Министерство образования Республики Беларусь
Учреждение образования «Полоцкий государственный университет»

Факультет информационных технологий
Кафедра технологий программирования

Методические указания
к выполнению лабораторной работы №3

по дисциплине «**Компьютерные системы и сети**»
для специальности 1-40 01 01 Программное обеспечение информационных технологий

на тему «**Удалённый доступ через VPN**»

Полоцк, 2018 г.

Название: «Удалённый доступ через VPN».

Цель работы: Изучение удаленного доступа через VPN. Получение практических навыков в настройке сервера и клиента VPN.

Теоретическая часть

Удаленный доступ

В самом простом приближении под корпоративной сетью принято понимать локальную сеть некоторой организации (или совокупность локальных сетей, соединенных между собой некоторым образом). Достаточно важной составляющей любой современной корпоративной сети являются пользователи, внешние по отношению к локальной сети. Это могут быть как мобильные пользователи (например, сотрудники корпорации, путешествующие с ноутбуками), так и стационарные (например, удаленный дилер компании). Важным является тот факт, что независимо от типа, этим пользователям периодически необходим доступ к ресурсам вашей корпоративной сети.

Данная проблема может быть решена посредством развертывания в корпоративной сети службы удаленного доступа (remote access service). Под удаленным доступом понимается решение, основанное на маршрутизации обращений подключающегося удаленного клиента в локальную сеть корпорации. Все приложения, посредством которых происходит доступ к ресурсам корпоративной сети, функционируют непосредственно на стороне клиента.

Служба маршрутизации и удаленного доступа

В Windows Server 2003 реализована Служба маршрутизации и удаленного доступа (Routing and Remote Access Service, RRAS), позволяющая удаленным пользователям подключаться к корпоративным вычислительным сетям. При этом подключение может быть выполнено как по коммутируемой линии, так и через виртуальные частные сети (Virtual Private Network, VPN). При коммутируемом соединении клиент удаленного доступа устанавливает коммутируемую связь для подключения к физическому порту на сервере удаленного доступа, используя некоторую службу-посредника для передачи данных, например, аналоговый телефон, ISDN или X.25. Наиболее типичный пример коммутируемого доступа – установление соединения клиентом удаленного доступа при помощи модема, т. е. путем набора телефонного номера одного из портов сервера удаленного доступа. Соединение с виртуальной частной сетью (или VPN-подключение) представляет собой защищенное соединение типа «точка-точка» через сеть общего пользования (например, Интернет) или большую корпоративную сеть. Поддержка службой удаленного доступа механизма виртуальных частных сетей позволяет устанавливать безопасное соединение с корпоративной сетью через различные открытые сети (такие, например, как Интернет). Для эмуляции прямого соединения данные инкапсулируются специальным способом, т. е. снабжаются специальным заголовком, который предоставляет информацию, необходимую для маршрутизации, чтобы пакет

мог достигнуть адресата. Получателем пакета является VPN-клиент либо VPN-сервер. Часть пути, по которому данные следуют в инкапсулированном виде, называется туннелем. Для организации безопасной виртуальной частной сети перед инкапсуляцией данные шифруются. Перехваченные по пути следования пакеты невозможно прочитать без ключей шифрования. Участок VPN соединения, на котором данные передаются в зашифрованном виде, и называется, собственно, виртуальной частной сетью. Сервер удаленного доступа в случае использования механизма виртуальных частных сетей выступает в качестве посредника, осуществляя обмен данными между клиентом VPN и корпоративной сетью. При этом сервер удаленного доступа осуществляет все необходимые преобразования данных (шифрование/дешифрование). Для этого используются специальные протоколы туннелирования (tunneling protocols). VPN-клиент и VPN-сервер должны использовать один и тот же протокол туннелирования, чтобы создать VPN-соединение. В службе удаленного доступа в Windows Server 2003 реализована поддержка протоколов туннелирования PPTP и L2TP.

Сервер удаленного доступа в Windows Server 2003 является частью интегрированной Службы маршрутизации и удаленного доступа (Routing and Remote Access Service, RRAS). Пользователи устанавливают соединение с сервером удаленного доступа при помощи клиентского программного обеспечения удаленного доступа, которое имеется в составе любой версии Windows. Сервер удаленного доступа (под которым мы в дальнейшем подразумеваем любой компьютер под управлением Windows Server 2003, на котором установлена служба маршрутизации и удаленного доступа) аутентифицирует как пользователей, так и сеансы связи удаленных маршрутизаторов. Все службы, доступные пользователям, работающим в локальной сети (включая доступ к совместно используемым файлам и принтерам, доступ к веб-серверам и серверам электронной почты), доступны также и пользователям, подключающимся удаленно (через сервер удаленного доступа).

Устройства и порты службы удаленного доступа

На сервере удаленного доступа под управлением Windows Server 2003 установленное сетевое оборудование отображается в виде ряда устройств и портов. Под устройством (devices) понимается аппаратное или программное обеспечение, которое предоставляет службе удаленного доступа порты для установки соединений «точка-точка». Различают устройства физические (такие, например, как модем) и виртуальные (например, VPN-подключение). Устройство может поддерживать как один порт (например, модем), так и несколько портов (например, модемный пул, способный предоставить 64 независимых входящих аналоговых коммутируемых соединения). Протоколы PPTP или L2TP – примеры виртуальных многопортовых устройств. Каждый из этих туннельных протоколов поддерживает несколько одновременных VPN-подключений. Под портом (port) понимается отдельный канал устройства, способный поддерживать одно соединение «точка-точка». Для однопортовых устройств типа модема понятия «устройство» и «порт»

совпадают. Для многопортовых устройств порт представляет собой часть устройства, посредством которого может быть установлено отдельное соединение «точка-точка».

Использование сервера удаленного доступа для обслуживания VPN-подключений

Сервер удаленного доступа под управлением Windows Server 2003 может обслуживать VPN-подключения, выступая в качестве VPN-сервера. Необходимо понимать, что фактически речь идет о все том же удаленном доступе к ресурсам корпоративной сети. Однако, в отличие от обычного удаленного доступа, взаимодействие клиента и сервера осуществляется по защищенному каналу, который реализуется за счет использования специальных протоколов туннелирования. Использование механизма виртуальных частных сетей (VPN) оправдано в ситуации, когда нельзя исключать риск перехвата конфиденциальных данных (например, если взаимодействие с удаленным клиентом реализуется через открытые общественные сети). Если администратор планирует использовать сервер удаленного доступа для обслуживания VPN-подключений, он должен определить, какой из протоколов туннелирования будет использоваться для создания защищенного канала. Администратор должен выбрать между протоколом PPTP и протоколом L2TP. **Протокол PPTP** поддерживается всеми клиентами Microsoft (в том числе старыми версиями Windows). Минусом этого протокола является отсутствие механизмов, гарантирующих целостность передаваемых данных и подлинность участников соединения. **Протокол L2TP** свободен от этих недостатков. В целом он является более предпочтительным вариантом, нежели протокол PPTP. Протокол L2TP базируется на использовании протокола IPSec, поддержка которого реализована в операционных системах Windows 2000/XP и Windows Server 2003. Для использования протокола L2TP на других Windows-платформах (Windows 98/ME и Windows NT 4.0) требуется специальный клиент – Microsoft L2TP/IPSec Client.

Если администратором в качестве средства создания защищенного канала был выбран протокол туннелирования L2TP, он должен определить, как именно будет осуществляться взаимная аутентификация участников VPN-соединения. Протокол IPSec, поверх которого функционирует протокол туннелирования L2TP, поддерживает **два способа аутентификации участников соединения**: **цифровые сертификаты** (речь идет о цифровых сертификатах, назначаемых компьютерам) и **разделяемый ключ** (pre-shared key). С точки зрения безопасности более надежным способом является использование цифровых сертификатов.

Внимание:

Для получения цифровых сертификатов в корпоративной сети должна быть развернута служба сертификации (PKI). Если взаимодействие с удаленными пользователями строится через открытую общественную сеть (такую, как Интернет), необходимо позаботиться о том, чтобы настройки корпоративного брандмауэра разрешали

прохождение VPN-трафика. В противном случае удаленные пользователи не смогут создать VPN-соединение с сервером удаленного доступа.

Развертывание сервера удаленного доступа

Чтобы обеспечить работу сервера удаленного доступа на Windows Server 2003, необходимо соответствующим образом сконфигурировать службу маршрутизации и удаленного доступа (**Routing and Remote Access Service**). Для управления этой службой используется оснастка **Routing and Remote Access** (Маршрутизация и удаленный доступ), которая располагается в меню **Administrative Tools** (Администрирование). Данная оснастка может использоваться в качестве инструмента для управления всеми серверами удаленного доступа под управлением Windows Server 2003, установленными в пределах корпоративной сети. В ходе инсталляции системы устанавливаются все программные компоненты, необходимые для функционирования службы маршрутизации и удаленного доступа. Однако по окончании установки эта служба отключена. Прежде чем администратор сможет запустить данную службу, он должен выполнить ее конфигурирование, определив ее роль.

Конфигурирование службы маршрутизации и удаленного доступа осуществляется при помощи специального мастера Routing and Remote Access Server Setup Wizard. Для запуска этого мастера необходимо в пространстве имен оснастки вызвать контекстное меню объекта, ассоциированного с сервером, и выбрать в нем пункт **Configure and Enable Routing and Remote Access** (Настроить и включить маршрутизацию и удаленный доступ) (рисунок 1).

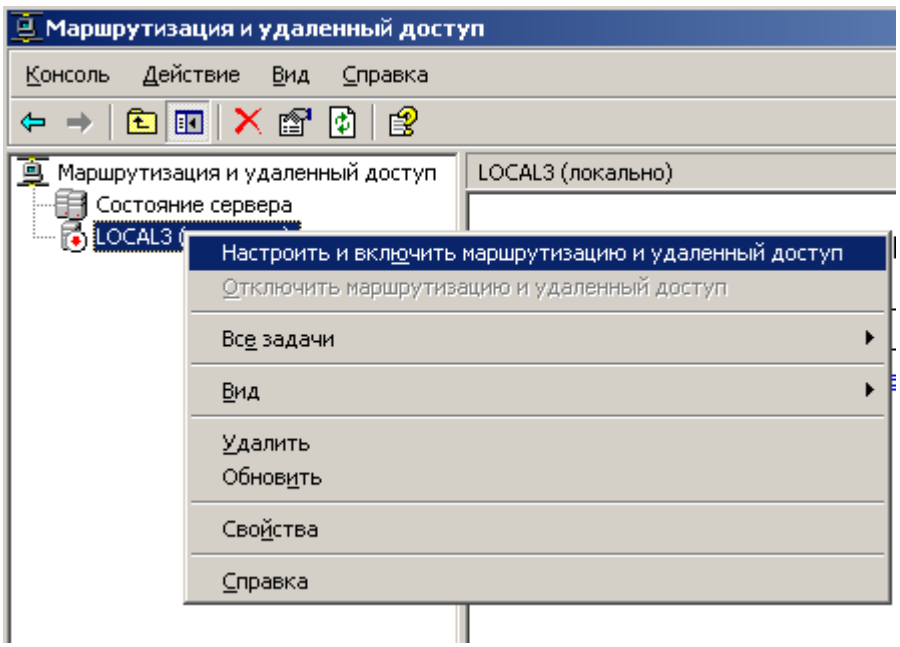


Рисунок 1 – Конфигурирование сервера «Маршрутизации и удаленного доступа»

При помощи указанного мастера администратор может сконфигурировать сервер в качестве маршрутизатора, сервера удаленного

доступа, активизировать на нем механизм трансляции сетевых адресов. В контексте нашей темы, рассмотрим процесс конфигурирования сервера удаленного доступа. Перед выполнением процедуры конфигурирования сервера удаленного доступа необходимо принять решение по следующим вопросам:

- **каким образом будет осуществляться распределение IP-адресов между клиентами удаленного доступа?** Существует два варианта решения этой проблемы. Первый вариант предполагает использование корпоративного DHCP-сервера. Во втором случае клиенты получают IP-адреса непосредственно от сервера удаленного доступа из некоторого статического пула, определенного администратором;
- **какое максимальное количество входящих подключений будет использоваться?** От ответа на этот вопрос зависит то, сколько модемов, ориентированных на подключение удаленных пользователей, потребуется подключить к серверу удаленного доступа;
- **какая модель конфигурирования параметров удаленного подключения будет использоваться?** Параметры удаленного подключения могут задаваться на уровне учетных записей отдельных пользователей или определяться политикой удаленного доступа. На этапе развертывания сервера удаленного доступа должны быть произведены все необходимые настройки учетных записей пользователей, а также определены параметры политик удаленного доступа;
- **какая будет использоваться схема аутентификации?** Имеется два варианта — либо аутентификация выполняется непосредственно сервером удаленного доступа, либо используются средства протокола RADIUS и службы аутентификации IAS. Использование службы аутентификации IAS и протокола RADIUS оправдано в ситуации, когда в сети имеется несколько серверов удаленного доступа. В этом случае администратор имеет возможность реализовать централизованное управление процессом аутентификации пользователей.

Запустив, мастер конфигурирования сервера удаленного доступа, необходимо перейти к окну **Configuration** (Конфигурация), в котором мастер предлагает определить роль конфигурируемого сервера (рисунок 2). Выберите пункт **Remote access (dial-up or VPN)** («Удаленный доступ (VPN или модем)») и перейдите к следующему окну. В окне **«Remote Access»** (рисунок 3) необходимо уточнить функции, которые будет выполнять конфигурируемый сервер. Если сервер должен обслуживать обычные модемные подключения удаленных пользователей, необходимо установить флажок **Dial-up**. Флажок **VPN** следует устанавливать только в том случае, если сервер должен также обслуживать VPN-подключения внешних пользователей (подключающихся, например, через Интернет). Далее требуется определить способ предоставления подключающимся клиентам IP-адресов, необходимых для работы в корпоративной сети (рисунок 4).

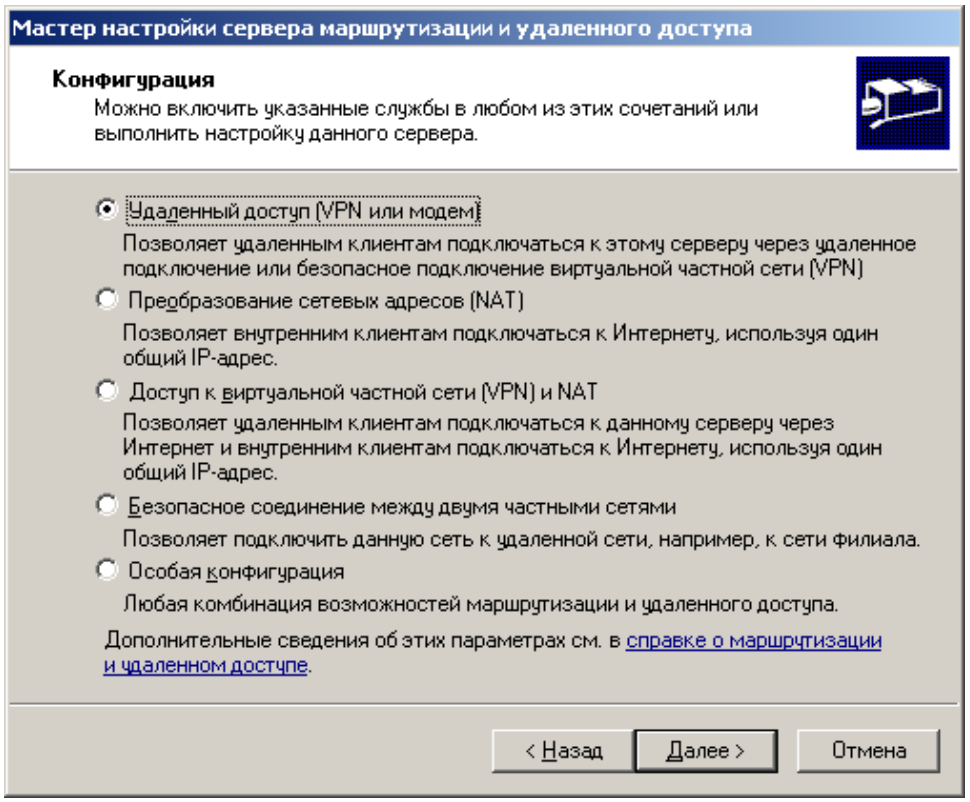


Рисунок 2 – Определение роли службы маршрутизации и удаленного доступа

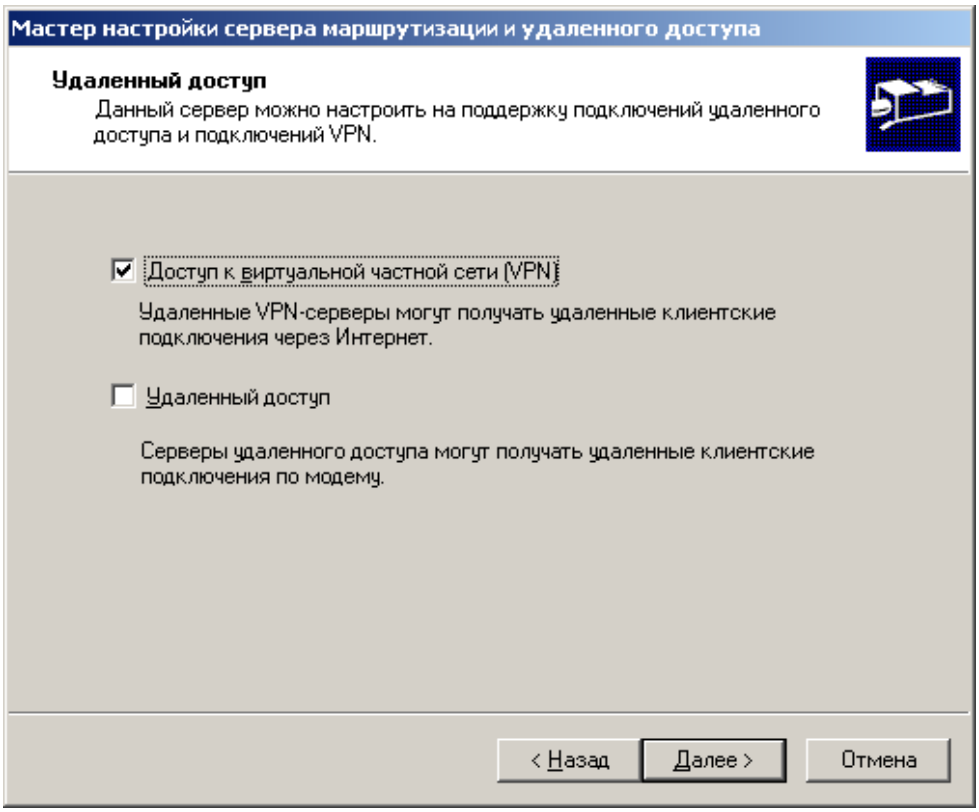


Рисунок 3 – Определение типов подключений, которые будут разрешены на конфигурируемом сервере удаленного доступа

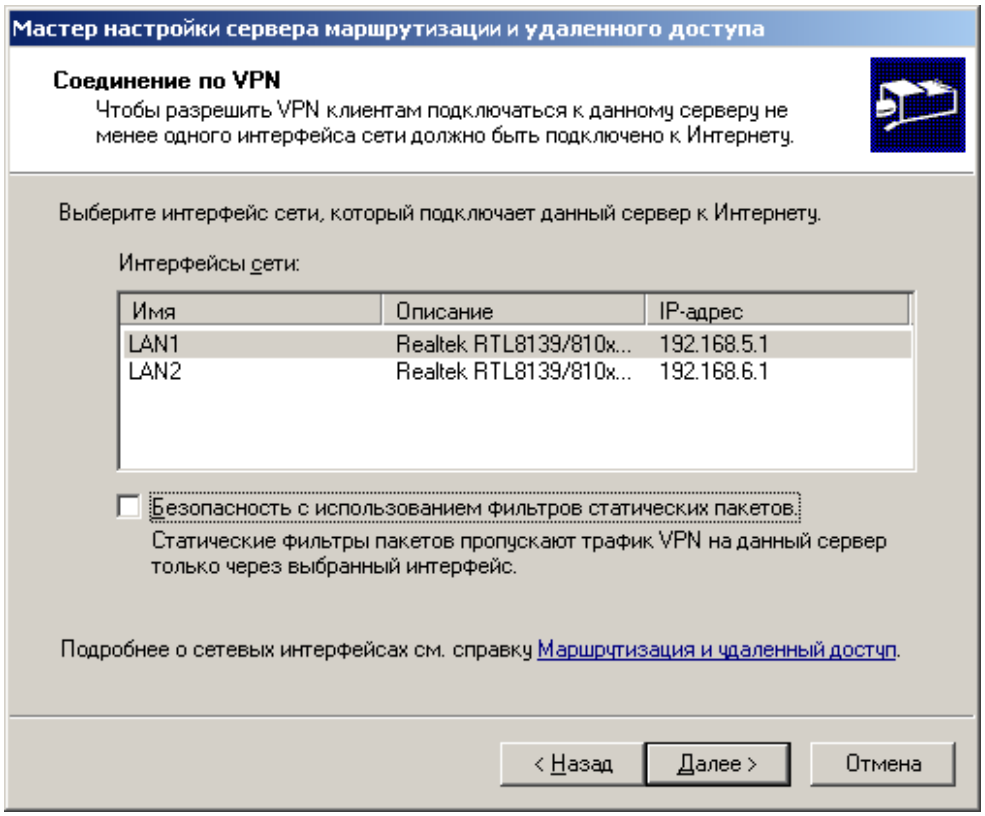


Рисунок 4 – Указание способа предоставления клиентам IP-адреса

Выбор опции **Automatically** (Автоматически) означает использование DHCP-сервера. Если администратор хочет выделять адреса из статического пула, необходимо выбрать опцию **From a specified range of addresses** (Из заданного диапазона адресов). В последнем случае администратор должен будет задать этот диапазон в следующем окне. И, наконец, в последнем окне мастера (рисунок 6) необходимо ответить на запрос об использовании сервера RADIUS – т. е. выбрать схему аутентификации пользователей. Если аутентификация будет выполняться непосредственно сервером удаленного доступа, необходимо выбрать опцию **No, use Routing and Remote Access to authenticate connection requests** (Нет, использовать для аутентификации запросов службу маршрутизации и удаленного доступа). В случае использования для аутентификации сервера RADIUS необходимо выбрать значение **Yes, set up this server to work with a RADIUS server** (Да, настроить этот сервер для работы с RADIUS-сервером).

По окончании своей работы мастер запустит службу маршрутизации и удаленного доступа. Начиная с этого момента, сервер удаленного доступа готов обслуживать подключения удаленных пользователей.

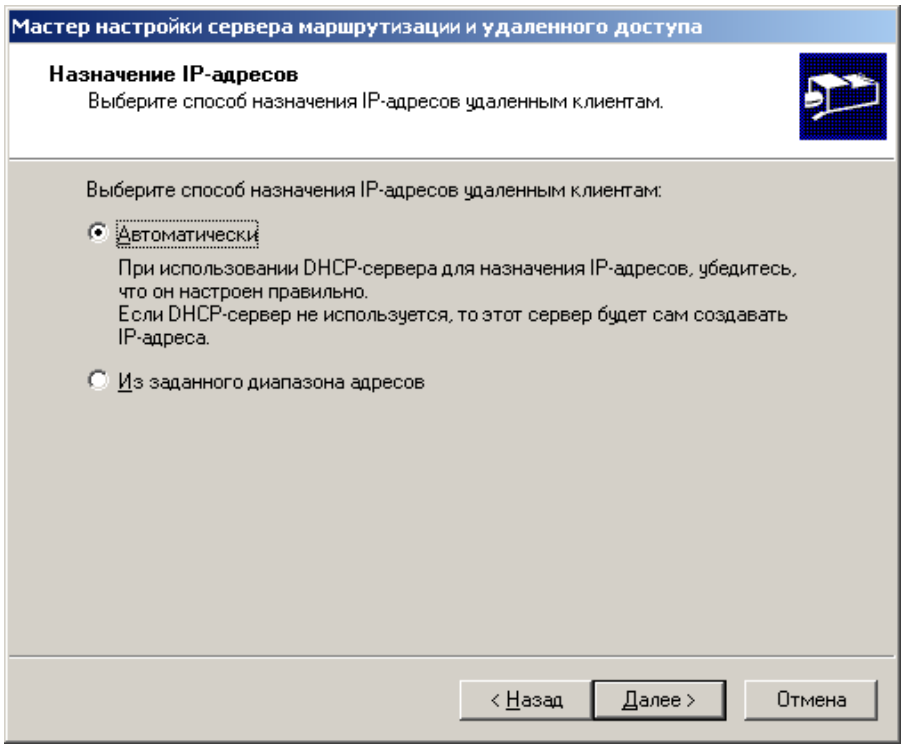


Рисунок 5 – Определение способа назначения IP-адресов удаленным клиентам

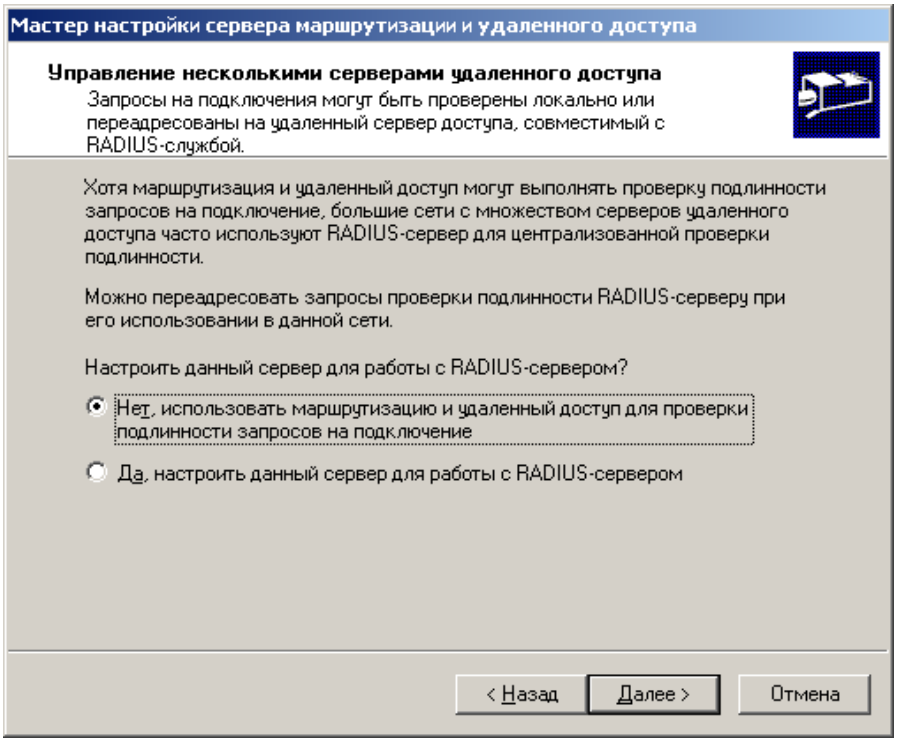


Рисунок 6 – Выбор способа аутентификации клиентов удаленного доступа

Настройки необходимые для подключения клиента

Настройка профиля пользователя на сервере.

Для организации VPN подключения необходимо создать профиль пользователя, который будет подключатся через удаленный доступ.

Зайдите в «Управление компьютером», далее в «Локальные пользователи и группы», «Пользователи».

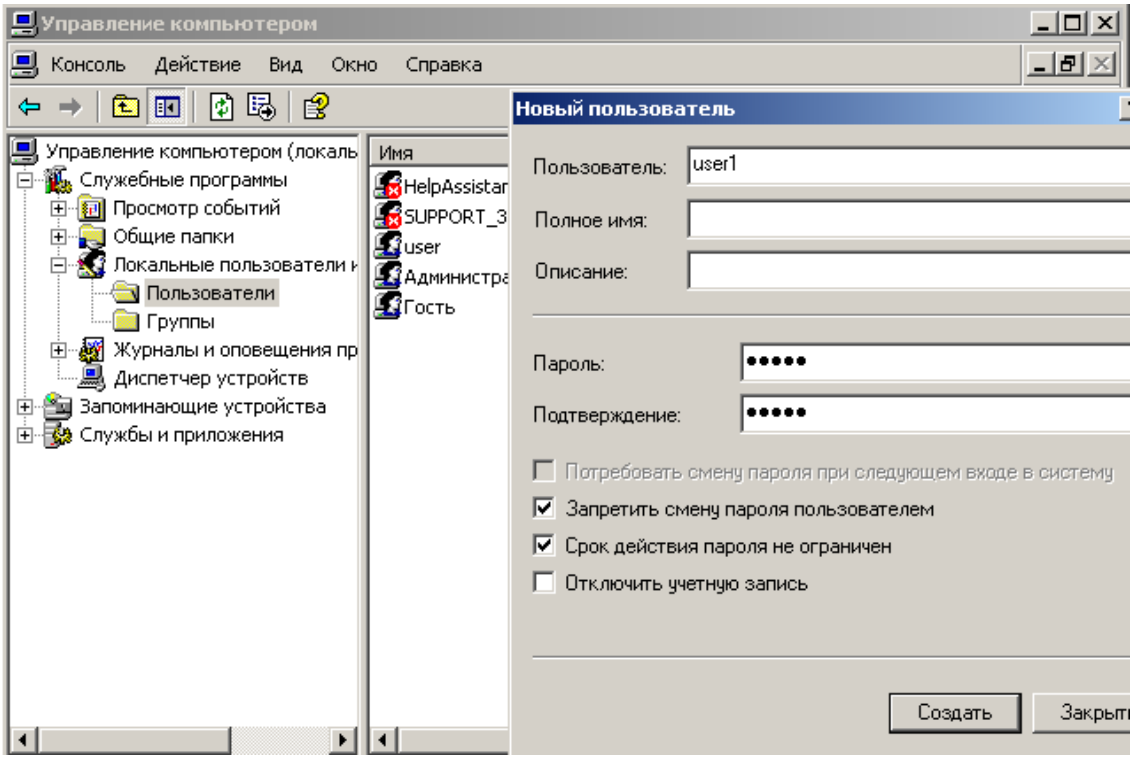


Рисунок 7 – Создание пользователя

Создайте пользователя далее зайдите во вкладку «Входящие звонки», поставьте указатель напротив «Разрешить доступ».

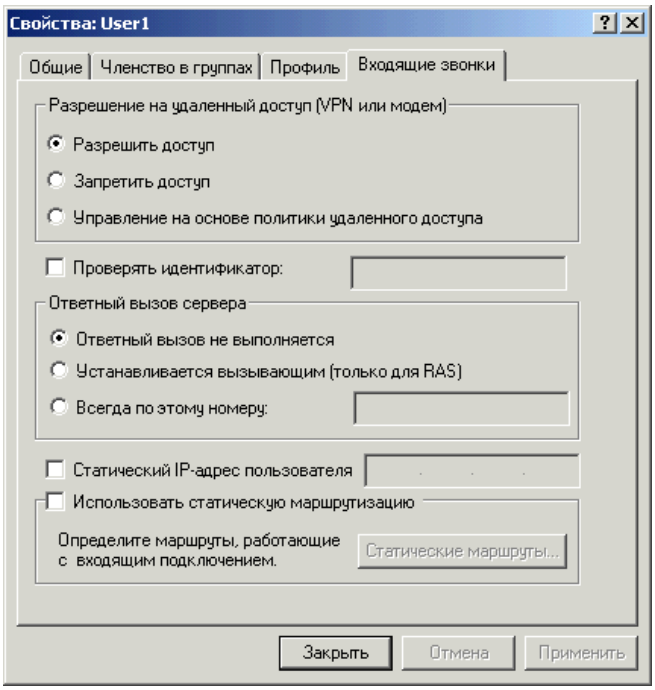


Рисунок 8 – Разрешение на удаленный доступ

Открытие доступных ресурсов

Для открытия доступа к папке зайдите в «Свойства»-> «Доступ», установите «Открыть общий доступ к этой папке».

Затем зайдите на вкладку «Безопасность». Нажмите кнопку «Добавить» (рисунок 9). В открывшемся окне «Выбор: «Пользователи» или «Группы»» нажмите «Дополнительно…», «Поиск», выберите пользователя, нажмите «ОК» (рисунок 10). Установите права для выбранного пользователя.

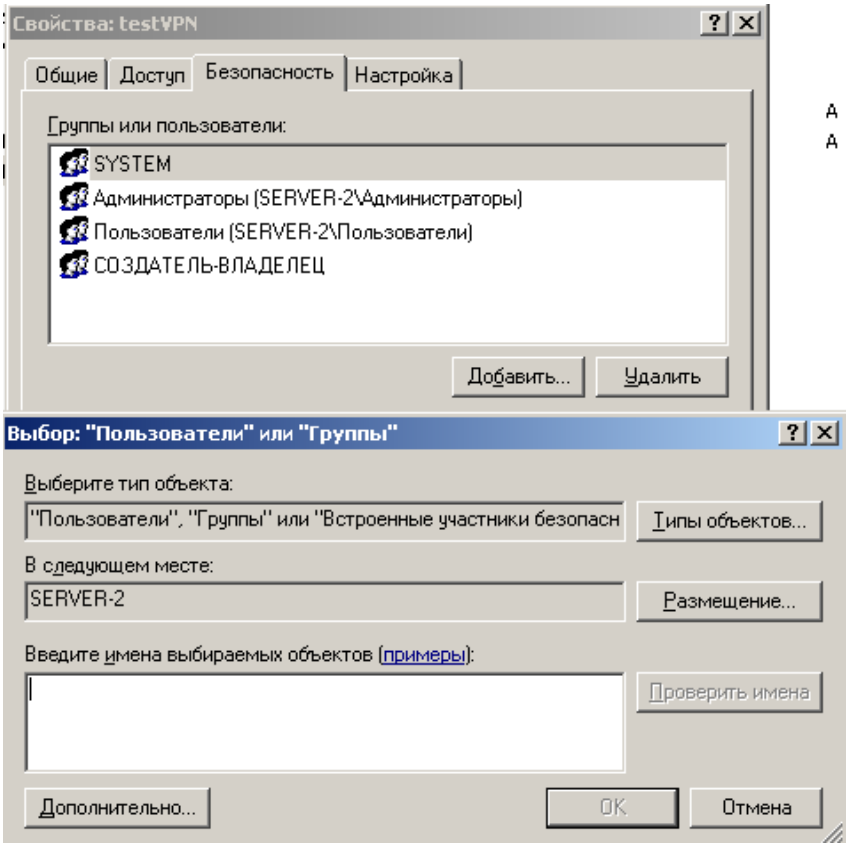


Рисунок 9 – Добавление пользователя в группу пользователей папки

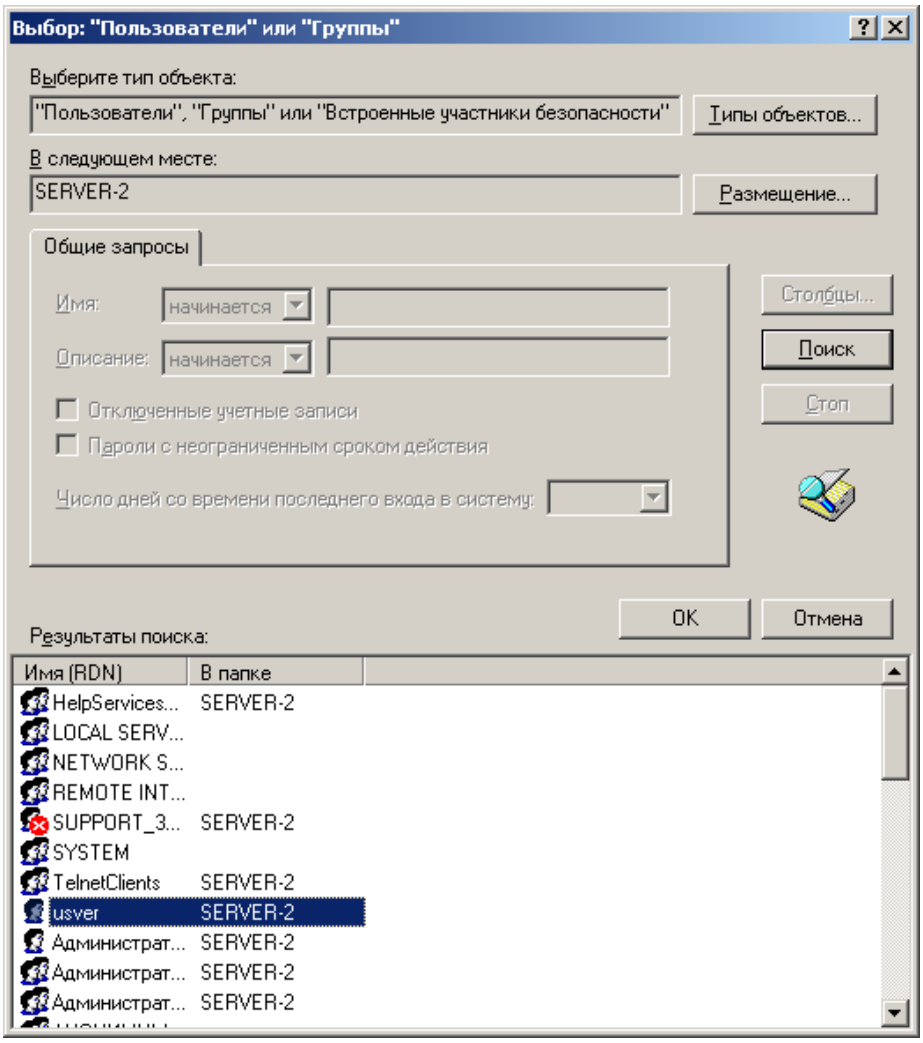
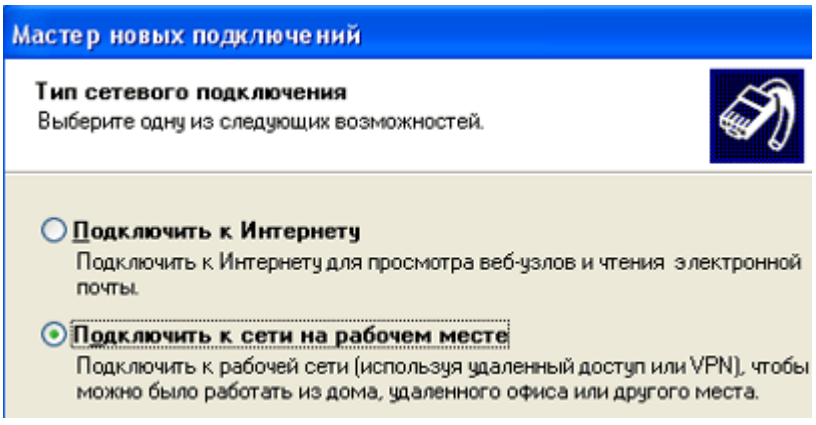


Рисунок 10 – Добавление пользователя в группу пользователей папки

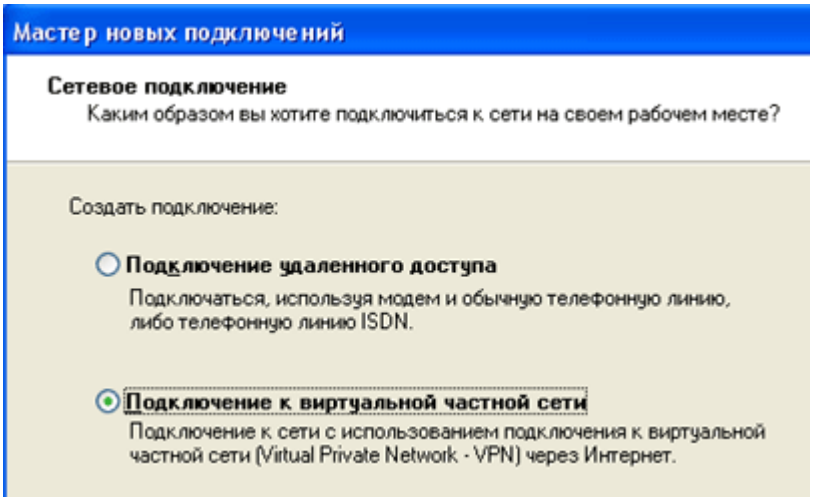
Настройка VPN подключения на клиенте

Теперь необходимо создать VPN подключение на компьютере клиента.

Нажмите кнопку «Пуск», выберите пункт «Настройка» и затем «Панель управления». В окне «Панель управления» выберите иконку «Сетевые подключения». Выберите пункт «Создание нового подключения».

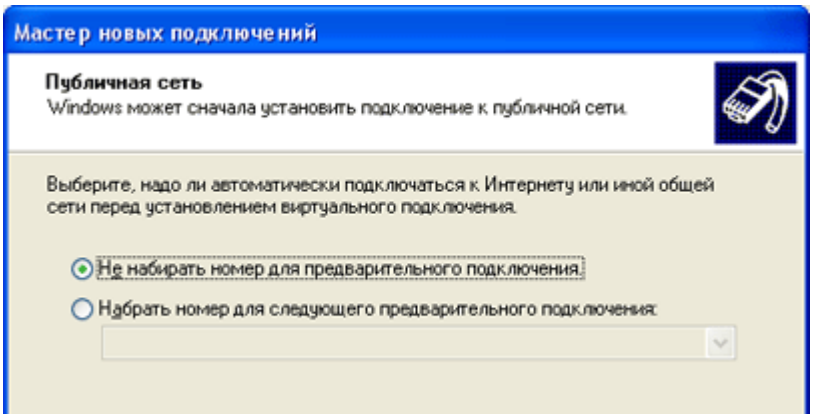


В «Мастере новых подключений» выберите тип сетевого подключения «Подключить к сети на рабочем месте».

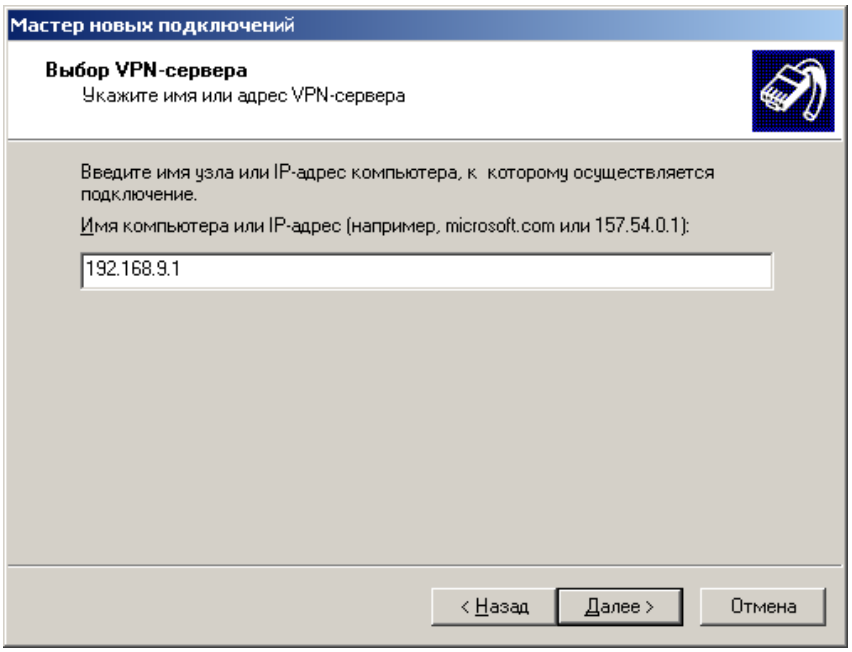


Затем создайте «Подключение к виртуальной частной сети». Нажмите кнопку «Далее»

В окне «Имя подключения» введите «Any_name». Нажмите кнопку «Далее».



Затем может появиться окно «Публичная сеть», в котором выберите пункт «Не набирать номер для предварительного подключения». Нажмите кнопку «Далее».



В окне Выбор VPN-сервера введите **имя или IP-адрес VPN сервера** Нажмите кнопку «Далее».

В окне «Завершение работы мастера новых подключений» установите галку «Добавить ярлык на рабочий стол». Нажмите кнопку «Готово».

В окне «Сеть и удаленный доступ» теперь появилась иконка «Any_name». Кликните на ней правой кнопкой мыши. Выберите пункт «Свойства». В открывшемся окне перейдите на закладку «Сеть» и в списке используемых этим подключением компонентов уберите галочки напротив пунктов «Клиент для сетей Microsoft» и «Служба доступа к файлам и принтерам сетей Microsoft». Нажмите кнопку «Параметры». В окне «Параметры PPP» установите галочки напротив всех пунктов кроме пункта «Согласовывать многоканальное подключение для одноканальных подключений».

Перейдите в закладку «Безопасность». Уберите галочки напротив пункта «Требуется шифрование данных (иначе отключаться)». Нажмите кнопку «OK».

Теперь все готово для подключения. Щелкните два раза на иконке «Any_name», введите имя пользователя и пароль по карте регистрации и нажмите кнопку «Подключиться».

Практическая часть

Содержание задания

В рамках задания требуется настроить сервер с ОС Windows в качестве VPN-сервера. Проверить правильность функционирования путем настройки на клиенте службы VPN и открытия доступа к папке. По результатам работы составить отчет.

Порядок выполнения работы

1 Ознакомиться с теоретической частью.

2 Настроить сервер Windows 2003 в качестве VPN-сервера.

3 Проверить работу VPN-сервера (настроить на Windows XP VPN-клиент).

4 Открыть папку для полного доступа через VPN соединение на сервере.

5 Составить отчёт о проделанной работе.

6 Показать выполненную работу и отчёт преподавателю.

Содержание отчёта

1 Титульный лист.

2 Цель работы.

3 Краткие теоретические сведения.

4 Основные и промежуточные результаты по каждому пункту хода выполнения работы.

5 Описание проверок функционирования служб со скриншотами результатов.

6 Выводы о проделанной работе.

Защита работ проводится индивидуально.