Основу современных корпоративных сетей составляет стек протоколов TCP/IP. Поэтому в данном курсе этому стеку посвящена отдельная глава. Однако во многих сетях со старых времен остались другие сетевые протоколы. Наиболее часто используемые среди них — *NetBEUI*, IPX/SPX.

Основная инфраструктурная сетевая служба — это служба разрешения имен DNS, которая также составляет основу инфраструктуры современных сетей. Кроме этой службы, очень важную роль в сетевой инфраструктуре играет также служба DHCP, предназначенная для автоматизации управления конфигурацией протокола TCP/IP сетевых узлов.

Служба WINS, предназначенная для разрешения имен узлов в пространстве имен NetBIOS, сейчас играет все меньшую роль в сетевой корпоративной инфраструктуре, но по-прежнему используется достаточно широко.

Служба маршрутизации и удаленного доступа RRAS предоставляет возможность доступа в корпоративную сеть мобильным пользователям через различные средства коммуникаций — коммутируемые телефонные линии, сети Frame Relay и X.25, создание защищенных виртуальных частных сетей при доступе через публичные сети, а также выполняет функцию маршрутизации сетевых пакетов по протоколам TCP/IP и IPX/SPX в сетях, состоящих из множества подсетей.

**10.1 Обзор сетевых протоколов NetBEUI, IPX/SPX; служб DHCP, WINS, RRAS**

**Сетевые протоколы IPX/SPX, NetBEUI**

Существует достаточно много стеков протоколов, широко применяемых в сетях. Это и стеки, являющиеся международными и национальными стандартами, и фирменные стеки, получившие распространение благодаря распространенности оборудования той или иной фирмы. Примерами популярных стеков протоколов могут служить: стек IPX/SPX фирмы Novell, стек TCP/IP, используемый в сети Internet и во многих сетях на основе операционной системы UNIX, стек OSI международной организации по стандартизации и некоторые другие.

**Протокол NetBEUI**

Протокол *NetBEUI*( *NetBIOS Extended User Interface* ) ведет свою историю от сетевого программного интерфейса *NetBIOS* (*Network Basic Input/Output System* ), появившегося в 1984 году как сетевое расширение стандартных функций базовой системы ввода/вывода (BIOS) IBM PC для сетевой программы PC Network фирмы IBM.

Протокол *NetBEUI* разрабатывался как эффективный протокол, потребляющий немного ресурсов, для использования в сетях, насчитывающих не более 200 рабочих станций. Этот протокол содержит много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням модели OSI, однако с его помощью невозможна маршрутизация пакетов. Это ограничивает применение протокола *NetBEUI* локальными сетями, не разделенными на подсети, и делает невозможным его использование в *составных сетях*. Некоторые ограничения *NetBEUI* снимаются реализацией этого протокола NBF (*NetBEUI* Frame), которая включена в операционную систему Microsoft Windows NT.

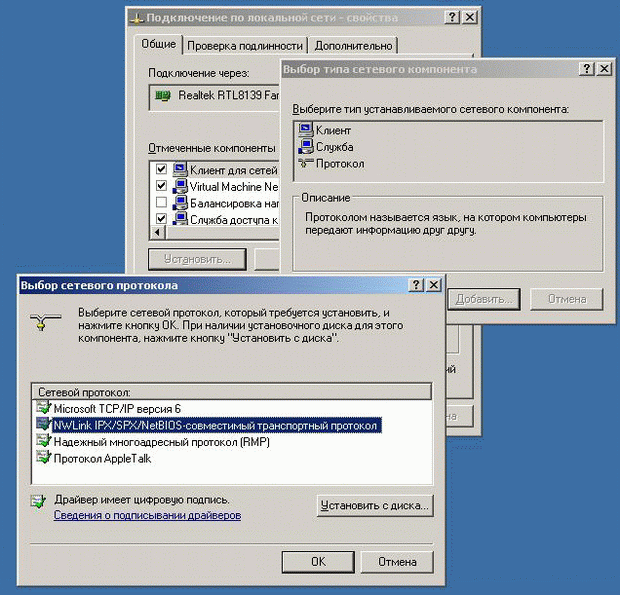
В настоящее время в операционных системах семейства Windows 2000 данный протокол уже практически не используется, а в системах Windows XP/2003 отсутствует даже возможность добавления данного протокола в *Свойствах* сетевого подключения системы (хотя, если необходима совместимость с какими-либо приложениями, унаследованными от старых систем и работающих только по протоколу *NetBEUI*, в дистрибутивах систем Windows XP/2003 имеются установочные файлы для добавления данного протокола).

**Стек протоколов IPX/SPX**

Этот стек является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов. Протоколы сетевого и сеансового уровня *Internetwork* Packet Exchange (IPX) и Sequenced Packet Exchange (SPX), которые дали название стеку, являются прямой адаптацией протоколов *XNS* фирмы Xerox, распространенных в гораздо меньшей степени, чем стек IPX/SPX. Популярность стека IPX/SPX непосредственно связана с операционной системой Novell NetWare.

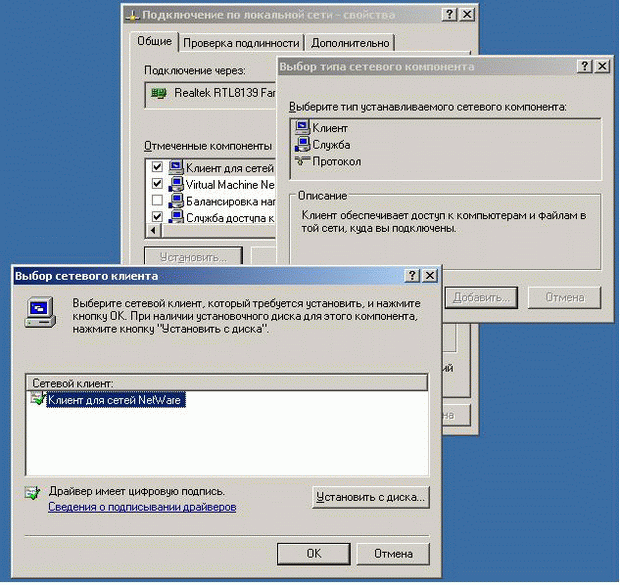
Многие особенности стека IPX/SPX обусловлены ориентацией ранних версий ОС NetWare (до версии 4.0) на работу в локальных сетях небольших размеров, состоящих из персональных компьютеров со скромными ресурсами. Понятно, что для таких компьютеров Novell нужны были протоколы, на реализацию которых требовалось бы минимальное количество оперативной памяти и которые бы быстро работали на процессорах небольшой вычислительной мощности. В результате протоколы стека IPX/SPX до недавнего времени хорошо работали в локальных сетях и не очень — в больших корпоративных сетях, так как они слишком перегружали медленные *глобальные связи* широковещательными пакетами, которые интенсивно используются несколькими протоколами этого стека (например, для установления связи между клиентами и серверами). Это обстоятельство, а также тот факт, что стек IPX/SPX является собственностью фирмы Novell, и на его реализацию нужно получать у нее лицензию, долгое время ограничивали распространенность его только сетями NetWare. С момента выпуска версии NetWare 4.0 Novell внесла и продолжает вносить в свои протоколы серьезные изменения, направленные на приспособление их для работы в корпоративных сетях. Сейчас стек IPX/SPX реализован не только в NetWare, но и в нескольких других популярных сетевых ОС, например, Microsoft Windows NT. Начиная с версии 5.0 фирма Novell в качестве основного протокола своей серверной операционной системы стала использовать протокол TCP/IP, и с тех пор практическое применение IPX/SPX стало неуклонно снижаться.

Как уже говорилось выше, стек протоколов IPX/SPX является фирменным запатентованным стеком компании Novell. Реализация данного протокола в операционных системах Microsoft называется NWLink (или IPX/SPX-совместимый протокол). Добавить данный протокол можно через *Свойства* " *Подключения по локальной сети* " (кнопка " *Установить* ", выбрать " *Протокол* ", кнопка " *Добавить* ", выбрать " *NWLink* ", кнопка " *ОК* "; рис. 10.1).



**Рис. 10.1.**

Для того, чтобы из сети под управлением систем семейства Windows получить доступ в сеть под управлением служб каталогов Novell, кроме NWLink, необходимо установить также клиента сетей Novell ( *Свойства* " *Подключения по локальной сети* ", кнопка " *Установить* ", выбрать " *Клиент* ", кнопка " *Добавить* ", выбрать "*Клиент для сетей NetWare* ", кнопка " *ОК* "; рис. 10.2).



**Рис. 10.2.**

В серверных системах Windows (до Windows 2000 включительно) имелась также служба под названием " *Шлюз для сетей NetWare* ", позволявшая клиентам сетей Microsoft без установки клиента сетей NetWare получать доступ к ресурсам серверов под управлением Novell NetWare (через шлюз, установленный на сервере Windows NT/2000). В системе Windows 2003 служба шлюза отсутствует.

**Служба DHCP**

Служба *DHCP* ( *Dynamic Host Configuration Protocol* ) — это одна из служб поддержки протокола TCP/IP, разработанная для упрощения администрирования IP-сети за счет использования специально настроенного сервера для централизованного управления IP-адресами и другими параметрами протокола TCP/IP, необходимыми сетевым узлам. Сервер DHCP избавляет сетевого администратора от необходимости ручного выполнения таких операций, как:

* автоматическое назначение сетевым узлам IP-адресов и прочих параметров протокола TCP/IP (например, маска подсети, адрес основного шлюза подсети, адреса серверов DNS и WINS);
* недопущение дублирования IP-адресов, назначаемых различным узлам сети;
* освобождение IP-адресов узлов, удаленных из сети;
* ведение централизованной БД выданных IP-адресов.

Особенности службы DHCP в системах семейства Windows Server:

* **Интеграция с DNS** — DHCP-серверы могут осуществлять динамическую регистрацию выдаваемых IP-адресов и FQDN-имен сетевых узлов в базе данных DNS-сервера (это особенно актуально для сетевых клиентов, которые не поддерживают динамическую регистрацию на сервере DNS, например, Windows 95/98/NT4);
* **Авторизация сервера DHCP в Active Directory** — если сетевой администратор установит службу DHCP на сервере Windows 2000/2003, то сервер не будет функционировать, пока не будет авторизован в AD (это обеспечивает защиту от установки несанкционированных DHCP-серверов);
* **Резервное копирование базы данных DHCP** — Созданная резервная копия может использоваться впоследствии для восстановления работоспособности DHCP-сервера.

Определим основные термины, относящиеся к службе DHCP

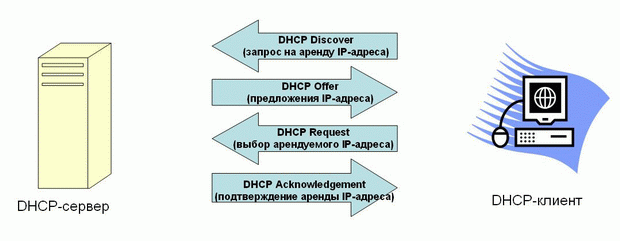
* **Клиент DHCP** — сетевой узел с динамическим IP-адресом, полученным от сервера DHCP;
* **Период аренды** — срок, на который клиенту предоставляется IP-адрес;
* **Область** — это полный последовательный диапазон допустимых IP-адресов в сети (чаще всего области определяют отдельную физическую подсеть, для которой предоставляются услуги DHCP);
* **Исключаемый диапазон** — это ограниченная последовательность IP-адресов в области, которая исключается из числа адресов, предлагаемых службой DHCP (исключаемые диапазоны гарантируют, что сервер не предложит ни один адрес из этих диапазонов DHCP-клиентам в сети);
* **Доступный пул адресов** в области — адреса, оставшиеся после определения области DHCP и исключаемых диапазонов (адреса из пула могут быть динамически назначены сервером DHCP-клиентам в сети);
* **Резервирование** — назначение DHCP-сервером определенному сетевому узлу постоянного IP-адреса (резервирования гарантируют, что указанный сетевой узел будет всегда использовать один и тот же IP-адрес).

Рассмотрим технологию предоставления IP-адресов DHCP-сервером DHCP-клиентам

При загрузке компьютера, настроенного на *автоматическое получение IP-адреса*, или при смене статической настройки IP-конфигурации на динамическую, а также при обновлении IP-конфигурации сетевого узла происходят следующие действия:

1. компьютер посылает широковещательный *запрос на аренду IP-адреса* (точнее, *на обнаружение доступного DHCP-сервера*, *DHCP Discover* );
2. DHCP-серверы, получившие данный запрос, посылают данному сетевому узлу свои *предложения IP-адреса* ( *DHCP Offer* );
3. клиент отвечает на предложение, полученное первым, соответствующему серверу запросом на *выбор арендуемого IP-адреса* ( *DHCP Request* );
4. DHCP-сервер регистрирует в своей БД выданную IP-конфигурацию (вместе с именем компьютера и физическим адресом его сетевого адаптера) и посылает клиенту подтверждение на *аренду IP-адреса* ( *DHCP Acknowledgement* ).

Данный процесс изображен на рис. 10.3:



**Рис. 10.3.**

**Планирование серверов DHCP**

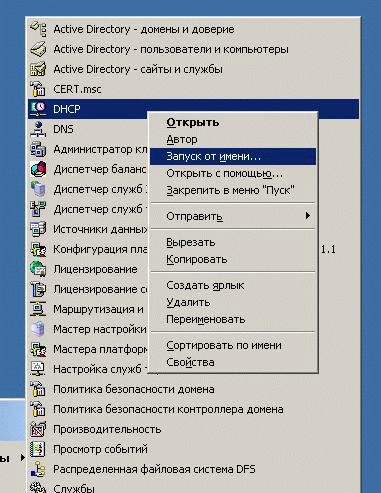
При планировании серверов DHCP необходимо учитывать в первую очередь требования производительности и отказоустойчивости (доступности) данной службы. Поэтому основные рекомендации при развертывании службы DHCP в корпоративной сети будут следующими:

* желательно в каждой IP-сети установить отдельный DHCP-сервер;
* если нет возможности установить свой сервер в каждой IP-сети, необходимо на маршрутизаторах, объединяющих IP-сети, запустить и настроить *агент ретрансляции DHCP-запросов* ( *DHCP Relay Agent* ) таким образом, чтобы он пересылал широковещательные запросы DHCP из подсети, в которой нет DHCP-сервера, на соответствующий DHCP-сервер, а на самом DHCP-сервере создать области для всех обслуживаемых IP-сетей;
* для повышения отказоустойчивости следует установить несколько серверов DHCP, при этом на каждом DHCP-сервере, кроме областей для "своих" IP-сетей, необходимо создать области для других подсетей (при этом диапазоны IP-адресов в таких резервных областях не должны пересекаться с основными областями, созданными на серверах DHCP в "своих" подсетях);
* в больших IP-сетях DHCP-серверы должны иметь мощные процессоры, достаточно большие объемы оперативной памяти и быстродействующие дисковые подсистемы, т.к. обслуживание большого количества клиентов требует интенсивной работы с базой данных DHCP-сервера.

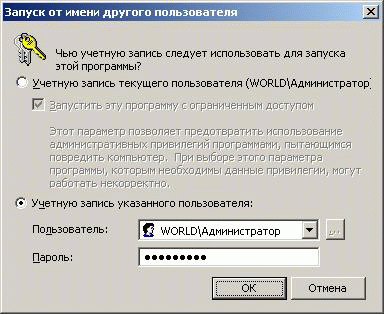
**Установка и авторизация сервера DHCP**

Установка службы DHCP выполняется так же, как и установка любой другой компоненты Windows Server: " *Пуск* " — " *Панель управления* " — " *Установки и удаление программ* " — " *Установки компонентов Windows* " — " *Сетевые службы* " — кнопка "*Состав* " — выбрать пункт " *DHCP* " — кнопки " *ОК* ", " *Далее* " и " *Готово* " (если потребуется, то указать путь к дистрибутиву системы).

Для *авторизации* сервера DHCP в БД Active Directory необходимо запустить появившуюся в разделе " *Администрирование* " консоль управления службой DHCP. Консоль обязательно следует запустить с учетной записью пользователя, являющегося членом группы " *Администраторы предприятия* ". Если ваша текущая рабочая учетная запись не входит в эту группу, то для запуска консоли с соответствующими полномочиями необходимо щелкнуть *правой кнопкой* мыши на ярлыке консоли и выбрать пункт меню " *Запуск от имени…* " (рис. 10.4), после чего указать имя пользователя, являющегося членом группы "*Администраторы предприятия* " и ввести его пароль (рис. 10.5).

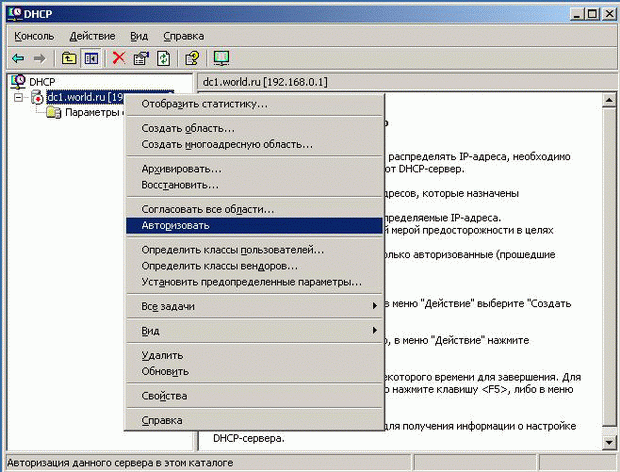


**Рис. 10.4.**



**Рис. 10.5.**

Для авторизации сервера необходимо в консоли DHCP выбрать сервер, щелкнуть на имени сервера правой кнопкой мыши и выбрать пункт меню " *Авторизовать* " (рис. 10.6). Когда авторизация будет завершена, значок у имени сервера изменится — вместо красной стрелки, направленной вниз, появится зеленая стрелка, направленная вверх.



**Рис. 10.6.**

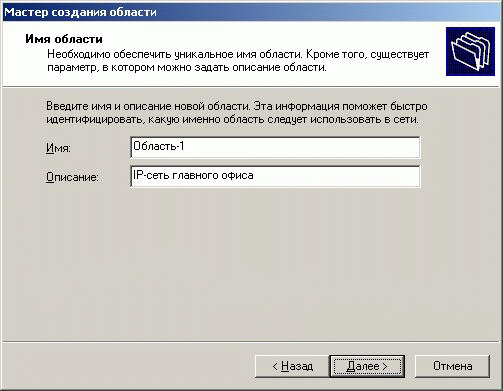
Заметим, что дальнейшие операции с DHCP-сервером не потребуют от администратора членства в группе " *Администраторы предприятия* ", достаточно быть локальным *администратором данного* сервера или членом группы " *Администраторы DHCP* ".

**Настройка параметров DHCP-сервера**

**Создание области и настройка ее параметров**

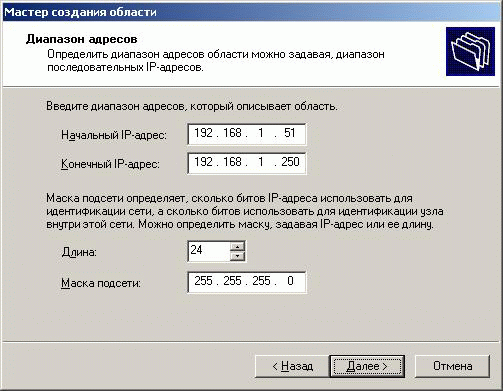
Создать область можно, щелкнув правой кнопкой мыши на имени сервера и выбрав пункт меню " *Создать область* " (или выбрав аналогичный пункт в меню "*Действие* " консоли DHCP). Консоль запустит " *Мастер создания области* ", который позволяет по шагам определить все необходимые параметры:

1. Имя и описание области. В больших сетях *именование областей* и задание их краткого описания облегчает работу администратора за счет более наглядного отображения в консоли всех созданных областей (рис. 10.7).



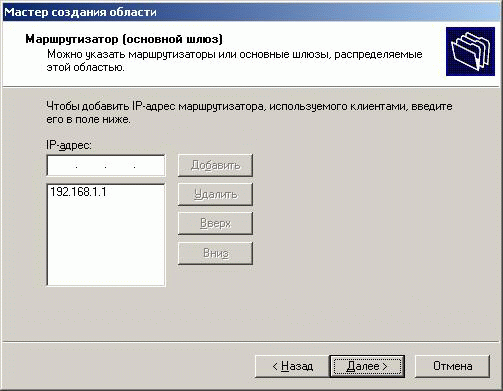
**Рис. 10.7.**

1. Определение диапазона IP-адресов и маски подсети (рис. 10.8):



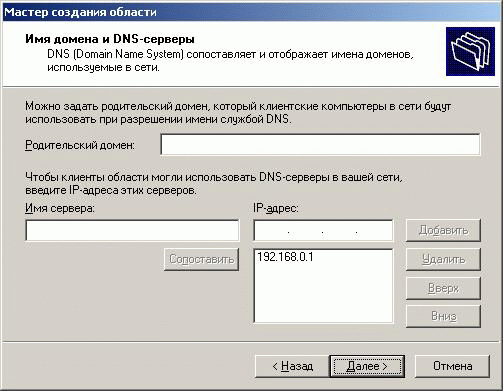
**Рис. 10.8.**

1. Добавление исключений. На данном шаге задаются диапазоны IP-адресов, который будут исключены из процесса выдачи адресов клиентам.
2. Срок действия аренды. Стандартный срок действия — 8 дней. Если в вашей сети редко происходят изменения (добавление или удаление сетевых узлов, перемещение сетевых узлов из одной подсети в другую), то срок действия можно увеличить, это сократит количество запросов на обновление аренды. Если же ваша сеть более динамичная, то срок аренды можно сократить, это позволит быстрее возвращать в пул свободных те IP-адреса, которые принадлежали компьютерам, уже удаленным из данной подсети.
3. Далее мастер предложит настроить параметры, специфичные для узлов IP-сети, относящихся к данной области:
   * маршрутизатор (основной шлюз; рис. 10.9);



**Рис. 10.9.**

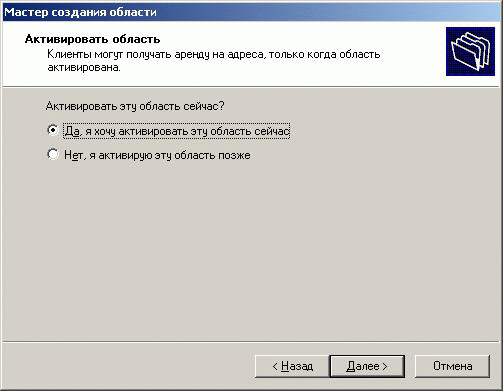
* + адрес DNS-сервера (можно назначить несколько адресов; рис. 10.10);



**Рис. 10.10.**

* + адрес WINS-сервера (аналогично серверу DNS; можно также назначить несколько адресов);

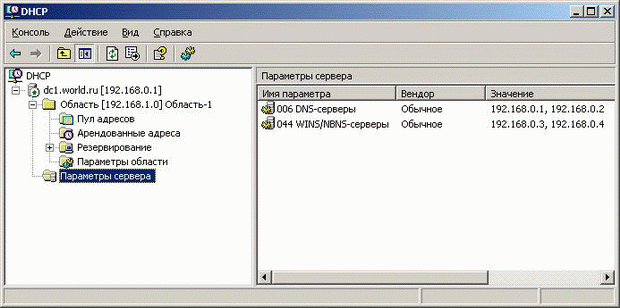
1. Запрос на активацию области. IP-адреса, заданные в созданной области, не будут выдаваться клиентам, пока область не будет активирована (рис. 10.11):



**Рис. 10.11.**

1. Нажимаем кнопку " *Готово* " и завершаем работу мастера. Область готова к использованию.

Если какие-либо параметры (например, адреса серверов DNS или WINS) являются общими для всех областей, управляемых данным DHCP-сервером, то такие параметры лучше определить не в разделе параметров каждой области, а в разделе параметров самого сервера (рис. 10.12).



**Рис. 10.12.**

**Настройка DHCP-клиентов**

Клиентом DHCP может быть практически любое сетевое устройство, настроенное на автоматическое получение IP-адреса. Из операционных систем корпорации Microsoft клиентом DHCP могут быть все системы, имеющие стек TCP/IP (вплоть до системы MS-DOS).

Клиенты посылают запрос на аренду IP-адреса при своей первой загрузке, при смене настройки получения IP-адреса со статической на динамическую, а также с помощью команд ipconfig /release (освобождение арендованного IP-адреса) иipconfig /*renew* (запрос на новую аренду).

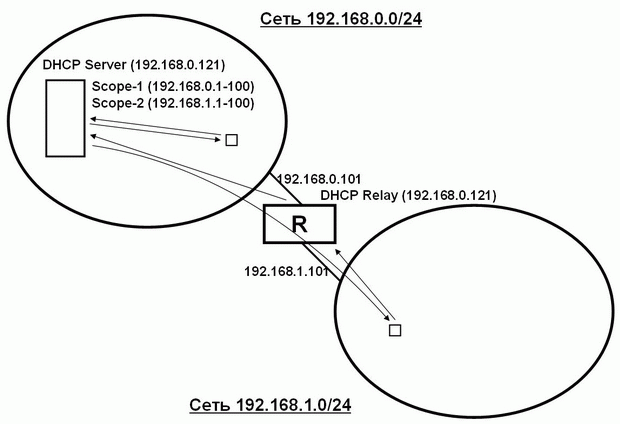
**Внимание**! Сервер DHCP обязательно должен иметь **статические IP-адреса** на всех установленных в нем сетевых адаптерах.

Авторы рекомендуют вообще на всех серверах использовать только статические IP-адреса.

**Замечание**. При отсутствии в сети DHCP-сервера клиенты, настроенные на автоматическую настройку IP-адреса будут самостоятельно назначать себе IP-адреса из подсети класса B — 169.254.0.0/16. Данная технология называется*автоматической IP-адресацией* ( *APIPA, Automatic Private IP Addressing* ) и поддерживается операционными системами Microsoft, начиная с Windows 98.

**Агент ретрансляции DHCP-запросов**

Как уже говорилось выше, один сервер DHCP может обслуживать клиентов, расположенных в различных IP-сетях. Чтобы широковещательные запросы на аренду IP-адреса достигали DHCP-сервер из любой подсети, необходимо на маршрутизаторах, объединяющих разные IP-сети в единую сеть, установить и настроить *агент ретрансляции DHCP* ( *DHCP Relay Agent* ). Пример такой конфигурации изображен на рис. 10.13.



**Рис. 10.13.**

В данном примере изображены две IP-сети класса C — 192.168.0.0/24 и 192.168.1.0/24. DHCP-сервер (имеющий IP-адрес 192.168.0.121 ) установлен в первой подсети и содержит 2 области — *Scope-1* с диапазоном адресов 192.168.0.1–192.168.0.100 и *Scope-2* с диапазоном адресов 192.168.1.1–192.168.1.100. Между двумя подсетями установлен маршрутизатор *R*, имеющий в первой подсети сетевой интерфейс с IP-адресом 192.168.0.101, а во второй подсети сетевой интерфейс с IP-адресом 192.168.1.101. На маршрутизаторе запущен агент ретрансляции DHCP-запросов, настроенный на перенаправление широковещательных DHCP-запросов на сервер с IP-адресом 192.168.0.121.

Клиенты DHCP, находящиеся в первой подсети, посылают широковещательные запросы на аренду IP-адреса, которые напрямую попадают на DHCP-сервер.

Клиенты DHCP, находящиеся во второй подсети, также посылают широковещательные запросы на аренду IP-адреса, которые не могут напрямую попасть на DHCP-сервер, т.к. маршрутизаторы не пропускают широковещательные пакеты из одной подсети в другую. Но если широковещательный пакет является запросом на аренду IP-адреса, то агент ретрансляции перехватывает данный пакет и пересылает его напрямую на DHCP-сервер. DHCP-сервер, видя от агента ретрансляции, что запрос пришел из второй подсети, выдает клиенту IP-адрес из пула адресов, заданных во второй области.

**Служба WINS**

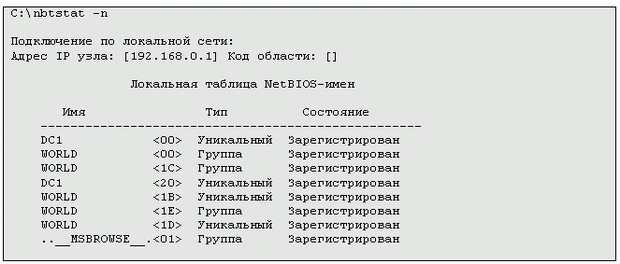
Служба *WINS* ( *Windows Internet Name Service* ) выполняет задачи, аналогичные задачам службы DNS, — динамическая регистрация имен компьютеров и других сетевых узлов и их IP-адресов в БД сервера WINS и разрешение имен компьютеров в IP-адреса. Главное отличие в том, что WINS функционирует в совершенно ином пространстве имен, т.н. пространстве имен NetBIOS, которое никак не пересекается с пространством FQDN-имен, в котором работает служба DNS. По этой причине службу WINS еще иначе называют *NetBIOS Name Service* ( *NBNS* ). До появления системы Windows 2000 сетевой программный интерфейс NetBIOS был основным сетевым интерфейсом для обмена данными между компьютерами в сетях на базе технологий Microsoft (технология SMB — предоставление *совместного доступа к файлам* и печати — работала только с помощью сетевого интерфейса NetBIOS), и поэтому служба WINS была основной службой разрешения имен компьютеров в IP-адреса. После выхода Windows 2000 служба файлов и печати может работать без NetBIOS, и основной технологией разрешения имен в IP-адреса стала служба DNS. Если в вашей сети нет операционных систем Windows 95/98/ME/NT, то вам служба WINS может вообще не потребоваться.

**Пространство имен NetBIOS**

Имена NetBIOS не образуют никакой иерархии в своем пространстве, это простой линейный список имен компьютеров, точнее работающих на компьютере служб. Имена компьютеров состоят из 15 видимых символов плюс 16-й служебный символ. Если видимых символов меньше 15, то оставшиеся символы заполняются нулями (не символ нуля, а байт, состоящий из двоичных нулей). 16-й символ соответствует службе, работающей на компьютере с данным именем.

Просмотреть список имен пространства NetBIOS, которые имеются на данном компьютере, можно с помощью команды " nbtstat –n ".

Рассмотрим пример на рис. 10.14. На рисунке изображен вывод команды " nbtstat –n " на сервере dc1.world.ru, являющийся списком NetBIOS-имен, сгенерированных данным сервером.



**Рис. 10.14.**

В угловых скобках указан шестнадцатиричный код 16-го служебного символа какого-либо имени. Например, имя *DC1* и 16-й символ " 00 " соответствуют службе "*Рабочая станция* ", которая выполняет роль *клиента* при подключении к ресурсам файлов и печати, предоставляемых *другими* *компьютерами* сети. А то же имя *DC1*и символ с кодом " 20 " соответствуют службе " *Сервер* ", которая предоставляет *ресурсы файлов и печати данного сервера* для других компьютеров сети. ИмяWORLD соответствует либо Net-BIOS-имени домена world.ru (вспомните установку *первого* контроллера домена), либо имени т.н. сетевой *рабочей группы*, отображаемой в *Сетевом окружении* любого Windows-компьютера.

Имя " ..\_\_MSBROWSE\_\_." говорит о том, что данный компьютер является *Обозревателем сетевого окружения* по протоколу TCP/IP. Т.е. если на каком-либо компьютере с системой Windows открыть " *Сетевое окружение* ", то данный компьютер будет запрашивать *список компьютеров*, сгруппированных в сетевой рабочей группе WORLD, именно с сервера DC1.

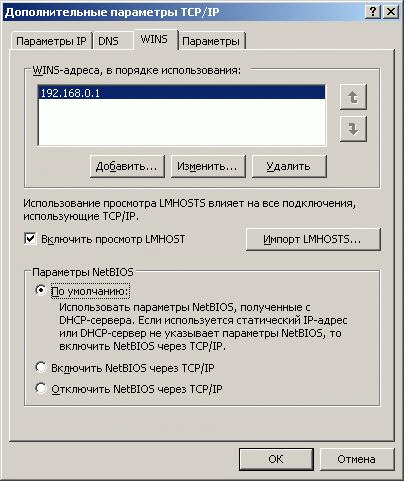
Все эти имена, перечисленные в данной таблице, будут автоматически регистрироваться в базе данных сервера WINS после того, как данный сервер будет установлен в сети и данный компьютер станет клиентом сервера WINS.

**Установка службы WINS**

Установка службы WINS выполняется по той же схеме, что и установка службы DHCP: " *Пуск* " — " *Панель управления* " — " *Установки и удаление программ* " — "*Установки компонентов Windows* " — " *Сетевые службы* " — кнопка " *Состав* " — выбрать пункт " *WINS* " — кнопки " *ОК* ", " *Далее* " и " *Готово* " (если потребуется, то указать путь к дистрибутиву системы).

**Настройка клиента WINS**

Для настройки сетевых компьютеров для использования ими сервера WINS необходимо в *Свойствах* протокола TCP/IP на закладке " *WINS* " указать IP-адреса используемых в сети WINS-серверов (для узлов со статическими IP-адресами; рис. 10.15) или добавить необходимые параметры в свойствах соответствующей области сервера DHCP (для узлов с динамическими IP-адресами).

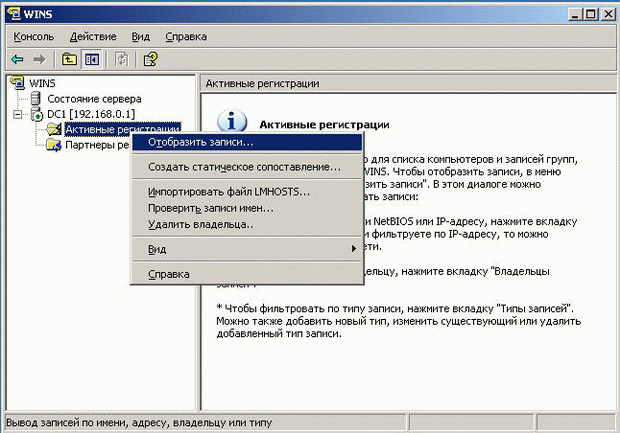


**Рис. 10.15.**

Клиент после таких изменений сделает попытку автоматической регистрации своих данных на сервере WINS. Автоматическая регистрация клиента на WINS-сервере осуществляется также в процессе загрузки системы на компьютере или командой " nbtstat –RR ".

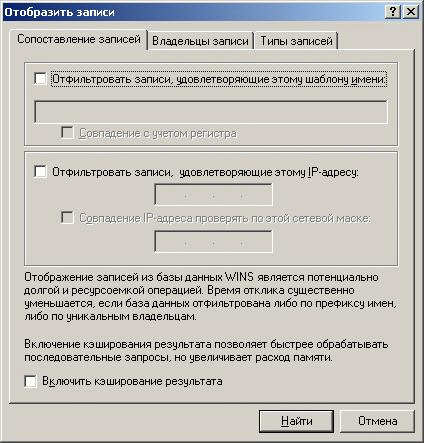
**Просмотр записей, зарегистрированных в БД сервера WINS**

Для просмотра записей, хранящихся в БД WINS-сервера, необходимо открыть консоль управления WINS, раскрыть в консоли узел, относящийся к данному серверу, щелкнуть правой кнопкой мыши на разделе " *Активные регистрации* " и выбрать " *Отобразить записи* " (рис. 10.15):



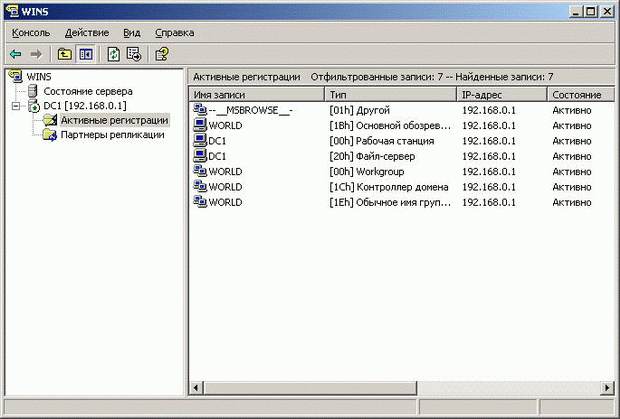
**Рис. 10.16.**

Затем нажать кнопку " *Найти* " (рис. 10.17):



**Рис. 10.17.**

На экране консоли будет таблица, изображенная на рис. 10.18:



**Рис. 10.18.**

Если система, поддерживающая NetBIOS, при этом не поддерживает автоматическую регистрацию в БД WINS-сервера, сетевой администратор может занести в БД сервера WINS *статические записи* для таких компьютеров.

**Процесс разрешения имен в пространстве NetBIOS**

Когда один компьютер пытается использовать ресурсы, предоставляемые другим компьютером через интерфейс NetBIOS поверх протокола TCP/IP, то первый компьютер, называемый клиентом, вначале должен определить IP-адрес второго компьютера, называемого сервером, по имени этого компьютера. Это может быть сделано одним из трех способов:

* широковещательный запрос;
* обращение к локальной базе данных NetBIOS-имен, хранящейся в файле LMHOSTS (этот файл хранится в той же папке, что и файл hosts, отображающий FQDN-имена);
* обращение к централизованной БД имен NetBIOS, хранящейся на сервере WINS.

В зависимости от *типа* узла NetBIOS, разрешение имен осуществляется с помощью различных комбинаций перечисленных способов:

* **b-узел** ( *broadcast node*, *широковещательный узел* ) — разрешает имена в IP-адреса посредством широковещательных сообщений (компьютер, которому нужно разрешить имя, рассылает по локальной сети широковещательное сообщение с запросом IP-адреса по имени компьютера);
* **p-узел** ( *peer node*, *узел "точка — точка"* ) — разрешает имена в IP-адреса с помощью WINS-сервера (когда клиенту нужно разрешить имя компьютера в IP-адрес, клиент отправляет серверу имя, а тот в ответ посылает адрес);
* **m-узел** ( *mixed node*, *смешанный узел* ) — комбинирует запросы b- и р-узла (WINS-клиент смешанного типа сначала пытается применить широковещательный запрос, а в случае неудачи обращается к WlNS-серверу; поскольку разрешение имени начинается с широковещательного запроса, m-узел загружает сеть широковещательным трафиком в той же степени, что и b-узел);
* **h-узел** ( *hybrid node*, *гибридный узел* ) — также комбинирует запросы b-узла и р-узла, но при этом сначала используется запрос к WINS-серверу и лишь в случае неудачи начинается рассылка широковещательного сообщения, поэтому в большинстве сетей h-узлы работают быстрее и меньше засоряют сеть широковещательными пакетами.

С точки зрения производительности, объема сетевого трафика и надежности процесса разрешения NetBIOS-имен самым эффективным является *h-узел*.

Если в свойствах протокола TCP/IP Windows-компьютера нет ссылки на WINS-сервер, то данный компьютер является b-узлом. Если в свойствах протокола TCP/IP имеется ссылка хотя бы на один WINS-сервер, то данный компьютер является h-узлом. Другие типы узлов настраиваются через реестр системы Windows.

**Репликация WINS-серверов**

В больших сетях для распределения нагрузки по регистрации и разрешению NetBIOS-имен необходимо использовать несколько серверов WINS (рекомендации Microsoft — один WINS-сервер на каждые 10000 сетевых узлов). При этом одна часть клиентов будет настроена на регистрацию и обращение для разрешения имен на один WINS-сервер, другая часть — на второй сервер и т.д. Для того, чтобы все серверы WINS имели полную информацию *обо всех* имеющихся в корпоративной сети NetBIOS-узлах, необходимо настроить репликацию баз данных серверов WINS между собой. После завершения репликации каждый сервер WINS будет иметь полный список NetBIOS-узлов всей сети. И любой клиент, регистрируясь на "ближайшем" к нему WINS-сервере, при этом может послать запрос "своему" серверу на разрешение имен NetBIOS-узлов, зарегистрированных не только на данном WINS-сервере, но и на всех остальных серверах WINS.

**Важное замечание**. Клиенты с системами Windows 2000/XP/2003 для разрешения имен *всегда* используют в *первую очередь* запросы к *серверам DNS*, даже если речь идет о пространстве имен NetBIOS.

**Служба RRAS**

Служба *RRAS* ( *Routing and Remote Access Service*, *Служба Маршрутизации и Удаленного Доступа* ) — служба системы Windows Server, позволяющая решать следующие задачи:

* подключение мобильных (или домашних) пользователей к корпоративной сети через коммутируемые телефонные линии и другие средства коммуникаций (например, сети Frame Relay, X.25);
* подключение к сети главного офиса компании удаленных офисов (через телефонные линии и сети Frame Relay, X.25);
* организация защищенных соединений (виртуальные частные сети) между мобильными пользователями, подключенными к сетям общего пользования (например, Интернет), и корпоративной сетью;
* организация защищенных соединений между офисами компании, подключенными к сетям общего пользования;
* маршрутизация сетевого трафика между различными подсетями корпоративной сети, соединенными как с помощью технологий локальных сетей, так и с помощью различных средств удаленных коммуникаций (например, по коммутируемым телефонным линиям).

Служба RRAS обладает богатым набором функций и возможностей. В рамках данного курса мы рассмотрим базовые функции и возможности данной службы, которые в первую очередь необходимо знать любому сетевому администратору.

Службы удаленного доступа, реализованные различными производителями, используют два основных коммуникационных протокола, которые образуют уровень, промежуточный между средствами коммуникаций (коммутируемые телефонные линии, Frame Relay, X.25) и сетевыми протоколами (TCP/IP, IPX/SPX):

* протокол *SLIP* ( *Serial Line Interface Protocol* ) — достаточно старый протокол, реализованный преимущественно на серверах удаленного доступа, функционирующих в системах семейства UNIX (разработан специально для подключения пользователей к сети Интернет); системы семейства Windows поддерживают данный протокол только на клиентской части (SLIP позволяет работать только с сетевым стеком TCP/IP, требует написания специальных сценариев для подключения клиента к серверу, не позволяет создавать виртуальные частные сети);
* протокол *PPP* ( *Point-to-Point Protocol* ) — используемый повсеместно коммуникационный протокол (точнее, семейство протоколов), позволяющий пользователям прозрачно подключаться к серверу удаленного доступа, использовать различные сетевые протоколы (TCP/IP, IPX/SPX, *NetBEUI*, AplleTalk), создавать виртуальные частные сети (служба удаленного доступа серверов Windows использует именно этот коммуникационный протокол).

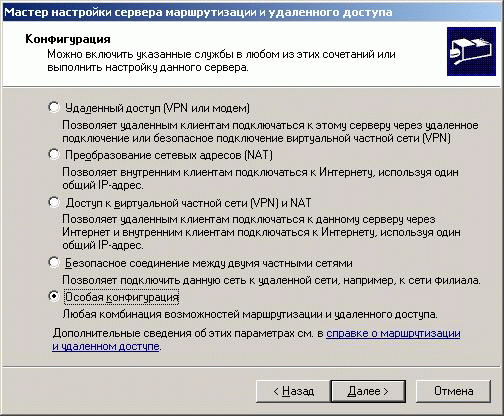
Начнем с примера, показывающего процесс установки начальной настройки службы, и обсудим терминологию, технологии, а также все необходимые нам параметры, функции и возможности данной службы.

**Установка и первоначальная настройка службы RRAS**

Службу RRAS не нужно добавлять через окно добавления *Компонент Windows*. Эта служба устанавливается при установке системы, но по умолчанию она отключена. Ее необходимо включить и настроить.

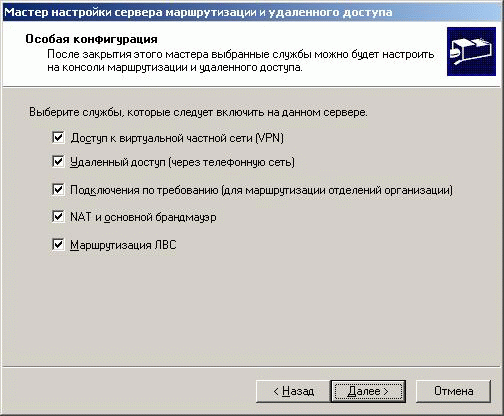
Нажмем кнопку " *Пуск* ", выберем " *Все* *программы* " — " *Администрирование* " — " *Маршрутизация и удаленный доступ* ". Откроется консоль управления службой RRAS, выберем в окне консоли имя сервера, щелкнем правой кнопкой мыши и выберем пункт меню " *Настроить и включить маршрутизацию и удаленный доступ* ". Запустится *Мастер установки сервера маршрутизации и удаленного доступа*:

1. Вначале мастер просит выбрать один из сценариев использования службы RRAS (рис. 10.19). Для нашего учебного примера выберем вариант " *Особая конфигурация* " (чтобы увидеть все возможности службы).



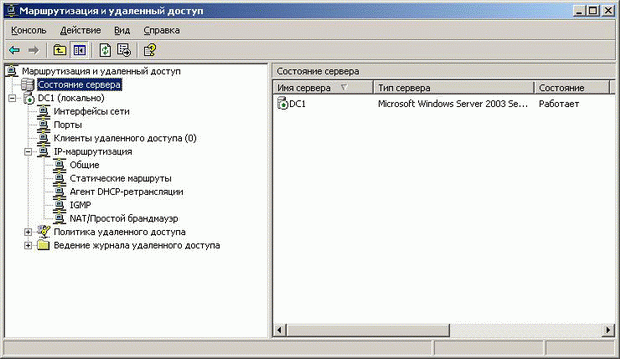
**Рис. 10.19.**

1. Далее для варианта " *Особая конфигурация* " надо выбрать нужные нам функции службы (отметим все варианты; рис. 10.20).



**Рис. 10.20.**

1. Нажмем кнопку " *Готово* ". Мастер спросит, запустить ли службу сразу после настройки, нажмем кнопку " *Да* ". Окно консоли управления службой примет вид, изображенный на рис. 10.21.



**Рис. 10.21.**

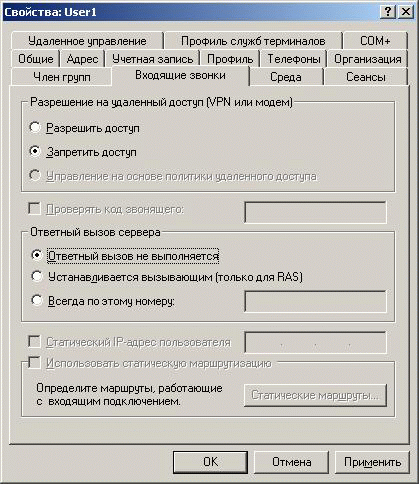
Нам для изучения службы RRAS потребуются не все установленные компоненты, поэтому мы часть компонент рассмотрим обзорно, а часть просто удалим из консоли.

**Настройка прав пользователей для подключения к серверу удаленного доступа**

При отсутствии сервера RADIUS (см. ниже) разрешения на подключение пользователя к серверам удаленного доступа определяются комбинацией *Свойств*пользователя и *Политик удаленного доступа*, настраиваемых индивидуально для каждого сервера удаленного доступа.

Если домен Active Directory работает в смешанном режиме, то разрешения на удаленный доступ определяются только в *Свойствах* пользователя на закладке "*Входящие звонки* " ( *Dial-In* ). При этом есть только два варианта — *разрешить* или *запретить* (рис. 10.22). по умолчанию для каждого нового пользователя задается запрещающее правило. Кроме разрешения/запрета можно также настроить *Обратный вызов сервера* ( *Call-back* ). Здесь имеются три варианта:

* " *Ответный вызов не выполняется* " — при подключении пользователя к серверу удаленного доступа вначале устанавливается телефонное соединение между модемом пользователя и модемом клиента, если доступ разрешен, то устанавливается сетевое соединение и пользователь получает возможность работать в сети;
* " *Устанавливается вызывающим* " — в этом варианте после установления телефонного соединения между модемами и проверки прав доступа система запросит у клиента ввести номер телефона, с которого подключается данный клиент, после этого сервер разрывает связь и уже самостоятельно производит соединение с клиентом по тому номеру телефона, который сообщил этот пользователь (данный вариант удобен для мобильных пользователей — пользователь экономит на телефонном звонке и повышается защищенность доступа, т.к. в идеале никто, кроме пользователя, не должен знать номер телефона, с которого пользователь инициировал соединение);
* " *Всегда по этому номеру* " (с указанием номера телефона) — данный вариант похож на предыдущий, только номер телефона уже введен в параметры пользователя и сервер будет перезванивать именно на данный номер (этот вариант будет интересен домашним пользователям — здесь тоже пользователь экономит на телефонном звонке и, кроме того, дополнительная защита — злоумышленнику трудно будет подключиться к серверу, даже если ему известны имя и пароль пользователя).

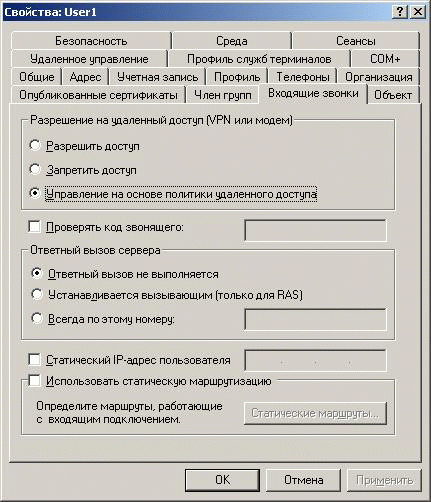


**Рис. 10.22.**

Если домен работает в основном режиме Windows 2000 или Windows 2003, то можно либо в явном виде разрешать или запрещать доступ к серверам удаленного доступа, причем ко всем сразу, либо настраивать разрешения через *Политики удаленного доступа* (о Политиках будет рассказано ниже; рис. 10.23). Заметим, что явное разрешения или явный запрет имеют более высокий приоритет, чем Политики удаленного доступа.

В основном режиме в *Свойствах* пользователя становятся доступны дополнительные параметры:

* " *Проверять код звонящего* " (Caller ID) — если оператор телефонной связи передает модему номер телефона, с которого был произведен звонок, то сервер будет разрешать подключение только при вызове с данного номера (это еще один уровень защиты от злоумышленников);
* " *Статический IP-адрес пользователя* " — при установлении соединения пользователю назначается фиксированный IP-адрес;
* " *Использовать статическую маршрутизацию* " — при установлении соединения пользователю пересылается указанный список маршрутизаторов.



**Рис. 10.23.**

**Настройка Свойств сервера**

Снова выберем в окне консоли имя сервера, щелкнем правой кнопкой мыши и выберем пункт меню " *Свойства* ".

1. 1. На закладке " *Общие* " можно изменить *сценарии использования службы*:
   * только как маршрутизатор (либо только для локальной сети, либо для локальной сети и удаленных сетей, подключенный через средства удаленных коммуникаций);
   * только как сервер удаленного доступа;
   * комбинация обоих вариантов.
2. На закладке " *Безопасность* " настраиваются используемые методы проверки подлинности (аутентификации) пользователей, подключающихся к службе удаленного доступа. Служба RRAS системы Windows Server поддерживает следующие методы аутентификации (по степени возрастания защищенности данной процедуры):
   * без проверки подлинности — при данном варианте вообще не проверяются имя и пароль пользователя, а также права доступа пользователя к службе RRAS (ни в коем случае не рекомендуем использовать на практике данный метод, т.к. открывает возможность подключения к корпоративной сети любому желающему, имеющему информацию о точке подключения, например, номера телефонов на модемном пуле);
   * протокол *PAP* ( *Password Authentication Protocol* ) — самый простой протокол, унаследованный от старых версий служб удаленного доступа (реализованных не только в системе Windows), при данном протоколе имя и пароль пользователя передаются через средства коммуникаций открытым текстом, по умолчанию данный метод аутентификации отключен;
   * протокол *SPAP* ( *Shiva Password Authentication Protocol* ) — использует протокол шифрования паролей, разработанный компанией Shiva (в прошлом — один из разработчиков средств удаленного доступа), алгоритм шифрования паролей слабее, чем в методах *CHAP* и MS *CHAP*, по умолчанию этот метод также отключен;
   * протокол *CHAP* ( *Challenge Handshake Authentication Protocol* ) — для шифрования пароля используется метод хэширования MD-5 (по сети передается значение хэш-функции пароля), данный протокол является одним из отраслевых стандартов и реализован во многих системах удаленного доступа, его рекомендуется использовать при подключении клиентов, работающих не на платформе Windows, по умолчанию также отключен;
   * протокол *MS-CHAP* ( *Microsoft Challenge Handshake Authentication Protocol* ) — версия протокола *CHAP*, реализованная корпорацией Microsoft с хэш-функцией MD-4;
   * протокол MS-*CHAP* версии 2 (Microsoft Challenge Handshake Authentication Protocol version 2) — усиленная версия MS *CHAP* (более длинный ключ шифрования при передаче пароля, вычисление нового ключа при каждом новом сеансе подключения, взаимная аутентификация пользователя и сервера удаленного доступа);
   * протокол расширенной проверки подлинности ЕАР (Extensible Authentication Protocol) — позволяет использование смарт-карт при аутентификации пользователя (требуются сертификаты как для сервера RRAS, так и для пользователей).

Клиенты удаленного доступа, имеющиеся в системах Windows, при подключении к серверу удаленного доступа всегда начинают использовать самый защищенный метод аутентификации. Если на сервере не реализован запрашиваемый протокол аутентификации, клиент пробует менее защищенный протокол. И так до тех пор, пока не будет подобран протокол, поддерживаемый обеими сторонами.

Кроме указанных протоколов можно осуществлять подключение к службе RRAS с помощью службы RADIUS (рассмотрим ниже).

На этой же закладке настраивается использование службы учета сеансов пользователей (служба учета Windows, служба учета RADIUS, либо отсутствие службы учета), по умолчанию — служба учета Windows.

И здесь же задается *общий секрет* при использовании протокола L2TP для организации *виртуальных частный сетей* ( *VPN* ). Возможность использования общего секрета для VPN на базе протокола L2TP имеется только в Windows Server 2003, в версии Windows 2000 протокол L2TP можно было использовать только при наличии сертификатов для обеих сторон частной сети.

1. На закладке " *IP* " настраивается разрешение маршрутизации IP-пакетов между компьютером клиента и корпоративной сетью (по умолчанию) и задается способ формирования пула IP-адресов, выдаваемых RRAS-сервером подключаемым к нему клиентам.

Есть два способа формирования пула — использование сервера DHCP, установленного в корпоративной сети, и задание пула IP-адресов на самом сервере удаленного доступа (при этом способе 1-й IP-адрес из пула будет назначен интерфейсу " *Внутренний* " на самом сервере RRAS, а оставшиеся в пуле адреса будут назначаться RRAS-клиентам)

1. Закладка " *PPP* ". Здесь разрешается или запрещается использование *многоканальных подключений протокола PPP* ( *multilink PPP* ). Протокол PPP позволяет использовать несколько коммуникационных каналов (например, несколько коммутируемых телефонных линий и, соответственно, одновременное использование нескольких модемов на серверной и на клиентской стороне) как одно подключение с соответствующим увеличением пропускной способности и назначением по одному IP-адресу на стороне клиента и сервера. При этом возможно использование динамического управления пропускной способностью (с помощью протоколов *BAP* / *BACP*, *Bandwidth Allocation Protocol* / *Bandwidth Allocation Control Protocol* ), которые позволяют при возрастании трафика активизировать дополнительные телефонные линии из имеющегося пула телефонных линий, а при уменьшении трафика — отключать телефонные линии.
2. Закладка " *Ведение журнала* ". На этой закладке настраивается уровень протоколирования событий, связанных с сеансами работы удаленных пользователей.

**Использование службы RADIUS**

Служба *RADIUS* ( *Remote Authentication Dial-in User Service* ) является промежуточным звеном между сервером удаленного доступа (который в данном случае называют клиентом RADIUS) и службой каталогов корпоративной сети. Сервер RADIUS позволяет решить две основные задачи:

* интеграция в единую систему серверов удаленного доступа от различных производителей;
* централизованное управление доступом в корпоративную сеть (служба RRAS в системе Windows Server настраивается*индивидуально для каждого сервера* RRAS).

Служба RADIUS работает по следующей схеме:

1. вначале устанавливается телефонное (или иное) соединение между клиентом и сервером удаленного доступа;
2. пользователь пересылает серверу RAS запрос на аутентификацию (свои имя и пароль);
3. сервер удаленного доступа (являющийся клиентом сервера RADIUS) пересылает данный запрос серверу RADIUS;
4. сервер RADIUS проверяет запрос на аутентификацию в службе каталогов (например, в службе Active Directory) и посылает в ответ RAS-серверу разрешение или запрещение данному пользователю на подключение к серверу удаленного доступа;
5. сервер удаленного доступа либо подключает пользователя к корпоративной сети, либо выдает отказ в подключении.

Реализация службы RADIUS в системе Windows Server называется службой *IAS* ( *Internet Authentication Service* ).

Раздел " *Интерфейсы сети* " консоли " *Маршрутизация и удаленный доступ* "

В данном разделе консоли перечисляются все сетевые интерфейсы, установленные на сервере (сетевые адаптеры, модемы). Напомним, что интерфейс " *Внутренний* " — это интерфейс, к которому подключаются *все* клиенты удаленного доступа, независимо от типа подключения (по коммутируемым телефонным линиям, через виртуальную частную сеть и т.д.).

Раздел " *Клиенты удаленного доступа* " консоли " *Маршрутизация и удаленный доступ* "

В данном разделе осуществляется мониторинг в реальном времени клиентов, подключившихся к серверу удаленного доступа.

Раздел " *Порты* " консоли " *Маршрутизация и удаленный доступ* "

В разделе " *Порты* " перечисляются все доступные точки подключения к службе удаленного доступа:

* параллельный порт (для прямого соединения двух компьютеров через порт LPT);
* модемы, доступные для службы удаленного доступа;
* порты, доступные для подключений с помощью виртуальных частных сетей (если администратор при настройке сервера указал, что будут использоваться виртуальные частные сети, то на сервер автоматически добавляются по 128 портов для каждого из протоколов PPTP и L2TP, в дальнейшем администратор может изменить количество портов, доступных для того или иного протокола).

Раздел " *IP-маршрутизация* " консоли " *Маршрутизация и удаленный доступ* "

В этом разделе добавляются, удаляются и настраиваются как статические маршруты, так и необходимые динамические протоколы маршрутизации:

* *Агент ретрансляции DHCP-запросов* ( *DHCP Relay Agent* ) — использование агента ретрансляции запросов DHCP подробно обсуждалось в пункте, посвященном службе DHCP, настройка данного агента производится именно в данном разделе службы RRAS;
* Протокол *IGMP* — данный протокол предназначен для маршрутизации multicast-пакетов протокола TCP/IP (данный вид пакетов и адресов используется в основном при передаче мультимедиа-информации);
* *Служба трансляции сетевых адресов* ( *NAT*, *Network Address Translation* ) — данная служба позволяет обмениваться информацией между сетями с внутренними IP-адресами и сетями с адресами, зарегистрированными в сети Интернет (упрощенный вариант прокси-сервера);
* Протокол *RIP версии 2 для IP* — протокол динамической маршрутизации IP-пакетов;
* Протокол *OSPF* ( *Open Shortest Path First* ) — также протокол динамической маршрутизации IP-пакетов, более сложный в настройке по сравнению с RIP, но более эффективный в больших сетях.

Подробное изучение протоколов маршрутизации выходит за рамки данного курса.

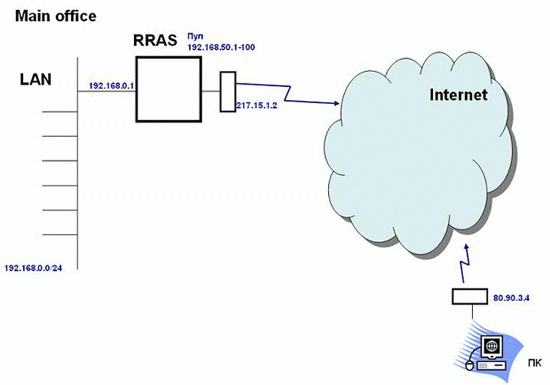
**Виртуальные частные сети**

*Виртуальные частные сети* ( *Virtual Private Networks* ) — технология создания защищенных подключений между компьютерами, подключенными к публичным сетям (например, к сети Интернет).

Рассмотрим пример на рис. 10.24. Допустим, некий мобильный пользователь желает подключиться к корпоративной сети. Он может это сделать, подключившись к корпоративному серверу удаленного доступа по коммутируемой телефонной линии. Однако, если пользователь находится в другом городе или даже другой стране, такой звонок может обойтись очень дорого. Может оказаться значительно дешевле подключиться к сети Интернет через местного Интернет-провайдера. Корпоративная сеть, в свою очередь, тоже имеет свое подключение к Интернет. В этом случае нужно решить две задачи:

* как получить доступ в корпоративную сеть (в данном примере IP-адреса корпоративной сети принадлежат к диапазону внутренних адресов и пакеты от мобильного пользователя не смогут попасть в эту сеть);
* как защитить данные, передаваемые через Интернет (все сетевые пакеты, передаваемые через Интернет, содержат информацию в открытом тексте, и грамотный злоумышленник может перехватить пакеты и извлечь из них информацию).

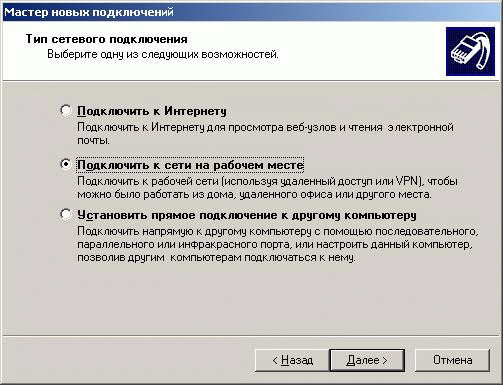
Обе эти задачи решаются созданием VPN-подключений между удаленным пользователем и сервером удаленного доступа. В данном примере пользователю необходимо создать еще одно подключение, но не через модем, а через " *Подключение к виртуальной частной сети* ". При этом в качестве "телефонного номера" выступит IP-адрес внешнего интерфейса сервера удаленного доступа.



**Рис. 10.24.**

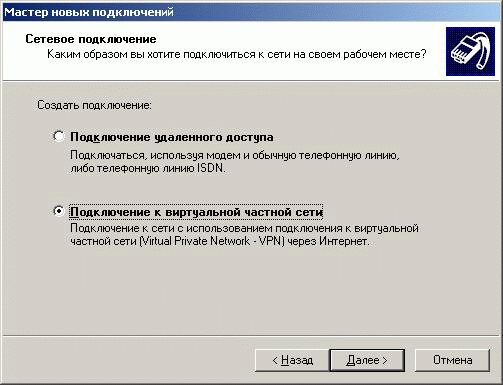
Процесс создания подключения выглядит следующим образом:

1. Запускаем *Мастер новых подключений* (кнопка " *Пуск* " — " *Панель управления* " — " *Сетевые подключения* " — " *Мастер новых подключений* ")
2. Выбираем тип сетевого подключения — " *Подключить к сети на рабочем месте* " (рис. 10.25):



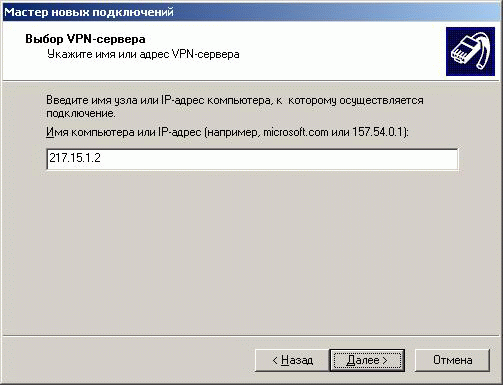
**Рис. 10.25.**

1. Выбираем способ сетевого подключения — " *Подключение к виртуальной частной сети* " (рис. 10.26):



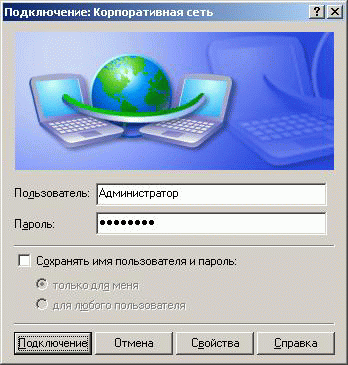
**Рис. 10.26.**

1. Задаем имя подключения.
2. Указываем VPN-сервер (имя или IP-адрес; в данном примере — *217.15.1.2* ; рис. 10.27):



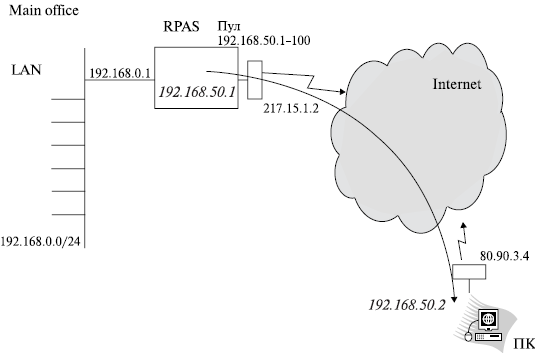
**Рис. 10.27.**

1. Определяем доступность ярлычка этого подключения (для данного пользователя или для всех пользователей).
2. Нажимаем кнопку " *Готово* ".
3. Вводим имя и пароль пользователя, нажимаем кнопку " *Подключение* " (рис. 10.28):



**Рис. 10.28.**

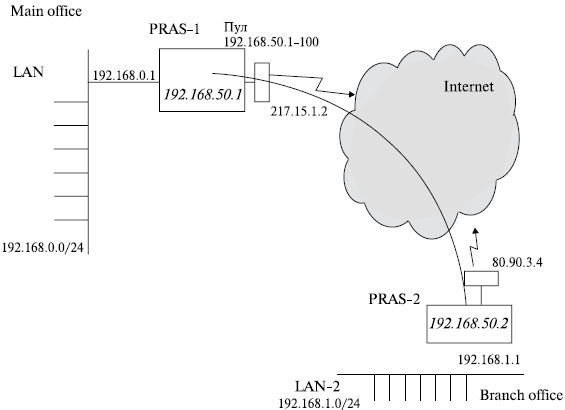
Если все настройки сделаны правильно, то будет установлено соединение с корпоративным сервером удаленного доступа. Сетевая конфигурация будет такая, как изображено на рис. 10.29:



**Рис. 10.29.**

Между ПК мобильного пользователя и сервером удаленного доступа будет установлен защищенный "виртуальный" канал, клиентский ПК получит IP-адрес из пула адресов сервера RRAS (таким образом будет решена задача маршрутизации IP-пакетов между клиентом и корпоративной сетью), все пакеты, передаваемые между клиентом корпоративной сетью, будут шифроваться.

Аналогично можно создать защищенное виртуальное подключение между двумя офисами корпоративной сети, подключенными к различным Интернет-провайдерам (рис. 10.30):



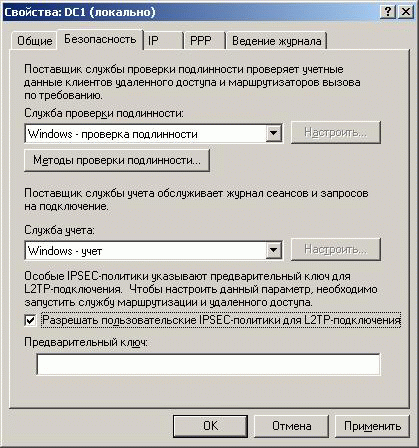
**Рис. 10.30.**

**Технологии виртуальных частных сетей**

Для создания виртуальных частных сетей в системах семейства Windows используются два различных протокола — *PPTP*разработки корпорации Microsoft ( *Point-to-Point Tunneling Protocol* ) и *L2TP*, объединивший лучшие черты протоколов PPTP и*L2F* компании Cisco ( *Level 2 Tunneling Protocol* ). Основной принцип работы обоих протоколов заключается в том, что они создают защищенный " *туннель* " между пользователем и корпоративной сетью или между двумя подсетями. Туннелирование состоит в том, что пакеты, передаваемые в защищенной сети, снабжаются специальными заголовками (у обоих протоколов свои заголовки), содержимое данных в этих пакетах шифруется (в PPTP — алгоритмом *MPPE* компании Microsoft, в L2TP — технологией IPSec), а затем пакет, предназначенный для защищенной корпоративной сети и имеющий заголовок с IP-адресами внутренней корпоративной сети, инкапсулируется в пакет, передаваемый по сети Интернет и имеющий соответствующий заголовок и IP- адреса отправителя и получателя.

Отличия между двумя протоколами следующие:

* алгоритмы шифрования (*MPPE* для PPTP, IPSec для L2TP);
* транспортная среда (PPTP работает только поверх протокола TCP/IP, L2TP может работать также поверх протоколов X.25, Frame Relay, ATM, хотя реализация L2TP в системе Windows работает только поверх TCP/IP);
* L2TP осуществляет взаимную аутентификацию обеих сторон, участвующих в создании защищенной сети, для этого используются сертификаты X.509 или *общий секрет* ( *preshared key* ). Общий секрет ( *предварительный ключ* ) реализован начиная с версии Windows 2003, устанавливается в *Свойствах* службы RRAS на закладке " *Безопасность* " (рис. 10.31).



**Рис. 10.31.**

**Политики удаленного доступа**

Как уже говорилось выше, в основном режиме домена Windows 2000/2003 разрешениями на подключения к службе удаленного доступа можно управлять с помощью*политик удаленного доступа*. Напомним, что политики удаленного доступа применяются к учетной записи пользователя при его попытке подключиться к службе удаленного доступа *только в том случае*, если в *Свойствах* этой учетной записи указано " *Управление на основе политики удаленного доступа* ". Если в явном виде указано разрешение или запрет подключения, то политики не проверяются.

Каждая политика состоит из трех компонент:

* *Условия* ( *Conditions* ) — определяются условия подключения пользователя (в сетях на базе MS Windows Server наиболее интересные условия — *день недели и время*, а также *членство в определенной группе* );
* *Профиль* ( *Profile* ) — определяются некие параметры подключения (например, тип аутентификации или вид коммуникаций);
* *Разрешения* ( *Permissions* ) — разрешить или запретить подключение.

В начале проверки политики всегда проверяются условия — если ни одно из условий не совпадает с параметрами учетной записи пользователя, то происходит переход к следующей политике. Если условия совпали, то проверяются параметры профиля подключения, если параметры политики и пользователя не совпадают, то также происходит переход к следующей политике. Если же параметры профиля совпали и данная политика разрешает подключение, то пользователю выдается разрешение на подключение к серверу удаленного доступа. Если же политика запрещает подключение, то пользователю выдается отказ на подключение к серверу.

**Резюме**

Данный раздел посвящен ознакомлению с наиболее часто используемыми, кроме TCP/IP, сетевыми протоколами и основными инфраструктурными сетевыми службами — DHCP, WINS, RRAS.

Служба DHCP значительно облегчает работу сетевого администратора по управлению конфигурацией протокола TCP/IP на множестве сетевых узлов (преимущественно на рабочих станциях пользователей), позволяя автоматически настраивать параметры TCP/IP на этих узлах.

Задачи сетевого администратора:

* планирование пространства IP-адресов для тех узлов, которые будут конфигурироваться автоматически службой DHCP;
* планирование установки серверов DHCP (количество серверов, их размещение, какие IP-диапазоны они будут обслуживать и т.д.);
* установка серверов DHCP, создание и настройка параметров областей;
* установка и настройка, при необходимости, агентов ретрансляции DHCP.

Служба WINS, хотя и теряет постепенно свою актуальность, еще полностью не вышла из использования в корпоративных сетях.

Задачи сетевого администратора:

* планирование установки серверов WINS;
* установка и настройка серверов WINS, установление партнеров репликации;
* настройка клиентов WINS (статическая или автоматическая через службу DHCP).

Служба RRAS необходима:

* для подключения мобильных и домашних пользователей к корпоративной сети (преимущественно через модемы по коммутируемым телефонным линиям);
* объединения в единую сеть удаленных сегментов корпоративной сети (подключенных друг к другу по коммутируемым или выделенным телефонным линиям);
* создания защищенных виртуальных частных сетей между мобильными пользователями и корпоративной сетью или сегментами корпоративной сети, подключенными к сетям общего пользования (например, к сети Интернет);
* для маршрутизации пакетов между IP-сетями корпоративной сети.

Задачи сетевого администратора:

* планирование серверов маршрутизации и удаленного доступа;
* установка и настройка серверов;
* планирование работы пользователей через службу удаленного доступа;
* определение разрешений пользователей на подключение к серверам удаленного доступа и настройка политик удаленного доступа;
* планирование и настройка маршрутизации в корпоративной сети.