о захваченных пакетах. Если щелкнуть мышью по одной из строчек этой области, в левой части окна отобразится детальная информация о пакете, в правой нижней части можно видеть этот же пакет в шестнадцатеричном представлении.

Вы можете редактировать пакеты, используя пункт меню Session \to PacketEditing, можете отправлять пакеты, используя средство, которое скрывается за пунктом меню Session \to SendPacket ( [рис. 3.8](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=2#image.3.8)).



**Рис. 3.8.** Правка и отсылка пакета

Новый пакет можно создать на основе выделенного пакета. Отредактировав выделенный пакет (правка осуществляется в шестнадцатеричном виде), вы можете нажать на кнопку SendOne для его отправки.

Результаты сканирования можно сохранить в файл (File \to Save). Так же программа умеет работать с файлами-результатами сканирования в различных форматах.

Теперь давайте рассмотрим вкладки окна сканирования.

Так, вкладка Protocols содержит информацию о типе и количестве пакетов, соответствующих тому или иному протоколу. Информация выводится в графическом виде с разбиением протоколов на группы.

* Вкладка Connections содержит информацию о сетевых соединениях.
* Вкладка *Statistics* – статистику работы программы.
* Вкладка *Wireless* – информацию о работе программы с беспроводными сетями.
* Вкладка CaptureFilter содержит информацию о фильтрах пакетов, в соответствии с которыми осуществляется захват.

Теперь давайте рассмотрим достаточно простую, но эффективную программу для сканирования ресурсов сети.

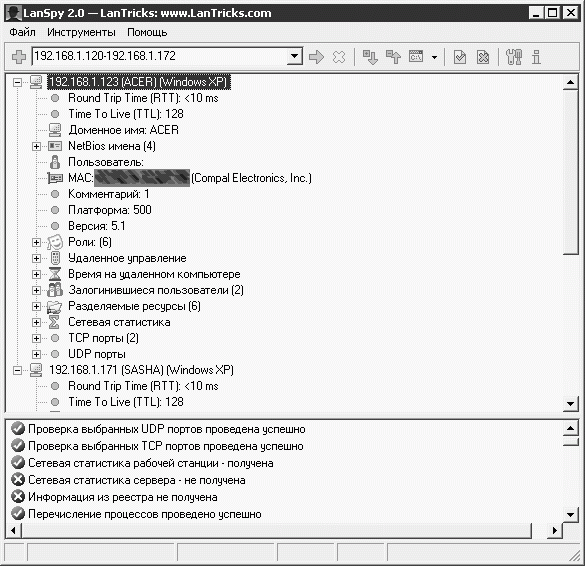
**LanSpy**

Авторы программы утверждают, что LanSpy способен рассказать все или почти все об удаленном компьютере. Если вы попробуете эту программу – вы поймете, что это утверждение очень близко к истине. Программу можно скачать на <http://lantricks.com/lanspy/> , размер дистрибутива составляет около 1,1 Мб.

Итак, перед нами программа для сканирования диапазонов IP-адресов и получения информации о компьютерах, которым соответствуют те или иные адреса. Если вы – администратор достаточно большой локальной сети – эта программа поможет вам узнать подробности о компьютерах, подключенных к вашей сети.

LanSpy поддерживает русский и английский языки. Для переключения между языками используйте меню Файл \to Язык или File \to Language.

Программа проста в использовании – вы запускаете ее, задаете диапазон IP-адресов ( [рис. 3.9](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.9)) в поле, расположенном в верхней части окна программы и нажимаете Enter или кнопку с зеленой стрелочкой.



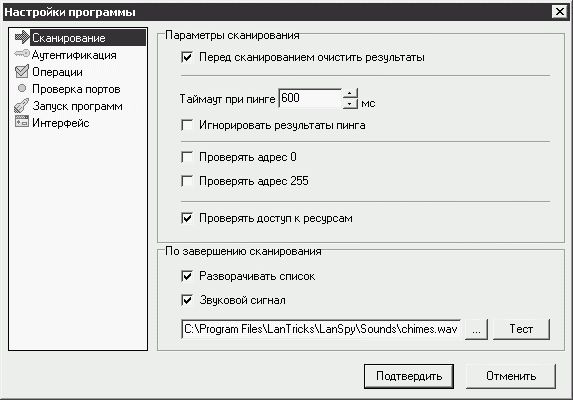
**Рис. 3.9.** Сканирование сети с помощью LanSpy

После этого начинается сканирование, ход которого отображается в окошке, расположенном в нижней части окна программы. А в верхней части вы можете видеть информацию об активных компьютерах. Информация это довольно обширна. Кроме различных статистических данных о работе сети, мы получаем сведения о IP-адресе, сетевом имени и MAC-адресе компьютера, далее, программа выводит список общих ресурсов, открытых TCP и UDP-портов и так далее.

LanSpy имеет настройки (Файл \to Настройки), наиболее полезные из которых мы сейчас рассмотрим.

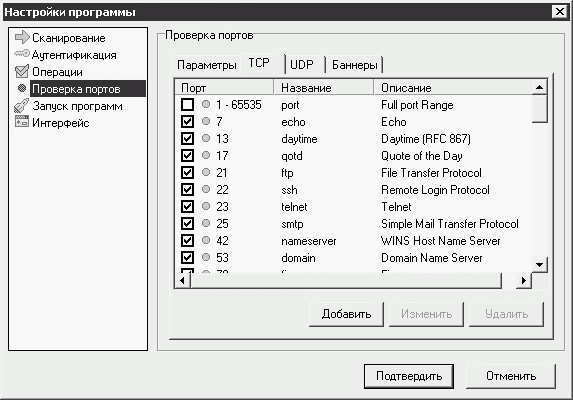
Так, в разделе настройки Сканирование ( [рис. 3.10](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.10)). вы можете уменьшить таймаут при пинге для увеличения скорости сканирования, однако, помните, что при слишком малом таймауте (это зависит от скорости соединения и загруженности сети) система может просто не успеть ответить.

Установив галочку Игнорировать результаты пинга вы можете повысить вероятность нахождения рабочей системы в вашей сети даже в том случае, если она не отвечает на **ping** -запрос.



**Рис. 3.10.** Настройка параметров сканирования

На [рис. 3.11](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.11) вы можете видеть окно настройки параметров сканирования TCP-портов.



**Рис. 3.11.** Настройка параметров сканирования TCP-портов

По умолчанию программа производит сканирование обычно применяемых портов из списка. При желании вы можете просканировать весь диапазон TCP-портов, установив галочку в поле 1-65535, либо – добавить порт, который вам хотелось бы просканировать, вручную, нажав на кнопку Добавить и заполнив поля появившегося окна.

Эту возможность удобно использовать для проверки вашей сети на предмет наличия *троянских программ* на ее компьютерах. Для быстрой проверки можно задать известные порты троянцев (их можно найти в Интернете по ключевым словам "порты *троянских программ*") и периодически сканировать машины вашей сети на предмет наличия на них открытых портов, которые с высокой долей вероятности принадлежат "*троянским коням*".

Аналогичные настройки есть и для UDP-портов, для них также справедливо все вышесказанное о вредоносном ПО.

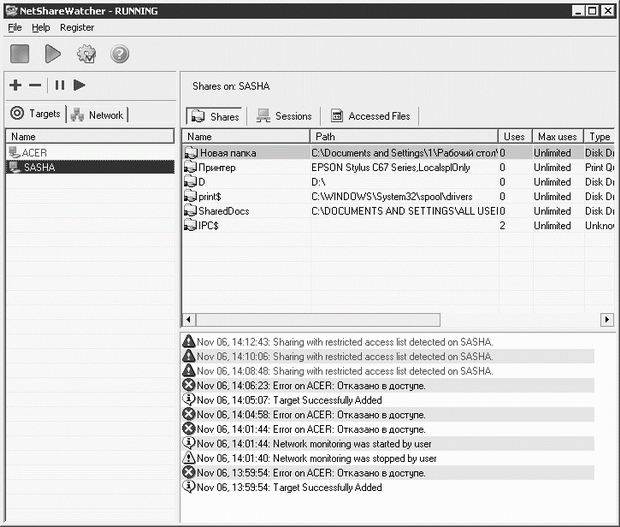
Теперь давайте рассмотрим программу для работы с разделяемыми ресурсами сети.

**NetShareWatcher**

Разделяемые ресурсы – например – папки – это один из обязательных атрибутов любой локальной сети. Но помимо очевидной пользы общая папка может послужить средством для распространения в сети вредоносных программ или, например, папка с файлами только для чтения может быть несанкционированно преобразована в папку, файлы которой могут быть изменены, что, в результате, может привести к плохим последствиям для локальной сети.

Программа, которую мы сейчас рассмотрим, называется NetShareWatcher. Предназначена она для мониторинга общих ресурсов компьютеров, подключенных к локальной сети. Дистрибутив программы занимает около 1,5 Мб, скачать ее можно с <http://netsharewatcher.nsauditor.com/>

На [рис. 3.12](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.12) вы можете видеть рабочее окно программы.

[](http://www.intuit.ru/EDI/14_08_14_2/1407964674-31059/tutorial/532/objects/3/files/03_12.gif)

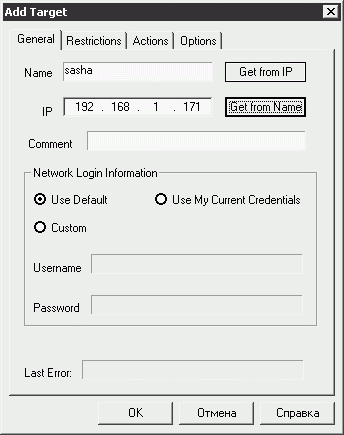
**Рис. 3.12.** Рабочее окно NetShareWatcher

В левой части окна программы можно увидеть две вкладки – Targets и Network. С помощью вкладки Network вы можете просматривать вашу локальную сеть и добавлять ее компьютеры и рабочие группы в список "целей" для слежения за общими ресурсам, то есть – на вкладку Target.

Сделав щелчок правой кнопкой мыши по имени компьютера или рабочей группы в окне Network, вы можете выбрать пункт Addtotargets (для компьютера) или AddDomaintotargets (для рабочей группы), после чего выбранный ресурс будет добавлен на вкладку Targets. Так же добавить компьютер на эту вкладку можно, щелкнув значок "+", расположенный над вкладками и в появившемся окне заполнить свойства "цели".

На этом этапе работы с программой мы остановимся подробно – именно он является ключевым в использовании программы так как окно, аналогичное добавлению "цели", служит для настройки слежения за общими ресурсами компьютеров, уже добавленных в список Targets.

Итак, первая вкладка окна настройки параметров "цели" называется General( [рис. 3.13](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.13)). Она имеет два *ключевых поля* – Namе – то есть имя компьютера, и IP – то есть его IP-адрес. Введя имя или адрес компьютера, вы можете заполнить второе автоматически, нажав соответствующую кнопку – Getfrom IP или GetFromName – для получения имени по IP-адресу или IP-адреса по имени компьютера.



**Рис. 3.13.** Настройка общих параметров устройства

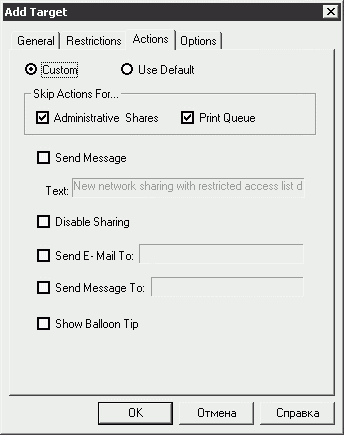
При необходимости установите переключатель NetworkLoginInformation в позицию Custom и введите в поле **Username** имя пользователя для входа в сеть и в поле **Password** сетевой пароль.

Далее, на вкладке Restrictions, вам понадобится задать группы пользователей ( [рис. 3.14](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.14)), для которых требуется назначить права доступа к общим ресурсам. Надо отметить, что назначать права доступа вы можете (даже скорее должны так как обычно различные общие ресурсы несут различные функции) для каждого отдельного общего ресурса.



**Рис. 3.14.** Назначение разрешений группам пользователей

Далее, обратите внимание на вкладку Actions( [рис. 3.15](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=3#image.3.15)).



**Рис. 3.15.** Настройка реакции программы на события

В случае, если произойдет какое-либо событие, касающееся нарушения прав доступа к общему ресурсу, программа может отправить сообщение (SendMessage), заданное полем Text, на E-Mail, показать предупреждение в трее (ShowBaloonTip), запретить доступ к общему ресурсу (DisableSharing). Выполняемое действие может не выполняться для особых административных разделяемых ресурсов (их можно задать на вкладке Options) и для очередей печати – включить или отключить эту возможность можно галочками AdministrativeShares и PrintQueue.

Когда опции разделяемых ресурсов настроены, программа работает в фоновом режиме, отслеживая события, связанные с этими ресурсами. Включать и выключать мониторинг ресурсов можно кнопками StartMonitoring и StopMonitoring, расположенными в верхней части окна программы.

Кроме всего прочего NetShareWatcher может показывать информацию о том, кто в настоящий момент использует общие ресурсы компьютера – для этого вам нужно выделить интересующий вас компьютер в окне Targets и выбрать в правой части окна программы вкладку AccessedFiles

Поговорив о мониторинге общих ресурсов, перейдем к еще одной интересной теме, а именно – к удаленному управлению компьютером.

**AccessRemote PC**

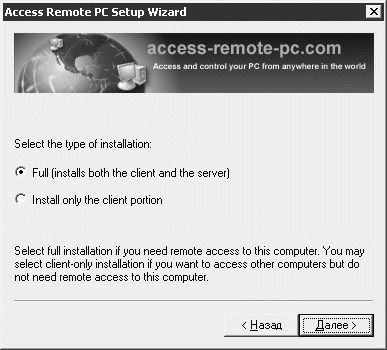
Существует немало программ, организующих удаленный доступ к компьютеру. Как правило, схема такого доступа выглядит так: на управляемом компьютере запускается серверная часть программы, на управляющем – клиентская, после чего пользователь, сидящий за компьютером-клиентом может управлять машиной, где работает серверная часть. AccessRemote PC построен именно по такому принципу. Программа позволяет получать полный доступ к удаленному компьютеру, причем не только через локальную сеть, но и через Интернет. Помимо доступа у нее есть некоторые полезные возможности, которые делают ее интересной для целей обучения (в частности – в компьютерных классах учебных заведений).

Итак, AccessRemote PC можно скачать на [http://www.access-remote-pc.com](http://www.access-remote-pc.com/) Размер дистрибутива составляет около 1,8 Мб. Программа это платная, причем, существует она в разных версиях, с особенностями которых можно ознакомиться на ее сайте. Пробная версия рассчитана на 30 запусков, причем в ходе испытания программы она функционирует без каких-либо ограничений, то есть вы сможете в полной мере испытать ее возможности.

Давайте рассмотрим особенности установки и использования AccessRemote PC.

Программу надо установить на всех компьютерах, которыми вы хотите управлять, равно как и на том компьютере (или компьютерах), с которого вы хотите заниматься управлением других машин.

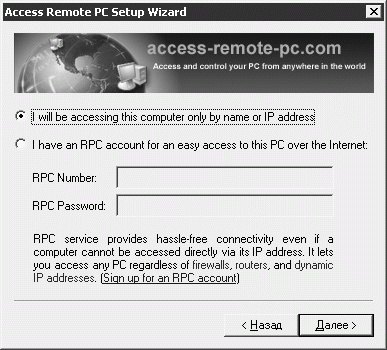
В ходе установки вам будет предложено либо установить на компьютере полную конфигурацию программы, либо – лишь клиентскую часть ( [рис. 3.16](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.16)).



**Рис. 3.16.** Выбор объема устанавливаемой программы

Если вы хотите, чтобы компьютером, на который устанавливается программа, можно было управлять с других машин – выбирайте полную версию (Full), если же вы не хотите этого, то есть собираетесь лишь управлять с этого компьютера другими – можете выбрать Installonlytheclientportion.

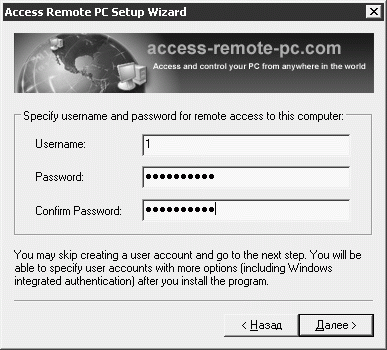
В одном из следующих окон вам зададут вопрос – хотите ли вы получать доступ к вашему ПК лишь используя его IP-адрес или сетевое имя (I willbeaccessingthiscomputeronlybynameor IP-Address) , или же вы желаете воспользоваться сервисом RPC (I havean RPC account…) ( [рис. 3.17](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.17)).



**Рис. 3.17.** Выбор способа подключения к ПК

Если вы собираетесь пользоваться программой серьезно и долго, получать доступ к вашему ПК через Интернет – вам есть смысл зарегистрироваться на сервере компании, получить номер RPС и пользоваться ими. Ну а если ваши нужды ограничены локальной сетью – ничего не меняйте в этом окне, просто нажав кнопку Далее.

Теперь – еще один ключевой момент установки. Вам предложат задать имя пользователя и пароль, которые впоследствии будут использоваться для управления данным компьютером с других машин ( [рис. 3.18](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.18)).



**Рис. 3.18.** Задаем имя пользователя и пароль для доступа к ПК

Эти параметры можно задать и позже, после установки программы, но мы зададим их сразу. Теперь установка программы на одном из компьютеров завершена. Точно также установим ее на другие машины (в целях безопасности вы можете задавать разные пароли на разных компьютерах, хотя если вы не хотите возиться с разными именами и паролями – можете задать один и тот же для всех компьютеров сети).

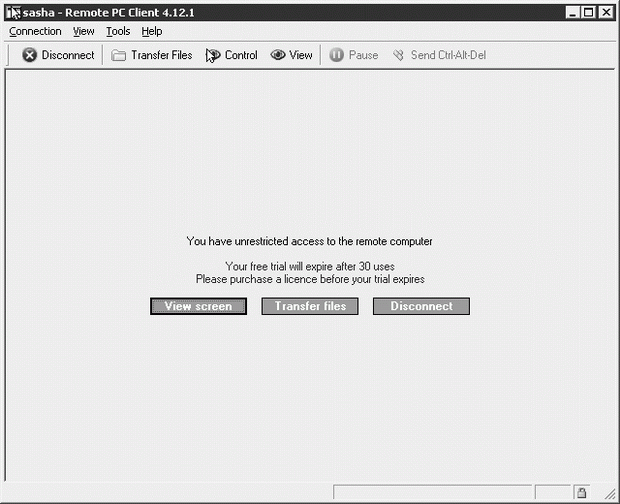
После установки значок программы появляется в трееWindows. По умолчанию AccessRemote PC запускается вместе с системой.

После того, как программа установлена на всех машинах, можно попытаться установить соединение. Для этого надо запустить Remote PC Client с помощью значка на рабочем столе ( [рис. 3.19](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.19))

[](http://www.intuit.ru/EDI/14_08_14_2/1407964674-31059/tutorial/532/objects/3/files/03_19.gif)

**Рис. 3.19.** Начало подключения к удаленному компьютеру

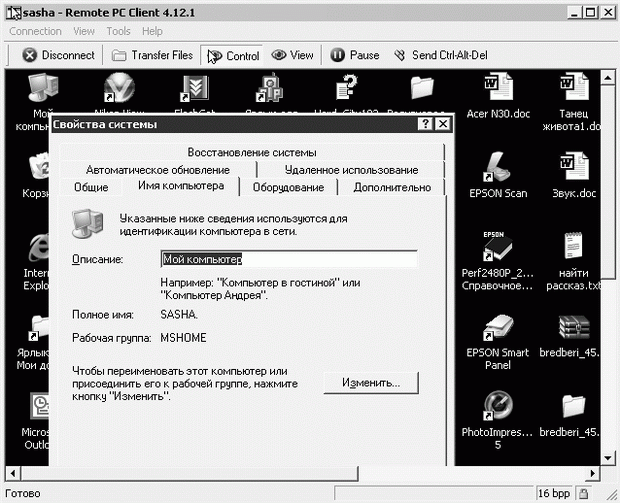
В первом окне Remote PC Client попросит вас ввести имя, IP-адрес или RPC-номер компьютера, к которому вы хотите подключиться. Мы ввели имя компьютера (Sasha), после чего система запросила ввод имени пользователя и пароля. Мы ввели имя пользователя и пароль (те, которые указывали при установке программы на компьютер, видимый в сети под именем Sasha) и Remote PC Client предложил выбрать один из вариантов действий ( [рис. 3.20](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.20)).

[](http://www.intuit.ru/EDI/14_08_14_2/1407964674-31059/tutorial/532/objects/3/files/03_20.gif)

**Рис. 3.20.** Выбор действия

А именно, нажав кнопку ViewScreen (просмотр экрана) мы увидим экран управляемого компьютера в окошке клиента, нажав Transferfiles (передача файлов) увидим нечто вроде двух Проводников – один – в правой части окна – для удаленной системы, второй – в левой – для той, за которой мы работаем. Эти же кнопки продублированы в верхней части окна.

Теперь нажимаем кнопку ViewScreen и тут же можем работать с удаленным компьютером так, как будто сидим за ним ( [рис. 3.21](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.21)).

[](http://www.intuit.ru/EDI/14_08_14_2/1407964674-31059/tutorial/532/objects/3/files/03_21.gif)

**Рис. 3.21.** Работа с удаленным компьютером

В ходе работы вы можете переключаться между режимами взаимодействия с компьютером с помощью кнопок в верхней части окна программы и управлять некоторыми параметрами.

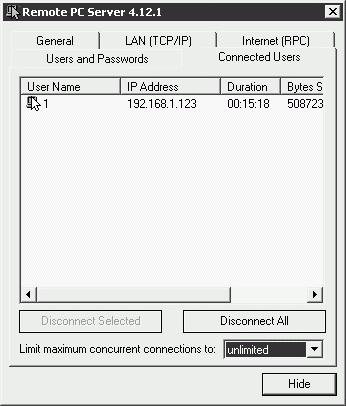
В частности, командой Tools \to EnableSound можно передачу звуков с удаленного компьютера и, при желании, настроить качество звука командой Tools \to SoundOptions.

Очень удобно использовать удаленный рабочий стол в полноэкранном режиме – так разница между работой непосредственно за компьютером и управлением им практически незаметна. Для того, чтобы включить полноэкранный режим – выберите пункт меню View \to FullScreen. Для возврата в оконный режим нажмите Ctrl+Escape.

Переключив программу в режим View и подключив несколько компьютеров к одному, вы передаете изображение с одного ПК на многие, что удобно, например, при объяснении новой темы в компьютерном классе.

Для завершения сеанса связи нажмите кнопку Disconnect.

Теперь давайте рассмотрим настройки серверной части программы. Открыть их окно можно, сделав двойной щелчок по пиктограмме AccessRemote PC в трее ( [рис. 3.22](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.22)).

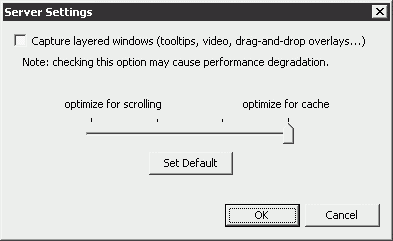


**Рис. 3.22.** Настройка серверной части программы

Вкладка ConnectedUsers позволяет просматривать информацию о подключенных пользователях, отключать их всех (DisconnectAll), либо – только выделенного (DisconnectSelected), а также управлять количеством подключений.

Вкладка UsersandPasswords позволяет добавлять в систему новых пользователей (New), редактировать существующих (Edit) и удалять их (Delete).

Вкладка General помимо вполне стандартных установок AutomaticallystartwhenWindowsStarts (Запускаться вместе с Windows) и ShowIconinTascbar (показывать иконку на панели задач) содержит очень важную группу настроек, к которой ведет ссылка AdvancedSettings( [рис. 3.23](http://www.intuit.ru/studies/courses/509/365/lecture/8669?page=4#image.3.23)).



**Рис. 3.23.** Дополнительные опции сервера

Установив галочку в поле CapturelayeredWindows… вы сможете просматривать видео, воспроизводимое на удаленном компьютере, в окне клиента. Однако, это сильно увеличит нагрузку на систему, что может привести к замедлению ее работы.

Вкладка LAN (TCP/IP) содержит настройки порта, на котором "сидит" сервер и параметров подключения (их вполне можно оставить по умолчанию), а вкладка Internet (RPC) позволяет настраивать доступ к ПК через Интернет, в частности, позволяет ввести его RPC-номер если вы зарегистрировались в системе.

В ходе работы программы не было замечено серьезных сбоев. Как видите, AccessRemote PC – это отличное решение для тех, кто хочет управлять компьютером дистанционно.

**Задание на лабораторную работу**

Оформите отчет по лабораторной работе. Выполнить работу с 5 и более работоспособными сервисами, опишите последовательность действий.