МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ

А. В. ГОРДЕЕВ

АДМИНИСТРИРОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Учебное пособие

ГУАП
Санкт-Петербург
2020

УДК 004.7 : 681.384

Рецензенты:
доктор технических наук, доцент С.В. Беззатеев

Утверждено редакционно-издательским советом университета
в качестве лабораторного практикума

Гордеев А.В.

Администрирование вычислительных сетей. Учебное пособие /СПб.: ГУАП, 2020

Учебное пособие «Администрирование вычислительных сетей» предназначено для изучения одноимённой дисциплины и содержит, помимо теоретического материала и контрольных вопросов по каждой рассмотренной теме, задания (для выполнения лабораторных работ) и краткое описание основных шагов, позволяющих справиться с заданием. Данный учебный материал входит также и в дисциплину «Корпоративные сети со службой каталога», которая изучается в рамках другого направления.
Таким образом, пособие предназначено для студентов, обучающихся по направлению 02.03.03 — «Математическое обеспечение и администрирование информационных систем», по направлению 09.03.04 — «Программная инженерия», и по направлению 09.03.01 — «Информатика и вычислительная техника».

ПРЕДИСЛОВИЕ

Учебные планы подготовки бакалавров по направлениям 02.03.03 « Математическое обеспечение и администрирование информационных систем» и 09.03.04 «Программная инженерия» содержат двух семестровую дисциплину «Администрирование вычислительных сетей», которая помимо лекционного материала и лабораторного практикума включает в себя курсовую работу. Учебный план подготовки бакалавров по направлению 09.03.01 «Информатика и вычислительная техника» включает в себя дисциплину «Корпоративные сети со службой каталога», которая не имеет курсовой работы, но при этом студенты изучают ещё обязательную дисциплину «Сети ЭВМ и телекоммуникации», в которой есть курсовая работа. Поэтому в данном учебном пособии основное внимание уделяется вопросам конфигурирования и администрирования сетей типа «клиент-сервер», которые используются на предприятиях и в организациях, и основаны на технологиях корпоративного сектора.

Корпоративные сети, в отличие от обычных небольших локальных вычислительных сетей, характеризуются двумя основными факторами. Во-первых тем, что помимо технологий локальных сетей в них используются технологии и средства глобальных сетей, поскольку нужно связывать вместе порой сильно удалённые друг от друга фрагменты единой корпоративной сети. Причем некоторые части корпорации могут располагаться даже в разных странах и/или континентах и управляться своими местными администраторами, но подчиняться единому корпоративному центру. А во-вторых, такие сети объединяют очень большое количество компьютеров и их пользователей. Поэтому они должны иметь механизмы для иерархического и распределённого управления всеми объектами такой большой системы. И главным средством для этого является создание и использование единой базы данных, в которой хранятся все объекты корпоративной сети. А поскольку системы управления базами данных за рубежом называются службами каталогов (Directory Services), то для того чтобы подчеркнуть, что в дисциплине изучаются прежде всего методы и средства управления (администрирования) корпоративными сетями, она и получила такое название.

Основным стеком протоколов, на котором строятся сети корпоративного уровня, уже многие годы является стек TCP/IP. Поэтому первые три темы посвящены изучению основ этого стека. Причем упор делается на четвёртую версию этого стека, так как именно эта версия используется в Интернете и она, в отличие от шестой версии стека TCP/IP не является автоконфигурируемой. Это означает, что использовать этот стек без наличия достаточно большого объёма знаний невозможно. Остальные темы связаны с администрированием ресурсов вычислительных сетей.

В учебном пособии после краткого изложения теоретических сведений по каждой теме приводятся лабораторные работы. В первой работе изучается IP-адресация и настройки DHCP-сервера. Вторая работа связана с изучением системы доменных имен и настройкам DNS-сервера. Третья работа посвящена изучению основ маршрутизации. Четвёртая работа позволяет не только повторить первые три темы, но и наглядно увидеть как функционируют локальные сети и к чему приводят те или иные настройки вычислительной сети. В пятой работе рассматривается служба удаленного рабочего стола. Шестая работа связана с изучением дискреционного метода доступа к ресурсам.

При выполнении каждой работы необходимо делать отчёты. Все отчёты желательно создавать в программе LibreOffice Writer или OpenOffice Writer. Отчеты должны иметь титульные листы, на которых должна быть подпись студента. Отчеты распечатывать не надо! Все отчёты (файлы с отчётом) нужно именовать по правилу:

`АВС-НомерРаботы_ФамилияСтудента_НомерГруппы.odt` или `КС-НомерРаботы_ФамилияСтудента_НомерГруппы.odt`

В противном случае отчёты приниматься не будут. Автоматизированная информационная система (АИС) нашего университета позволяет загружать отчеты в виде файлов формата `ODT`.

ОСНОВНЫЕ ПОНЯТИЯ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Вычислительные сети - это системы связанных между собой специальными сетевыми технологиями различных компьютеров и другого вычислительного оборудования, устройств, систем хранения и передачи данных, и иных систем ввода и вывода данных, в том числе и специальных сетевых устройств. Принципиально важным является то, что взаимосвязь между всеми этими устройствами осуществляется с помощью специальных устройств ввода/вывода, которые могут отправлять, передавать и получать данные, которые распространяются от одного устройства к другому через так называемую сетевую среду. Данные по этой среде передаются либо в симплексном режиме, либо в полудуплексном, а иногда и в дуплексном (если это обеспечивают каналы передачи данных). То есть это прежде всего техническая система, которую могут использовать люди (пользователи сети). Поэтому для управления такой системой наиболее адекватным методом является администрирование. Как известно, этот термин означает «управлять». Причём управлять посредством приказов и команд, т. е. бюрократически, формально, а не посредством разъяснений, убеждений и воспитания. Поэтому «администрирование вычислительных сетей» - это управление работой сети, включая ее конфигурирование, хотя при этом безусловно затрагиваются и пользователи сети. Управляют вычислительными сетями и обслуживают их так называемые администраторы. При этом вопросы построения сети тоже достаточно часто относят к компетенциям администраторов.

Администрирование вычислительных сетей включает в себя выполнение достаточно большого перечня различных действий и реализуется посредством определённых методов и средств. Это конфигурирование и администрирование сетевых устройств, создание учетных записей и управление ими, создание различных ресурсов и предоставление их в общий доступ на разных условиях, создание резервных копий ресурсов и восстановление ресурсов в случае каких-либо аварий, мониторинг функционирования сети, установка и поддержка программного обеспечения, и многое другое.

Тема № 1: **IP-АДРЕСАЦИЯ**

Краткие теоретические сведения

Стандарты стека протоколов TCP/IP описываются в документах RFC (*Request For Comments*). Эти документы помимо статуса стандарта могут иметь и другие статусы. Например, предлагаемый стандарт (*Proposed Standard*), может перейти в стадию проектируемого стандарта (*Draft Standard*), а затем — в стадию завершенного стандарта (*Internet Official Protocol Standard*). Над каждой стадии рассматриваемый стандарт рецензируется, обсуждается, реализуется и тестируется. Не все используемые в Internet протоколы определены как стандарты Internet. Протокол, разработанный за рамками процесса рецензирования Internet, редко достигает широкого признания в сообществе TCP/IP. Это можно сказать, например, о протоколе NFS (*Network File System*), разработанном Sun Microsystems. NFS — это очень важный протокол TCP/IP, использующийся весьма широко, но не являющийся стандартом Internet. После того как документу присвоен номер RFC и осуществлено его издание, он не может быть изменен с сохранением прежнего номера RFC. После выполнения изменений документам присваиваются новые номера RFC. Если документу присваиваются новые номера RFC, прежние номера указываются на титульной странице. Кроме того, прежний номер RFC помечается как устаревший и классифицируется как архивный. Некоторые стандарты Internet обновлялись таким образом множество раз.

В настоящее время действуют две версии стека протоколов TCP/IP — 4 и 6 версии. Стек TCP/IP v. 4 был принят в 1981 г. и изначально был описан в RFC 791. А стек протоколов TCP/IP v. 6 был принят в 1996 г., он описан в RFC 8200. Однако несмотря на такие важные обстоятельства как диапазон возможных адресов (в стеке версии 6 он в 2^{96} раз больше!, к тому же ещё в 2014 г. был исчерпан весь диапазон IP-адресов стека TCP/IP v. 4) и автоконфигурируемость (стек версии 4, увы, не обладает таким важным свойством!) мы до сих пор вынуждены изучать четвёртую версию стека, т. к. именно она пока ещё используется в Интернете.

Итак, в стеке протоколов TCP/IP версии 4, с которой мы в настоящее время имеем дело в абсолютном большинстве случаев, IP–адрес имеет длину 32 бита. Причем этой 32-битовой сигнатурой указывается как идентификатор (номер) сети, так и идентификатор компьютера в этой сети (его часто называют *хост-номером*). Если быть более точным, то IP–адрес присваивается не компьютеру, а сетевой карте (сетевому интерфейсу). Дело в том, что компьютер может иметь несколько сетевых карт (сетевых адаптеров) и каждая карта должна иметь свой уникальный IP–адрес. Таким образом, компьютер может иметь несколько IP–адресов. Кроме этого, одна сетевая карта может иметь несколько IP–адресов, в результате чего можно говорить о нескольких виртуальных сетевых интерфейсах. Все сетевые интерфейсы (и реальные, и виртуальные) должны иметь уникальные IP–адреса.

Поскольку человеку очень трудно без ошибок записать 32-х символьную последовательность из нулей и единиц, было предложено каждый байт из такой 32-х битовой последовательности записывать в десятичной системе счисления, его называют *октетом*. А чтобы цифры (десятичные символы) одного октета не сливались с цифрами другого октета, между октетами ставят десятичную точку. Человек уже может работать с такой формой

представления IP-адресов, т. к. в этом случае он имеет дело всего с 4 числами, которые могут быть максимум трехразрядными.

Таким образом, двоичная запись 11011011000100010010000000001011 представляется в виде 219.17.32.11. Очевидно, что второй вариант представления IP–адреса удобнее для человека, хотя и он тоже кажется не очень понятным. Программное обеспечение переводит десятичную запись в двоичное представление и в дальнейшем обработка IP–адреса осуществляется в двоичном виде.

Вторая сложность восприятия IP–адреса заключается в том, что такая 32-х битовая последовательность должна нести в себе информацию и о сети, к которой мы подключаем компьютер, и об идентификаторе (хост–номере) компьютера, который он будет иметь в этой сети.

Номер IP–сети, к которой мы присоединяем компьютер, определяют старшие биты 4-х байтного IP–адреса. Оставшаяся часть IP–адреса указывает номер узла в этой сети (кроме использования термина «хост–номер» говорят еще «номер узла»). Например, для компьютера с IP–адресом 219.17.32.11 идентификатор сети (ее номер) по умолчанию будет равен 219.17.32, а хост–номер компьютера в этой сети будет равен 11. В то же время для компьютера, которому присвоили адрес 123.45.67.89, номер сети равен 123, а хост–номер компьютера описывается тремя октетами 45.67.89 (в двоичной записи мы будем иметь последовательность 001011010100001101011001, что соответствует десятичному числу 2966361). Возникает неопределенность в определении того, какие октеты нужно относить к номеру сети, а какие – к номеру узла.

Для того, чтобы упорядочить разделение всей 32-битовой последовательности на два поля, из которых первое указывает нам номер сети, а второе – номер компьютера, была введена классовая модель IP–адресов. В 1994 году была предложена бесклассовая модель IP–адресации, но знание классовой модели на сегодня является еще желательным.

Итак, существуют 5 классов IP–адресов. В каждом классе имеется свои правила интерпретации битов IP–адреса. Класс адреса определяется значением его первого октета. На рисунке 1 приведено соответствие классов адресов значениям первого октета и указано количество возможных IP–адресов каждого класса.

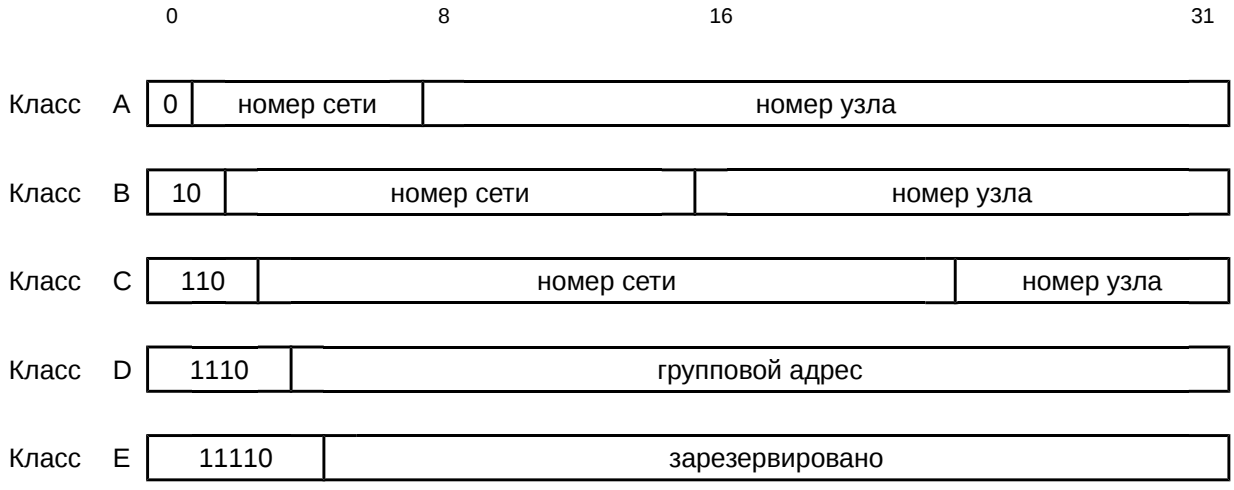

Рис.1. Структура классов IP–адресов

Из этого рисунка видно следующее:

- Если IP–адрес начинается с бита 0, то сеть относят к классу A.
- Если первые два бита IP–адреса равны 10, то сеть относится к классу B.
- Если IP–адрес начинается с последовательности 110, то это сеть класса C.
- Если IP–адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - *multicast*.
- Если IP–адрес начинается с последовательности 11110, то это адрес класса E, он был зарезервирован для будущих применений.

Итак, для сетей класса A граница между битами, которые идентифицируют сеть, и битами, которые указывают на хост-номер компьютера в этой сети, проходит между первым и вторым байтами. Адреса класса A были предназначены для использования в больших сетях общего пользования, поскольку число хостов них может достигать более 16 миллионов[1]. Количество сетей класса A невелико – всего лишь 126. Дело в том, что сеть с номером 0 запрещена и значение 0 в первом октете указывает, что сетевой интерфейс не работает по стеку TCP/IP. Значение 127 также является специальным. С другой стороны, сети класса A допускают очень большое количество номеров узлов, поскольку поле хост–номера имеет длину 24 бита. Правда, две двоичные комбинации хост–номера запрещены. Это последовательность из одних нулей в поле номера узла, поскольку она позволяет в явном виде выделить номер сети, т.е. для ссылок на всю IP–сеть в целом используется IP–адрес с нулевым номером узла. Вторая запрещенная комбинация битов – это последовательность в поле хост–номера, состоящая только из единиц, поскольку она указывает так называемый широковещательный адрес (*broadcasting*).

Количество сетей для каждого класса, возможные значения их номеров, а также возможное количество узлов в сети приведено в таблице 1.

Характеристики классов адресов Таблица 1

Класс	Диапазон значений первого октета	Возможное кол-во сетей	Возможное кол-во узлов
A	1 - 126	126	16777214
B	128-191	16382	65534
C	192-223	2097150	254
D	224-239	-	2^{28}
E	240-247	-	2^{27}

IP–адреса класса B предполагалось использовать в сетях среднего размера, например, сетях университетов и крупных компаний. Отметим, что граница между полем, идентифицирующим сеть, и полем, указывающим на хост–номер, для сетей класса B проходит между вторым и третьим байтами.

IP–адреса класса C используются в сетях с небольшим числом компьютеров. Для этих сетей граница между полем идентификатора сети и полем хоста проходит между третьим и четвертым байтами.

1 Количество узлов в сетях класса A может достигать 2^{24}-2

IP–адреса класса D используются при обращениях к группам машин. Их называют *групповыми* (*multicasting*) и они используются, например, для организации различных конференций. Такие адреса присваиваются соответствующим сетевым программным обеспечением.

IP–адреса класса E зарезервированы на будущее.

На рисунке 2 показано как надо трактовать некоторые IP–адреса, которые называют специальными.

все нули		данный узел
номер сети	все нули	данная IP-сеть
все нули	номер узла	узел в данной (локальной) IP-сети
все единицы		все узлы в данной (локальной) IP-сети
номер сети	все единицы	все узлы указанной IP-сети
127	что-нибудь (часто 1)	"Петля" (LocalHost)

Рис. 2. Специальные IP–адреса

Как показано на рис.2, в специальных IP–адресах все нули в соответствующем поле соответствуют либо данному узлу, либо данной IP–сети, а IP–адреса, состоящие из всех единиц, используются при широковещательных передачах. Для ссылок на всю IP–сеть в целом используется IP–адрес с нулевым номером узла. Особый смысл имеет IP–адрес, первый октет которого равен 127. Он используется для организации взаимодействия процессов в пределах одной машины и тестирования. Когда программа посылает данные по IP–адресу 127.0.0.1, то образуется как бы "петля" (*localhost*) и пакет возвращается в систему. Другими словами, данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Поэтому в IP–сети запрещается присваивать машинам IP–адреса, начинающиеся со 127.

Сетевая маска

Для явного указания того, где проходит граница между полем номера сети и полем номера узла применяется так называемая *сетевая маска – netmask*. Сетевая маска представляет собой 32-х битовую последовательность, в которой первое поле, соответствующее номеру сети, должно быть заполнено единицами. Второе поле сетевой маски, которое соответствует номеру узла, должно быть заполнено нулями. Очевидно, что для сетей класса A маска будет равна 11111111000000000000000000000000, что может быть записано как 255.0.0.0. Для сетей класса B сетевая маска записывается как 255.255.0.0. Наконец, сети класса C имеют маску 255.255.255.0.

Сетевая маска используется сетевым программным обеспечением для выделения номера сети из IP–адресов. Это может быть сделано поразрядным умножением IP–адреса на маску. Если инвертировать маску и опять побитно перемножить ее с IP–адресом, то мы получим номер узла. В явном виде сетевая маска наиболее востребована при разбиении сети на подсети, поскольку для классовой модели граница между полями IP–адреса четко определена рассмотренными спецификациями.

Обычно маска подсети указывается в файле стартовой конфигурации сетевого

программного обеспечения. Протоколы TCP/IP позволяют также запрашивать эту информацию по сети.

Подсети

Адресное пространство IP–сети может быть разделено на непересекающиеся подпространства – "*подсети*" (*subnet*), с каждой из которых можно работать как с обычной сетью TCP/IP. Таким образом, единая IP–сеть организации может строиться как объединение подсетей. Как правило, подсеть соответствует одной физической сети, например, одной сети Fast Ethernet. Хотя в ряде случаев IP–сеть разбивают на подсети логически, для того чтобы поместить какую-нибудь группу компьютеров в отдельную подсеть и, тем самым, отделить или совсем изолировать ее от остальных компьютеров. Дело в том, что для передачи данных из одной сети (подсети) в другую сеть (подсеть) нужно обратиться к специальному компьютеру, имеющему два сетевых интерфейса. Одним сетевым интерфейсом маршрутизатор связан с одной сетью, а другим интерфейсом – с другой. Такой компьютер называют *маршрутизатором* (*router*). Если передача данных разрешена с одного сетевого интерфейса на другой, то мы говорим «маршрутизация включена». Если же мы к одной среде передачи данных подключаем компьютеры, IP–адреса которых относятся к разным сетям (подсетям), то взаимодействие между компьютерами разных подсетей возможно только через маршрутизатор.

Тот маршрутизатор, расположенный в нашей подсети, через который мы можем обмениваться данными с компьютерами из других сетей (подсетей), называют *шлюзом* (*gateway*).

Разбиение сети на подсети осуществляется посредством того, что несколько первых битов из поля номера узла мы отводим для идентификации сети. Если мы поле номера сети увеличим на один бит, то тем самым мы разобьем нашу сеть на две подсети. Само собой, что максимально возможное количество узлов в такой подсети уменьшится. Если мы добавим к полю номера сети два бита, то получим уже четыре подсети. Добавление трех битов будет разбивать сеть уже на восемь подсетей, и так далее. Соответственно, тот байт из сетевой маски, из которого мы начинаем выделять дополнительные биты для идентификации сети, мы уже должны записывать не в виде 0, а в виде десятичного числа 128 при разбиении на две подсети. При разбиении на четыре подсети этот же октет сетевой маски должен быть записан в виде числа 192. Для случая разбиения на восемь подсетей октет получит значение 224, и так далее.

Например, IP–адрес 219.17.32.11 с маской 255.255.255.240 говорит нам о том, что мы имеем дело с нулевой подсетью сети 219.17.32.0 и узлом с номером 11, находящимся в этой подсети. Всего в этой подсети может быть до 14 узлов (2^4-2), поскольку для идентификации узлов осталось всего лишь 4 бита.

А для IP–адреса 123.45.67.89 с маской 255.255.248.0 мы должны понимать, что идентификатором сети будет значение 123.0.0.0, она разбивается на 2^{13}=8192 подсетей и наша подсеть имеет номер 1448. Номер узла для указанного IP–адреса равен 857; всего в этой подсети может быть до (2^{11}-2)=2046 узлов.

В бесклассовой модели IP–адресации маску записывают не в виде четырех октетов, а в виде целого числа, которое означает количество битов, отводимых для идентификации сети (подсети). Это целое число записывается после IP–адреса и отделяется от IP–адреса символом / (слэш). Например, только что рассмотренный IP–адрес 123.45.67.89 с маской

255.255.248.0 можно записать в виде 123.45.67.89/21. Из этой записи видно, что первые 21 бит из 32 указывает номер сети (подсети), а оставшиеся 11 битов – номер хоста.

Нелегальные (частные) IP–адреса

Среди всех возможных IP–адресов существует три диапазона (по одному в каждом классе), которые предназначены для частного использования и недействительны в Интернете (Internet). Другими словами, работать с ними можно, но только в своих локальных сетях (Intranet[2]), а не в Интернете. Правда, есть способ использования нелегальных адресов, позволяющий подключаться к Интернету и потреблять его ресурсы, но обратиться к компьютерам с нелегальными адресами из Интернета невозможно. Обеспечивается невозможность обращения из Интернета к компьютерам с нелегальными IP–адресами тем, что маршрутизаторы, получив пакет с нелегальным адресом, не пересылают его дальше, а уничтожают.

Первый диапазон частных IP–адресов находится в сетях класса A. Это сеть 10.0.0.0, которая может иметь до 2^{24}-2 узлов, и которая поэтому может быть разбита на очень большое число подсетей. Так, в нашем университете сеть 10.0.0.0 разбивается на подсети по правилу: второй и третий октеты IP–адреса должны указывать на номер аудитории. Например, в аудитории 52-08 организована своя подсеть (размером до 254 узлов), которая имеет идентификатор 10.52.8.0. А в аудитории 22-10 мы имеем подсеть 10.22.10.0. Такие подсети легко объединяются с помощью маршрутизаторов в большую университетскую сеть и, в то же время, позволяют каждой лаборатории быть относительно независимыми от других лабораторий и кафедр.

Второй диапазон нелегальных IP–адресов принадлежит сетям класса B. Он определяется значениями от 172.16.0.0 до 172.31.0.0. Очевидно, что эти сети так же могут быть разбиты на большое число подсетей, причем самыми разнообразными способами.

Наконец, третий диапазон нелегальных IP–адресов принадлежит сетям класса C. Это 256 сетей, которые первыми октетами имеют значения 192.168.X.X. Третий октет будет указывать конкретную сеть в этом диапазоне, а четвертый – номер узла. Хотя возможно организовать разбиение каждой такой сети на подсети. Например, в нашем университете третий октет мог бы соответствовать номеру кафедры или порядковому номеру подразделения. Каждая кафедра (подразделение) могут иметь в такой сети до 254 IP–адресов. Заметим, что для объединения этих подсетей нужно зарезервировать хотя бы по одному IP–адресу для маршрутизаторов, через которые можно организовать обмен данными между сетями.

Очевидно, что любая организация или ее подразделение может использовать любые нелегальные IP–адреса. Однако на практике в рамках одной организации предпочтительным является использование таких IP–адресов, которые позволяют легко объединять подсети и, в то же время, дают некоторую свободу каждому подразделению. Правилом хорошего тона является выделение первого или последнего IP–адреса в данной сети (подсети) для шлюза.

Назначение IP–адресов

Каждый администратор при назначении компьютерам и сетям IP–адресов должен в первую очередь определиться с тем, будут ли эти адреса легальными или нелегальными.

2 Термин Intranet применяют для указания таких сетей, которые работают по протоколам TCP/IP, но при этом либо не подключены к Internet-сети, либо имеют нелегальные IP–адреса и подключены к Internet-сети через Proxy-сервер.

Легальные IP–адреса получают у своего провайдера (ISP – *Internet Service Provider*). Их берут в аренду на оговоренный срок и за них нужно платить. Распределением адресного пространства занимается DDN Network Information Center (NIC), а далее провайдеры за свои услуги, в том числе и за регистрацию имен в системе доменного именования (DNS – Domain Name System) и ее поддержку берут плату. В настоящее время получить легальные IP-адреса уже невозможно, т. к. они давно все расспределены. При подключении к Интернету в большинстве случаев мы получаем от провайдера нелегальные адреса и провайдер сам обеспечивает доступ к Интернету через протокол NAT (Network Address Translation). Суть этого протокола заключается в том, что IP-адрес отправителя заменяется на другой адрес (адрес Proxy-сервера). Нелегальные IP–адреса бесплатны. Кроме того, компьютеры с нелегальными IP–адресами не видны в Интернете и это помогает их защитить.

IP–адреса являются идентификаторами, которые неудобны для человека. Их трудно запоминать, они малопонятны и, как правило, не ассоциативны. Человек предпочитает использовать символьные имена, поскольку само имя может нести некоторую полезную информацию о компьютере. Например, такой полезной информацией может быть место расположения компьютера, имя владельца или основного пользователя, роль компьютера, операционная система, и другие сведения. Поэтому необходима некоторая система трансляции символьных имен, которыми пользуются люди, в IP–адреса, которыми пользуется сетевое программное обеспечение. Соответственно при настройке сетевых интерфейсов нужно указывать не только IP–адрес с его маской, но и IP–адреса тех серверов, которые будут выполнять трансляцию символьных имен в IP–адреса. Символьные имена могут быть именами Интернета (такие имена называют *доменными*), а могут быть именами NetBIOS. Доменные имена транслируются в IP–адреса с помощью системы доменного именования (DNS – *Domain Name System*). Имена NetBIOS транслируются в IP–адреса с помощью серверов WINS – *Windows Internet Name System*.

Как известно, аппаратное обеспечение использует не IP–адреса, а MAC[3]–адреса. И для трансляции IP–адреса в MAC–адрес используется специальный протокол. Это протокол ARP – *Address Resolution Protocol*. Для обратной трансляции (сопоставление MAC-адреса сетевого адаптера его IP–адресу) имеется протокол RARP – *Reverse Address Resolution Protocol*. Поэтому для преобразования IP–адресов в аппаратные адреса и обратно нам не нужны никакие специальные серверы и при конфигурировании сетевых интерфейсов нам не нужно указывать, как будет осуществляться такая трансляция адресов.

Одно из важнейших решений, которое необходимо принять при установке и конфигурировании сети, заключается в выборе способа присвоения IP–адресов тем компьютерам, которые подключаются к сети. Этот выбор должен учитывать перспективу роста сети. Иначе в дальнейшем вам придется менять адреса. Когда к сети подключено несколько сотен машин, изменение адресов становится очень трудоемкой задачей.

Существует два способа назначения IP–адресов: *статический* и *динамический*.

Первый способ предполагает, что администратор сам, что называется «вручную», назначает IP–адреса для каждого компьютера, будь то рабочая станция, сервер или маршрутизатор. Помимо IP–адреса (и соответствующей ему маски) в настройках сетевого интерфейса, как правило, указываются IP–адрес шлюза для выхода в другие сети, IP–адреса серверов

3 MAC – Media Access Control – управление средой передачи данных. MAC–адрес – аппаратный адрес сетевого адаптера.

имен, которые будут транслировать логические имена в IP–адреса и, возможно, некоторые другие параметры. Пример окна, с которым работает администратор компьютера с Microsoft Windows Server 2003, приведен на рисунке 3. Чтобы получить это окно с настройками можно выполнить несколько различных последовательностей действий (шагов). Будем каждый шаг выделять особым шрифтом, а переход к следующему шагу – стрелкой. Например, чтобы получить это окно мы можем открыть Свойства: Сетевое окружение, далее взять Подключение по локальной сети и посмотреть Свойства: Протокол Интернета (TCP/IP). Такая последовательность может быть записана в виде Сетевое окружение → Подключение по локальной сети → Протокол Интернета (TCP/IP). Другой возможный путь – это Пуск → Панель управления → Сетевые подключения → Подключение по локальной сети → Свойства: Протокол Интернета (TCP/IP).

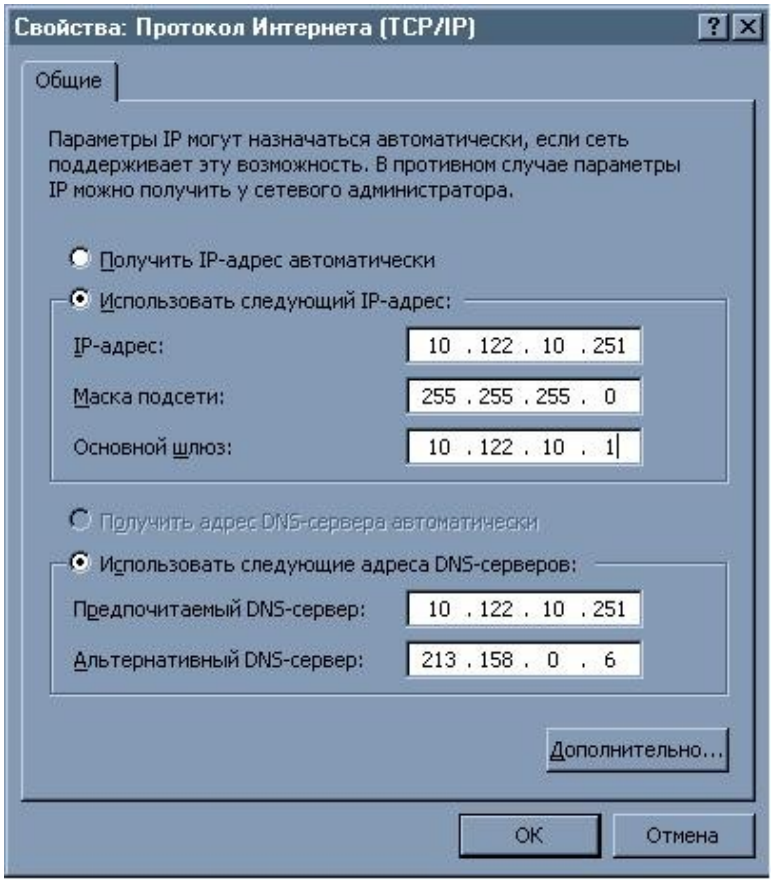

Рис. 3 Вид окна «Свойства протокола Интернета»

При необходимости уточнить эти свойства или дополнить их другими параметрами следует нажать на кнопку Дополнительно. В этом случае откроется окно, изображенное на рисунке 4. Здесь мы получим доступ к нескольким вкладкам. Их следует изучить самостоятельно, воспользовавшись системой встроенной помощи Windows (для ее вызова нажимаем на клавишу {F1}).

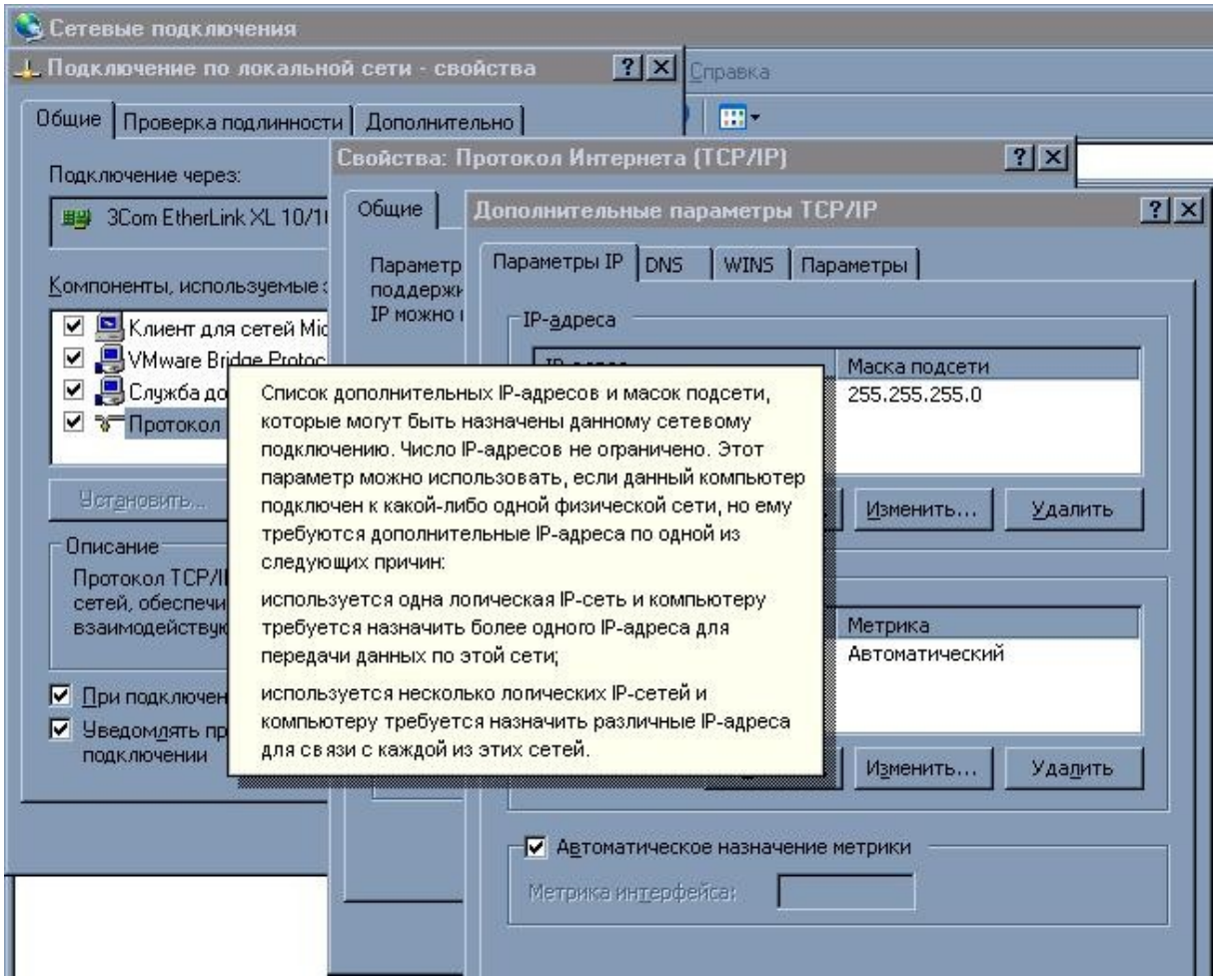

Рис. 4. Окно настройки дополнительных параметров TCP/IP

Второй способ назначения IP–адресов заключается в том, что администратор настраивает специальную службу, которая будет заниматься выдачей IP–адресов компьютерам по их запросам. Этот способ реализуется с помощью специального протокола DHCP –*Dynamic Host Configuration Protocol*.

Протокол DHCP

Протокол DHCP был разработан в 1993 г. с целью автоматического конфигурирования настройки стека TCP/IP сетевого адаптера во время загрузки системы. Можно сказать, что он появился как результат развития более раннего протокола BOOTP, который был создан в 1985 г. для поддержки бездисковых рабочих станций. Протокол BOOTP (Booting Protocol — протокол загрузки) позволял получить через сеть на рабочую UNIX-станцию код операционной системы и заодно передать этой станции IP-адрес. А в компании Microsoft решили передавать на компьютер, который загружает операционную систему с внешней памяти, только IP-адрес и некий набор дополнительных параметров, необходимых для работы по стеку протоколов TCP/IP. Это позволяет хранить все доступные IP–адреса в центральной базе данных на сервере DHCP вместе с соответствующей информацией о конфигурации, такой как маска подсети, адрес шлюза и адреса серверов имен (DNS и WINS), и некоторые другие параметры. Протокол DHCP упрощает работу системных администраторов. При этом чем больше сеть, тем выгоднее применять протокол DHCP. Без динамического назначения адресов адми-

нистратору пришлось бы настраивать сетевые интерфейсы клиентов вручную, последовательно назначая им IP–адреса. Изменения должны производиться для каждого клиента по отдельности. Чтобы избежать двойного использования, IP–адреса должны распределяться централизованно. Информация о конфигурации без протокола DHCP распределена по клиентам; в этом случае трудно получить представление о конфигурациях всех клиентов.

Рассмотрим основные понятия протокола DHCP.

- *Область DHCP* (*scope*). Под областью DHCP понимается административная группа, идентифицирующая полные последовательные диапазоны возможных IP–адресов для всех DHCP–клиентов в физической подсети. Области определяют логическую подсеть, для которой должны предоставляться услуги DHCP, и позволяют серверу задавать параметры конфигурации, выдаваемые всем DHCP–клиентам в подсети. Область должна быть определена прежде, чем DHCP–клиенты смогут использовать DHCP–сервер для динамической конфигурации TCP/IP.
- *Суперобласти* (*superscope*). Множество областей, сгруппированных в отдельный административный объект, представляет собой суперобласть. Суперобласти полезны для решения различных задач службы DHCP.
- *Пул адресов* (*address pool*). Если определена область DHCP и заданы диапазоны исключения, то оставшаяся часть адресов называется пулом доступных адресов (в пределах области). Эти адреса могут быть динамически назначены клиентам DHCP в сети.
- *Диапазоны исключения* (*exclusion range*). Диапазон исключения — ограниченная последовательность IP–адресов в пределах области, которые должны быть исключены из предоставления службой DHCP.
- *Резервирование* (*reservation*). Резервирование позволяет назначить клиенту постоянный адрес и гарантировать, что указанное устройство в подсети может всегда использовать один и тот же IP–адрес.
- *Период аренды* (*lease*). Под периодом аренды понимается отрезок времени, в течение которого клиентский компьютер может использовать выделенный IP–адрес. В момент истечения половины срока действия аренды клиент должен возобновить аренду, обратившись к серверу с повторным запросом. Следует помнить о том, что продолжительность периода аренды влияет на частоту обновления аренды (другими словами, на интенсивность обращений к серверу);
- *Опции DHCP* (*option DHCP*). Опции DHCP представляют собой дополнительные параметры настройки клиентов, которые DHCP–сервер может назначать одновременно с выделением IP–адреса. Опции могут быть определены как для каждой области отдельно, так и глобально для всех областей, размещенных на DHCP–сервере. Кроме стандартных опций, описанных в спецификации протокола DHCP, администратор может определять собственные опции.

Работа протокола DHCP базируется на классической схеме клиент–сервер. В роли клиентов выступают компьютеры сети, стремящиеся получить IP–адреса в аренду, а DHCP–серверы выполняют функции диспетчеров, которые выдают адреса, контролируют их использование и сообщают клиентам требуемые параметры конфигурации. Сервер поддерживает пул свободных адресов и, кроме того, ведет собственную регистрационную базу данных. Взаимодействие DHCP–серверов со станциями–клиентами осуществляется путем обмена сообщениями.

Для работы протокола используется протокол UDP[4] и порты 67 и 68. Клиент начинает

4 UDP – User Datagram Protocol – протокол передачи данных без установления соединения и не гарантирующий доставку пакетов.

свою работу с широковещательной посылки сообщения DHCPDISCOVERY, в котором могут указываться устраивающие его IP–адрес и срок его аренды. Если в данной подсети DHCP-сервер отсутствует, сообщение будет передано в другие подсети ретранслирующими агентами протокола (они же вернут клиенту ответные сообщения сервера). Если клиент еще не имеет IP–адреса, то в качестве IP адреса источника указывается 0.0.0.0:67, а в качестве адреса назначения указывается адрес 255.255.255.255:68 . В этой посылке клиент указывает свой MAC–адрес.

Все DHCP–серверы, получившие это сообщение, определяют: могут ли они предоставить IP–адрес для аренды. Все серверы, которые могут это сделать, высылают свои предложения аренды в сообщении DHCPOFFER и резервируют предложенный адрес. В своих ответах они сообщают свой MAC–адрес.

Далее клиент выбирает предложения аренды и посылает широковещательный пакет с сообщением DHCPREQUEST с указанием выбранного сервера. Клиент не обязан реагировать на первое же поступившее предложение. Допускается, чтобы он дождался откликов от нескольких серверов и, остановившись на одном из предложений, отправил в сеть широковещательное сообщение DHCPREQUEST. Все серверы кроме указанного освобождают условно выделенный для клиента IP–адрес. Кроме запроса на аренду IP–адреса клиент посылает список дополнительных запрашиваемых параметров, которые ему нужны для работы по стеку TCP/IP.

Сервер, которому был направлен запрос, отвечает сообщением DHCPACK в случае подтверждения аренды IP–адреса. Клиенту так же присылается запрошенный список параметров и время аренды адреса.

Если сервер не в состоянии выдать необходимые данные, то он отвечает сообщением DHCPNACK и клиент продолжает попытки получить нужные ему данные.

Получив сообщение DHCPACK, клиент обязан убедиться в уникальности IP–адреса (средствами протокола ARP) и зафиксировать суммарный срок его аренды. Последний рассчитывается как время, прошедшее между отправкой сообщения DHCPREQUEST и приемом ответного сообщения DHCPACK, плюс срок аренды, указанный в DHCPACK.

Обнаружив, что адрес уже используется другой станцией, клиент обязан отправить серверу сообщение DHCPDECLINE и не ранее чем через 10 с начать всю процедуру снова. Процесс конфигурирования возобновляется и при получении серверного сообщения DHCPNACK.

При достижении тайм-аута в процессе ожидания серверных откликов на сообщение DHCPREQUEST клиент выдает его повторно. Для досрочного прекращения аренды адреса клиент отправляет серверу сообщение DHCPRELEASE.

DHCP–сервер гарантирует, что выделенный адрес до истечения срока его аренды не будет выдан другому клиенту; при повторных обращениях сервер старается предложить клиенту IP–адрес, которым тот пользовался ранее. Со своей стороны, клиент может запросить пролонгацию срока аренды адреса либо, наоборот, досрочно отказаться от него. Протоколом предусмотрена также выдача IP–адреса в неограниченное пользование. При острой нехватке IP–адресов сервер может сократить срок аренды адреса по сравнению с запрошенным.

Описанная последовательность действий упрощается, если станция–клиент желает

повторно работать с IP–адресом, который когда-то уже был ей выделен. В этом случае первым отправляемым сообщением является DHCPREQUEST, в котором клиент указывает прежде использовавшийся адрес. В ответ он может получить сообщение DHCPACK или DHCPNACK (если адрес занят либо клиентский запрос является некорректным, например из-за перемещения клиента в другую подсеть). Обязанность проверить уникальность IP–адреса опять-таки возлагается на клиента.

По мере того как срок аренды подходит к концу, клиент может завершить работу с данным адресом, отправив на DHCP–сервер сообщение DHCPRELEASE, либо заблаговременно запросить продление срока аренды. В первом случае возвращение в сеть потребует выполнения всей процедуры инициализации заново. Во втором – станция продолжит функционировать в сети без видимого замедления работы пользовательских приложений.

Установка и настройка DHCP–сервера

В рамках лабораторного практикума мы будем изучать излагаемый здесь материал с помощью виртуальных машин, поэтому чтобы снизить нагрузку на компьютер, на котором будут запускаться виртуальные машины, предлагается использовать операционные системы, требующие как можно меньше вычислительных ресурсов. К таким системам можно отнести ныне уже не современные, но пригодные для освоения изучаемого материала Windows Server 2003 и Windows XP Professional. При желании можно использовать виртуальные машины с современными операционными системами, но понимать, что далеко не каждый компьютер может справиться с задачей запуска и работы сразу нескольких виртуальных машин.

Служба DHCP состоит из трех основных компонентов: сервера, клиента и агентов ретрансляции.

Сервер DHCP. Сервер DHCP также содержит базу данных для назначения IP–адресов и других параметров настройки. Если служба сервера DHCP установлена, то сразу после задания и активизации областей автоматически создается база данных DHCP

Клиенты DHCP. Клиентами сервера DHCP из состава Windows Server 2003 могут быть компьютеры, работающие на любой платформе.

Агенты ретрансляции DHCP. Работа протокола DHCP основана на механизмах широковещания. Маршрутизаторы обычно по умолчанию не ретранслируют широковещательные посылки, поэтому передача таких посылок выполняется агентом ретрансляции. Агент ретрансляции DHCP — это маршрутизатор, либо хост, который слушает широковещательные сообщения DHCP и переадресовывает их на заданный сервер (серверы) DHCP. Использование агентов ретрансляции избавляет от необходимости устанавливать сервер DHCP в каждом физическом сегменте сети. Агент не только обслуживает прямые локальные запросы клиента DHCP и перенаправляет их на удаленные серверы DHCP, но также возвращает ответы удаленных серверов DHCP клиентам DHCP.

Для установки службы DHCP–сервера в Windows Server 2003 можно воспользоваться процедурами установки дополнительных сетевых компонентов либо запустить мастер настройки сервера и добавить необходимую роль. Для первого варианта выполняем следующую последовательность шагов: Пуск → Настройка → Панель управления → Установка и удаление программ → Установка компонентов Windows → Networking Services → Состав → Dynamic Host Configuration Protocol (DHCP). При этом в компьютере должен быть установлен диск с дистрибутивом системы. После установки службы DHCP в меню

Administrative Tools (Администрирование) будет добавлен новый инструмент: оснастка DHCP для консоли управления Microsoft. Эта утилита используется для настройки DHCP-сервера; ее окно приведено на рисунке 5. Непосредственно после установки и должной настройки службы DHCP–сервера ее необходимо запустить. Если DHCP–сервер не сконфигурирован должным образом, то он может отдавать клиентам неправильные адреса или некорректные значения параметров, в результате чего компьютеры не смогут нормально работать в сети. В этом случае с помощью оснастки Services (Службы) следует остановить службу DHCP. В случае если DHCP–сервер подключен к нескольким сетям, необходимо отключить привязку службы к тем подключениям, которым не требуется поддержка DHCP. Компьютер, выбранный на роль DHCP–сервера, должен быть сконфигурирован со статическим IP–адресом.

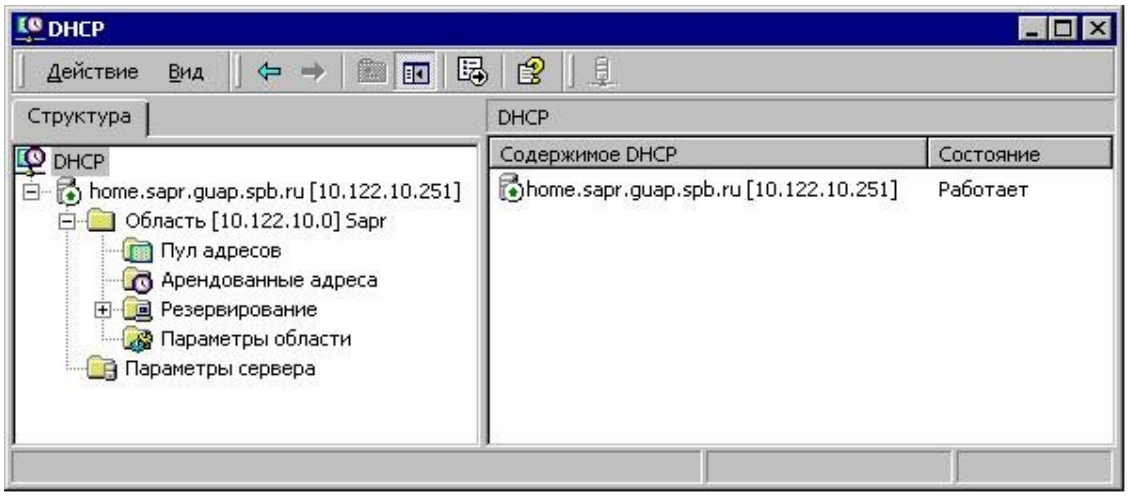

Рис.5 Окно настройки DHCP-сервера

Приступая к настройке службы DHCP, администратор должен создать отдельную область действия для каждой физической подсети. Если в сети имеется несколько DHCP–серверов, необходимо распределить имеющиеся диапазоны адресов между ними. Как правило, для каждой подсети должно быть как минимум два DHCP–сервера, способных выдать необходимый IP–адрес. Для этого имеющиеся диапазоны адресов делятся между двумя DHCP–серверами в некотором соотношении. При этом рекомендуется следующая схема. Для каждой подсети на ближайшем DHCP–сервере размещается 80 процентов имеющихся адресов. Остальные 20 процентов размещаются на одном из оставшихся DHCP–серверов. Этот сервер возьмет на себя обязанности по выдаче адресов для рассматриваемой подсети, если основной сервер выйдет из строя. Применение подобной схемы позволяет гарантировать, что ни один запрос клиента не останется без ответа.

Создание области действия

Приступим к настройке службы DHCP. Для начала определим необходимые области действия. Запустите оснастку DHCP консоли управления Microsoft, которая находится в меню Administrative Tools (Администрирование). В результирующей панели оснастки вызовите контекстное меню объекта, ассоциированного с конфигурируемым DHCP–сервером, и выберите пункт New Scope (Новая область действия). Будет запущен мастер конфигурирова-

ния области действия.

Первое окно мастера традиционно предоставляет информацию о его назначении. Поэтому можно сразу же перейти ко второму окну, в котором требуется определить имя для создаваемой области действия и дать ей краткое описание. В качестве имени можно использовать IP–адрес подсети или название подразделения, для которого предназначается создаваемое пространство IP–адресов (см. рис. 6). Это поможет вам легко ориентироваться в ситуации, когда на DHCP–сервере создано множество областей действия. В этом случае вы всегда сможете точно идентифицировать необходимую область.

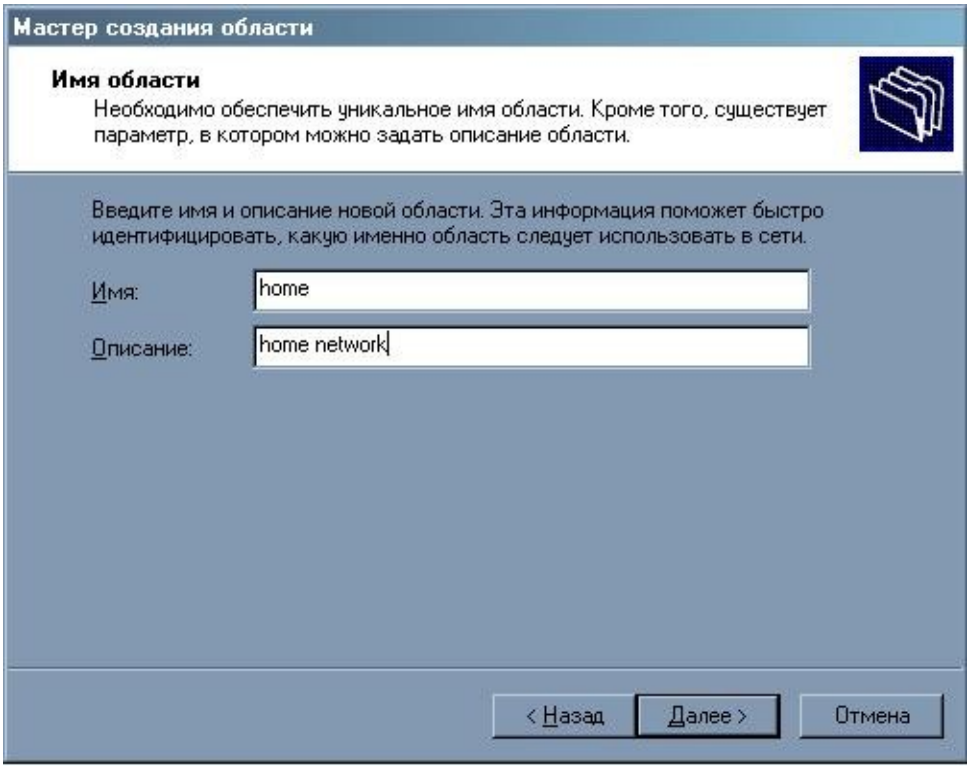

Рис. 6. Создание новой области действия DHCP–сервера

В третьем окне мастера следует определить пул IP–адресов, для которых создается область действия. Пул задается путем указания начального и конечного адреса диапазона. Потребуется также предоставить информацию о маске подсети (рис. 7).

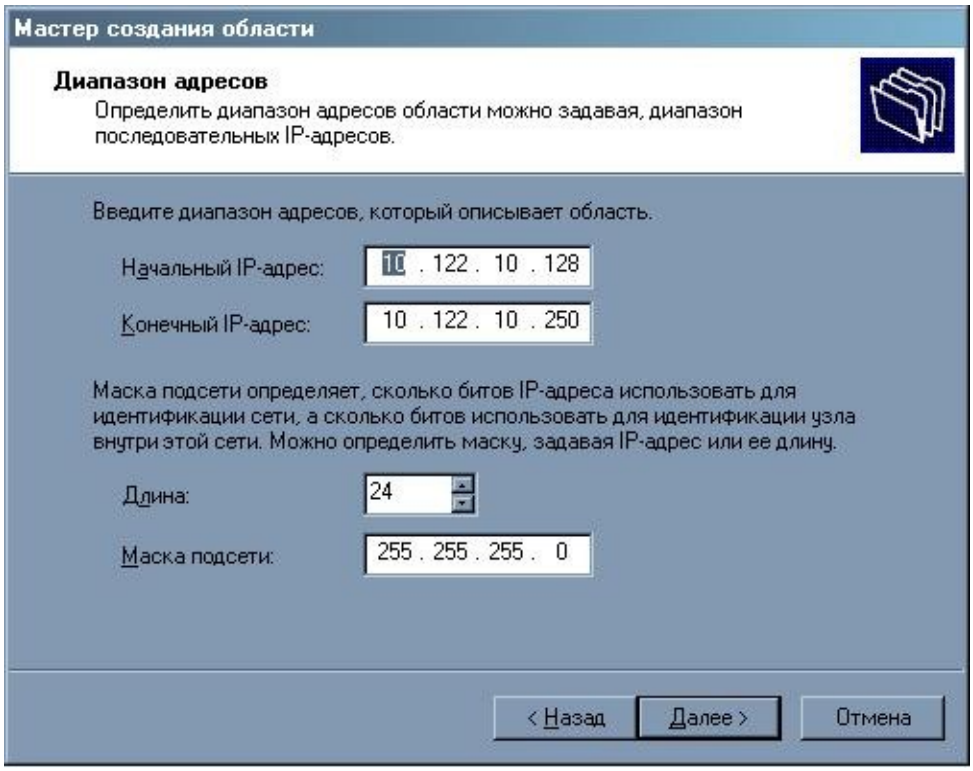

Рис. 7. Определение пула IP–адресов

В следующем окне мастера администратор может указать исключения из только что определенного диапазона IP–адресов. Для этого могут иметься различные причины. Например, в указанный пул могут войти адреса серверов, которые должны иметь статические IP–адреса. Администратор может исключать как отдельные адреса, так и целые диапазоны. Для исключения одиночного IP–адреса необходимо указать его в поле Start IP address (Начальный IP-адрес). Поле End IP address (Конечный IP адрес) необходимо оставить в этом случае пустым. После нажатия кнопки Add (Добавить) введенный адрес будет добавлен в список исключенных из диапазона адресов (см. рис. 8).

Перейдя к следующему окну мастера, необходимо определить для создаваемой области действия время аренды (*leasing*) IP–адресов. Время аренды может быть определено на уровне дней, часов и даже минут (рис. 9). Если сеть изменяется относительно редко, имеет смысл увеличивать срок аренды. Если же клиенты подключаются лишь на небольшой интервал времени, следует уменьшить срок аренды. Как правило, небольшой срок аренды назначают в случае настройки модемного пула. Клиенты подключаются с помощью модемного коммутируемого соединения к своему провайдеру Интернета (ISP – *Internet Service Provider*) и получают по протоколу PPP (*Point to Point Protocol*) IP–адрес для работы. При отключении от Интернета выданные клиентам на короткий срок IP–адреса скоро могут считаться свободными и предоставляться по запросам следующим клиентам. Хотя в стандарте протокола DHCP определена возможность аренды адреса на неопределенный срок (бесконечная аренда), реализация службы протокола в Windows Server 2003 не допускает сдачу адреса в бесконечную аренду.

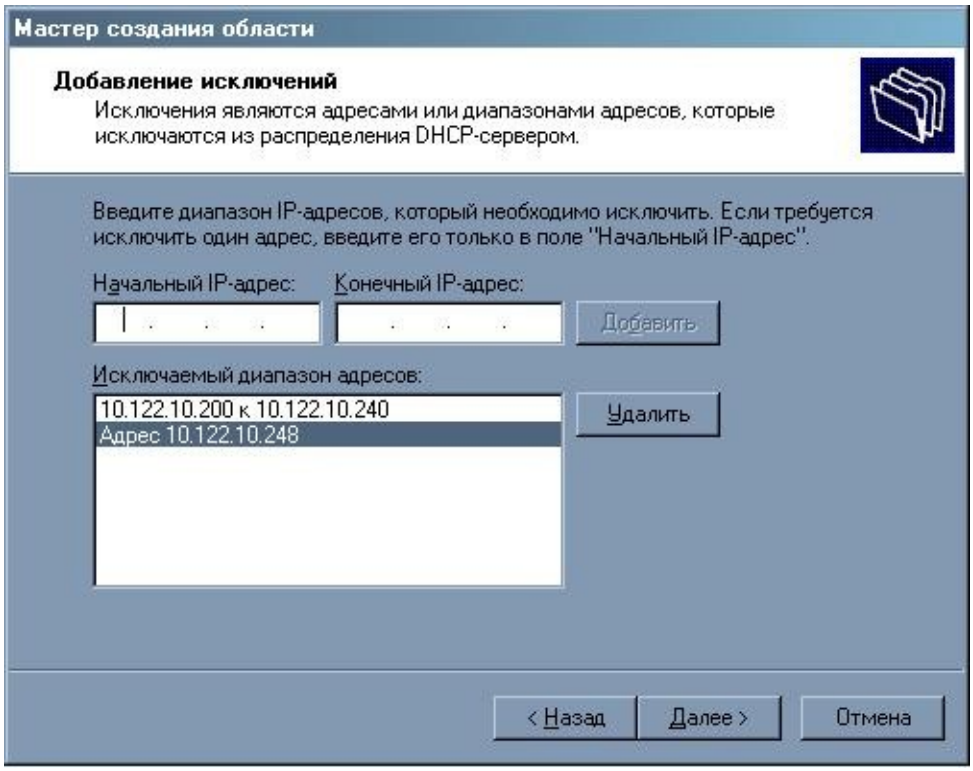

Рис. 8. Определение исключений из диапазона адресов

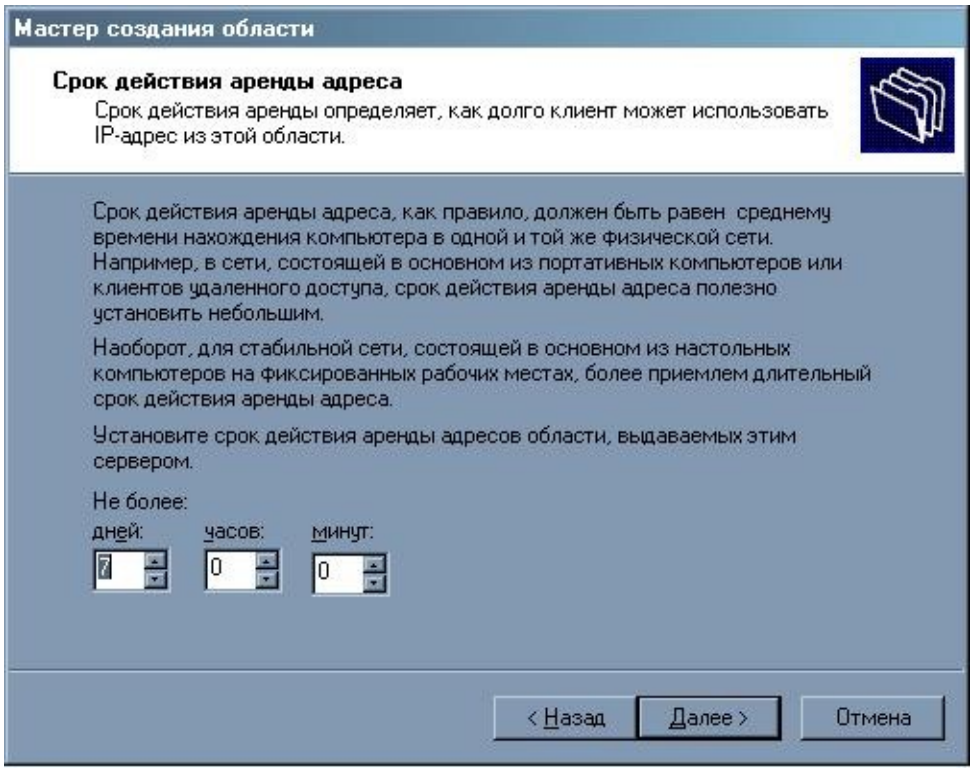

Рис. 9. Указание срока действия аренды IP–адресов

Определив время аренды, администратор фактически заканчивает конфигурирование

области действия. В ходе работы мастера, однако, администратор может сразу определить параметры (опции) DHCP для создаваемой области действия (рис. 10). В этом случае будет задан вопрос: требуется ли определить параметры непосредственно в ходе работы мастера или это будет сделано администратором впоследствии? В большинстве случаев удобнее тут же воспользоваться этой помощью мастера в определении опций. В противном случае нужно самому знать, какие дополнительные параметры следует указать в настройках сервера DHCP. Перечислим эти параметры.

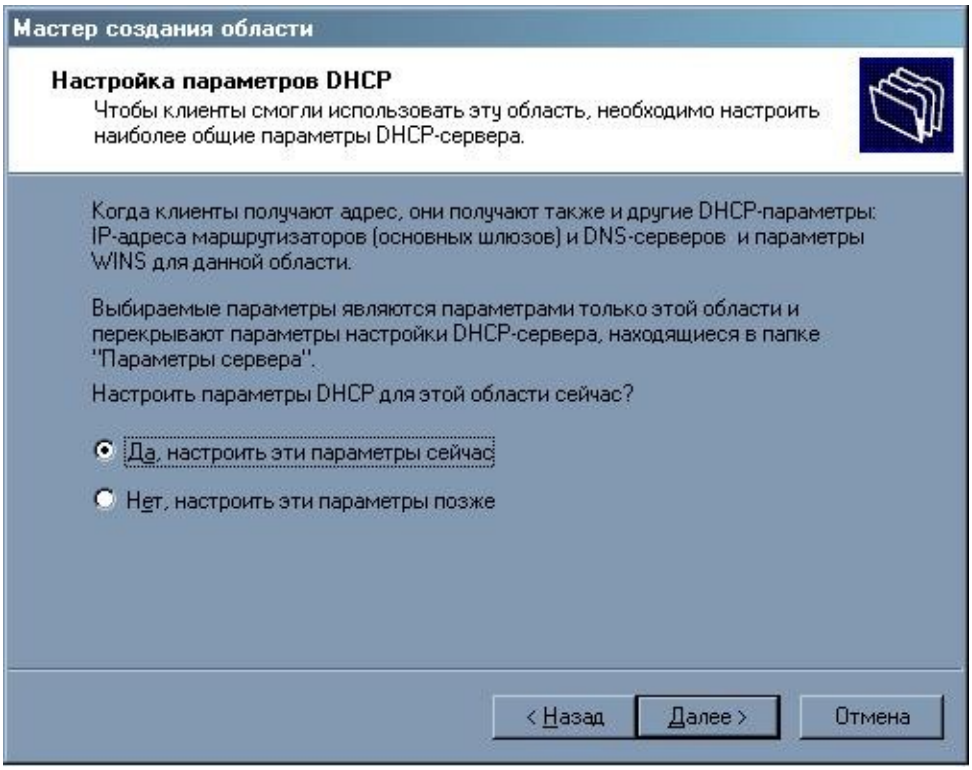

Рис. 10. Настройка параметров DHCP

- Адрес основного маршрутизатора. Основной маршрутизатор (шлюз по умолчанию) (*Default Gateway*) используется для маршрутизации пакетов, адресованных хостам в других подсетях. Если хост не располагает информацией о шлюзе по умолчанию, он не будет способен взаимодействовать с компьютерами из других сетей. В данной опции требуется определить адрес маршрутизатора, который будет осуществлять доставку пакетов хостам в других подсетях (рис. 11).
- DNS–имя домена и адреса DNS–серверов. Эти параметры используются для определения DNS–имени домена и DNS–серверов всех хостов, конфигурируемых посредством данной области действия. DNS–сервер может быть представлен как его именем, так и IP–адресом (доменное имя сервера транслируется в IP–адрес). Опция допускает указание нескольких DNS–серверов, что позволит обеспечить гарантированное разрешение имен в случае, если один из серверов выйдет из строя (см. рис. 12).
- Адреса WINS–серверов. WINS–серверы используются для организации процесса разрешения NetBIOS–имен хостов в IP–адреса этих хостов. Данная опция позволяет снабдить клиента адресами всех действующих в сети WINS–серверов. Так же, как и в случае с DNS–серверами, можно указать адреса нескольких WINS–серверов (рис. 13).

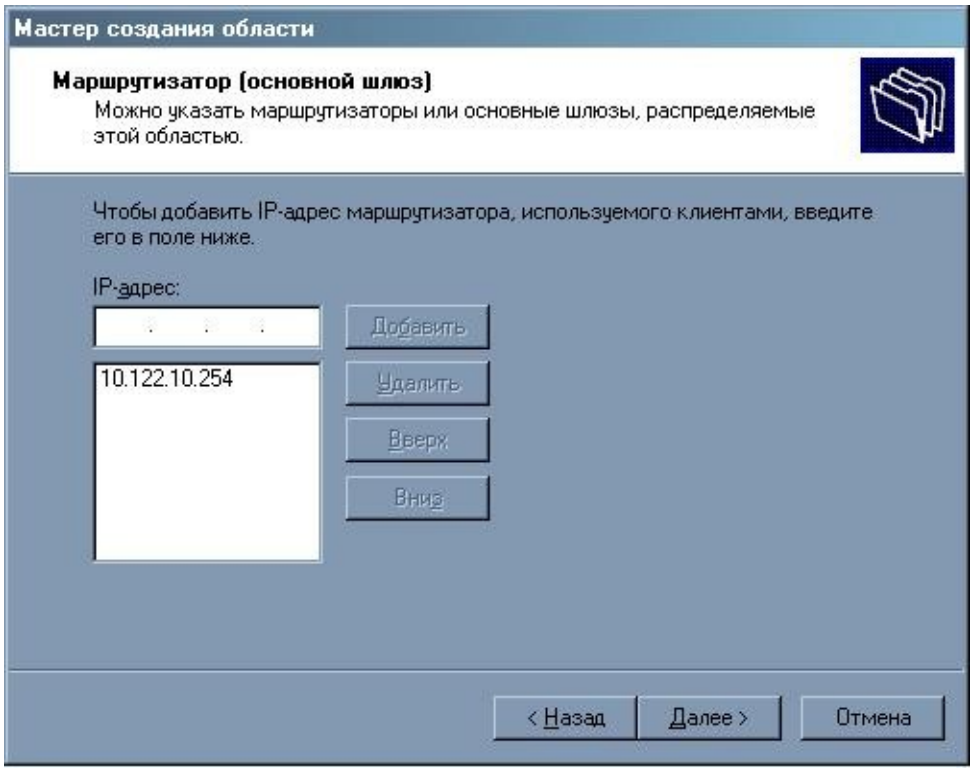

Рис. 11. Указание адреса шлюзов по умолчанию

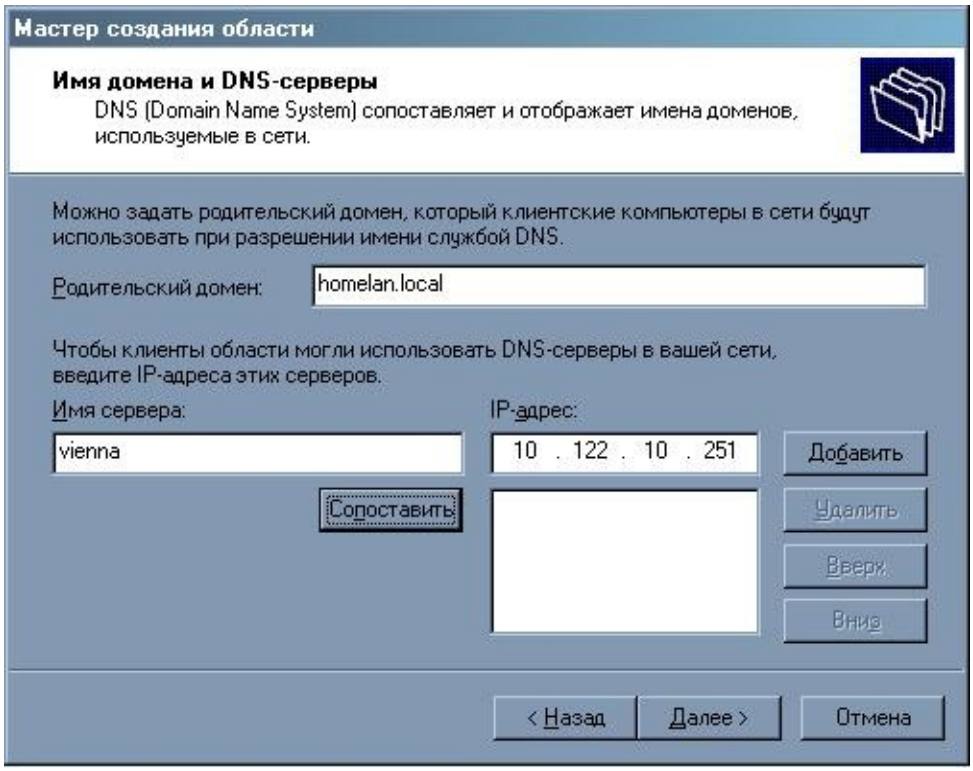

Рис. 12. Определение DNS–имени домена и адресов DNS–серверов

Создаваемые мастером опции определяются на уровне конкретной области действия.

Мастер не может создавать опции на других уровнях.

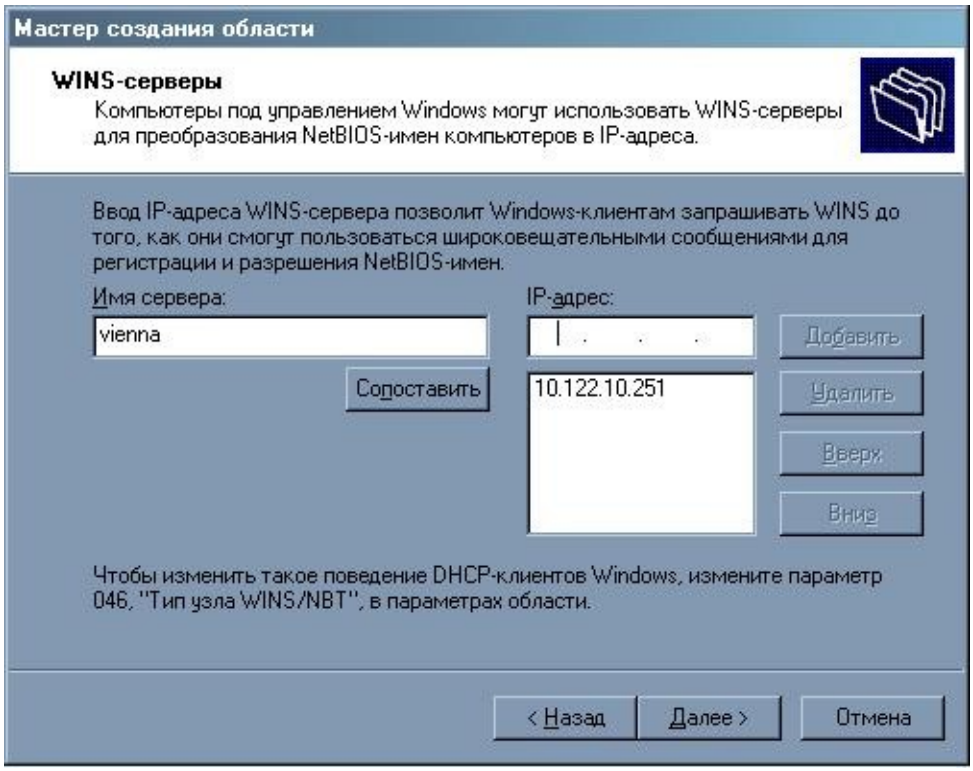

Рис. 13. Определение адреса WINS–сервера

Определяемая мастером информация является только малой частью того, что может быть определено посредством механизма опций. После создания области действия администратор может при необходимости вручную создать дополнительные опции. На заключительном этапе работы мастера нужно решить, будет ли область действия активизирована сразу после ее создания или нет. Активизация области действия приводит к тому, что IP–адреса, определенные в рамках области, могут быть по требованию сданы в аренду. Поэтому если, например, требуется определить ряд дополнительных опций, процесс активизации области действия следует отложить (рис. 14).

Резервирование IP–адресов

Достаточно часто администраторы используют резервирование IP–адресов (см. рис. 15). Привязка компьютера к конкретному (зарезервированному для него) IP–адресу осуществляется посредством указания MAC–адреса его сетевого адаптера. Окно, в котором указывается необходимая для резервирования информация, приведено на рис. 16. Администратор определяет нужный клиенту IP–адрес и сообщает имя этого компьютера и MAC–адрес его сетевой карты.

При необходимости администратор может либо изменить опции области или сервера, либо добавить новые параметры. На рис. 17 показано, что созданная область имеет сконфигурированные опции (это параметры с номерами 003, 006, 015, 044 и 046).

При использовании нескольких областей опции по умолчанию могут быть определены на уровне сервера. В этом случае данные опции будут унаследованы всеми областями. Для этого в контекстном меню контейнера Server Options (Опции сервера) необходимо выбрать

пункт Configure Options (Настроить опции) и определить требуемые параметры.

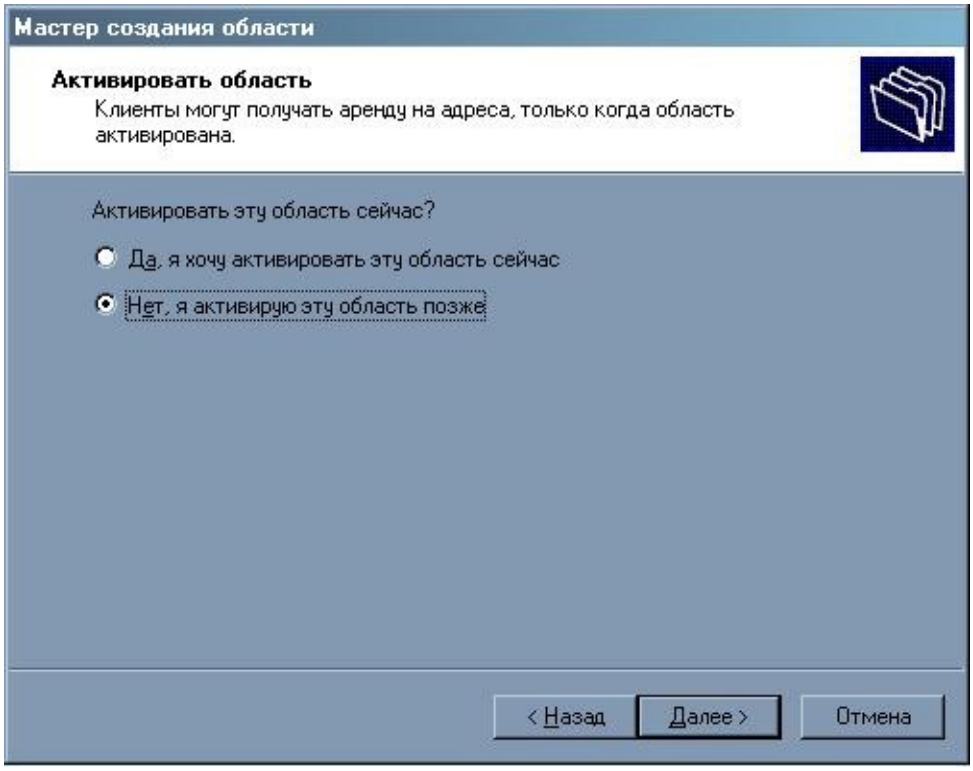

Рис. 14. Отказ от активирования созданной области с целью сконфигурировать для нее дополнительные параметры

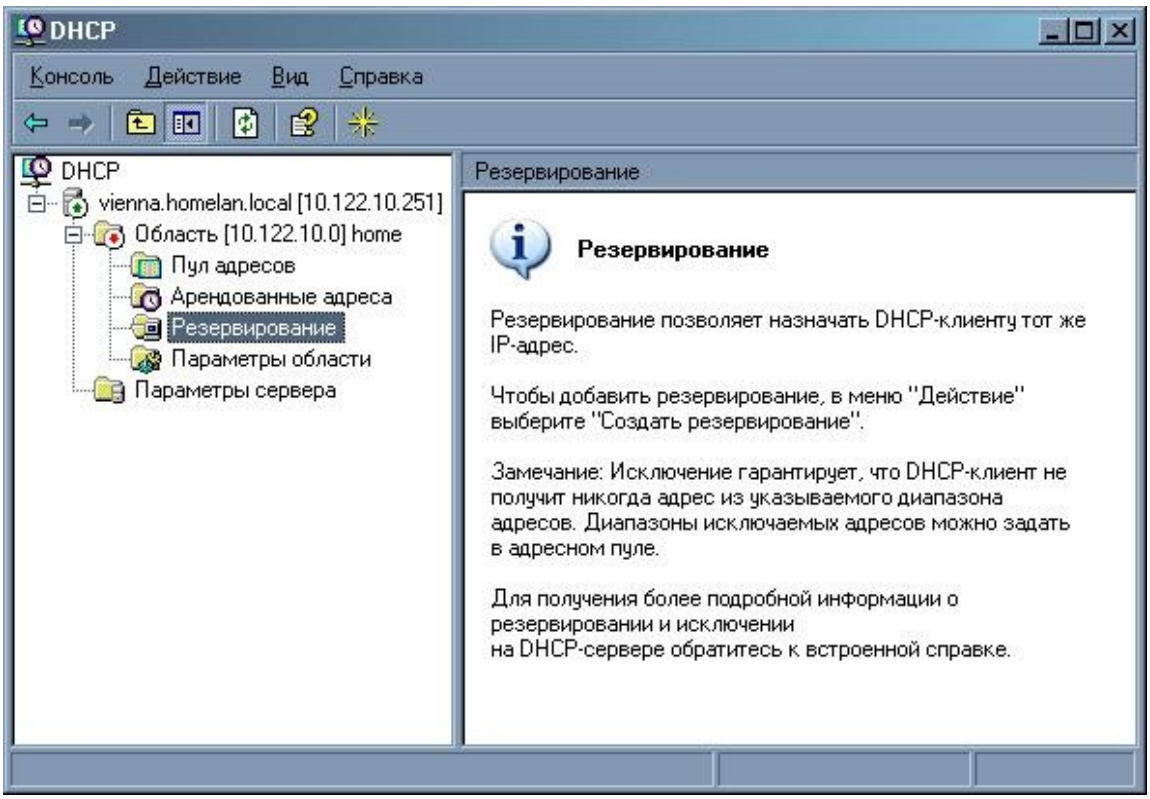

Рис. 15. Резервирование IP–адресов в созданной области

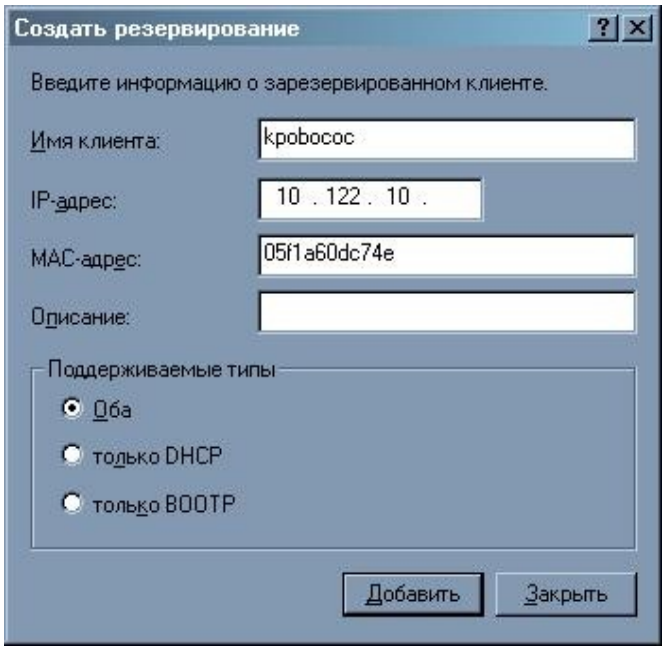

Рис. 16. Резервирование IP–адреса

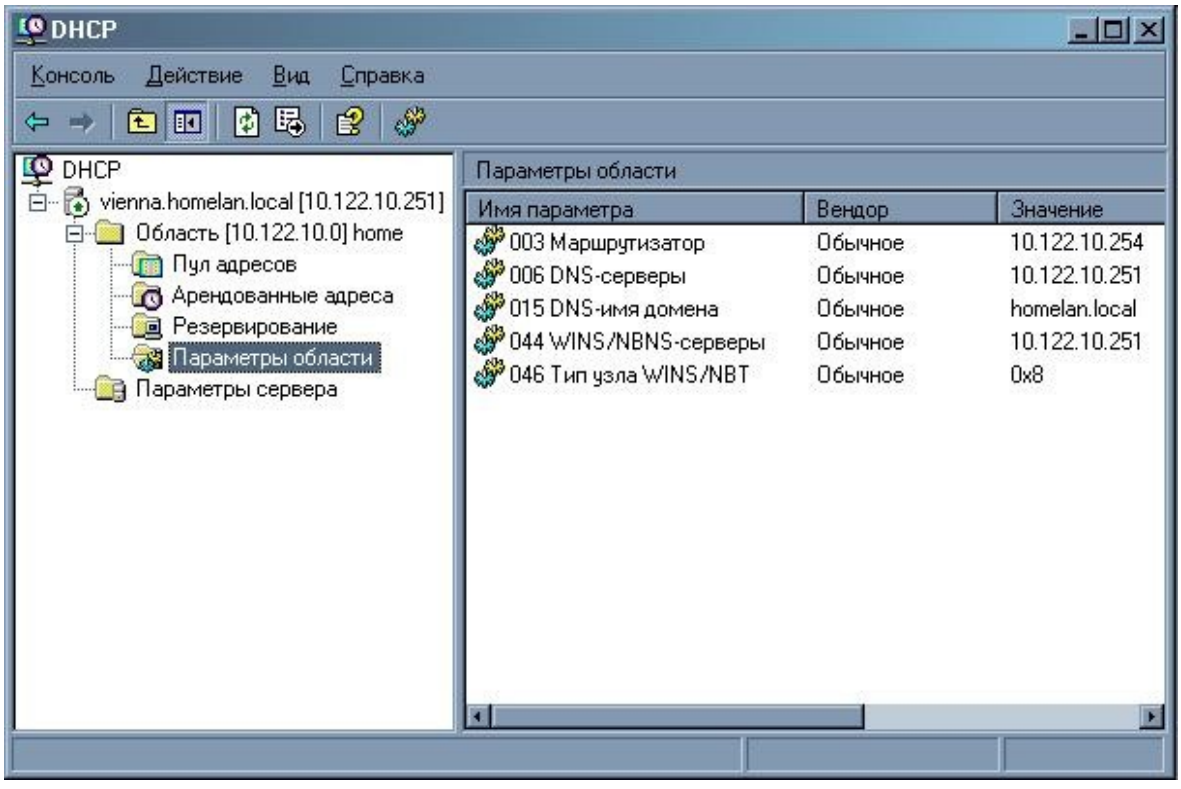

Рис. 17. Параметры области

Настройка механизма динамической регистрации доменных имен

Если нужно, чтобы регистрация доменных имен выполнялась непосредственно на уровне DHCP–сервера, необходимо в окне свойств объекта, ассоциированного с сервером, перейти на вкладку DNS и установить флажок Enable DNS dynamic updates according to the settings below (Разрешить динамические обновления в DNS в соответствии со следующими настройками) (рис. 18). Дополнительно нужно выбрать условия регистрации домен-

ных имен в базе данных DNS. Сервер DHCP будет посылать сообщение службе DNS каждый раз, когда клиенту выдается IP–адрес.

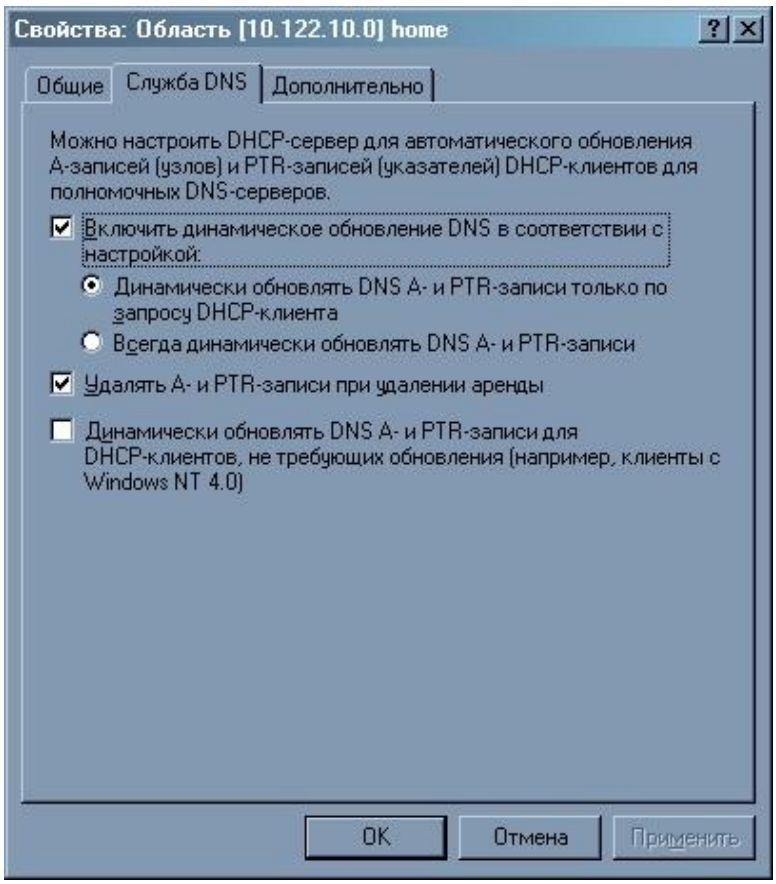

Рис. 18. Активизация режима автоматической регистрации доменных имен в базе данных DNS

Авторизация DHCP–сервера

Если мы имеем дело не с простой сетью типа «рабочая группа», а с корпоративной (доменной), то установленный и правильно сконфигурированный DHCP-сервер перестанет правильно работать при добавлении его в домен. Поэтому в корпоративной (доменной) сети прежде чем DHCP–сервер сможет приступить к процессу выделения адресов DHCP–клиентам, он предварительно должен быть авторизован. Авторизация DHCP–сервера является обязательным условием его нормального функционирования. Иными словами, в каталоге Active Directory должен быть создан объект, соответствующий установленному DHCP–серверу. Только после этого клиенты смогут работать с данным сервером. Все обязанности по осуществлению контроля над авторизацией DHCP–серверов возложены непосредственно на сами DHCP–серверы. Осуществляется это следующим образом. Служба DHCP–сервера при запуске обращается к Active Directory, чтобы просмотреть список IP–адресов авторизованных серверов. Если она не обнаруживает свой адрес в этом списке, она останавливает свою работу.

Для авторизации DHCP–сервера необходимо запустить оснастку DHCP и в контекст-

ном меню объекта, расположенного в корне пространства имен утилиты, выбрать пункт Manage authorized servers (Управление авторизованными серверами). Система покажет список уже авторизованных DHCP–серверов. Нажмите кнопку Authorize (Авторизовать) и укажите имя авторизуемого DHCP–сервера или его IP–адрес. Выбранный сервер будет немедленно добавлен в список авторизованных серверов.

Окончательно сконфигурированная область может быть активизирована (рис. 19).

В настоящей лабораторной работе Вы имеете дело не с корпоративной сетью, поэтому авторизации сервера DHCP не требуется. Программное обеспечение службы каталога в этой работе устанавливать не надо!

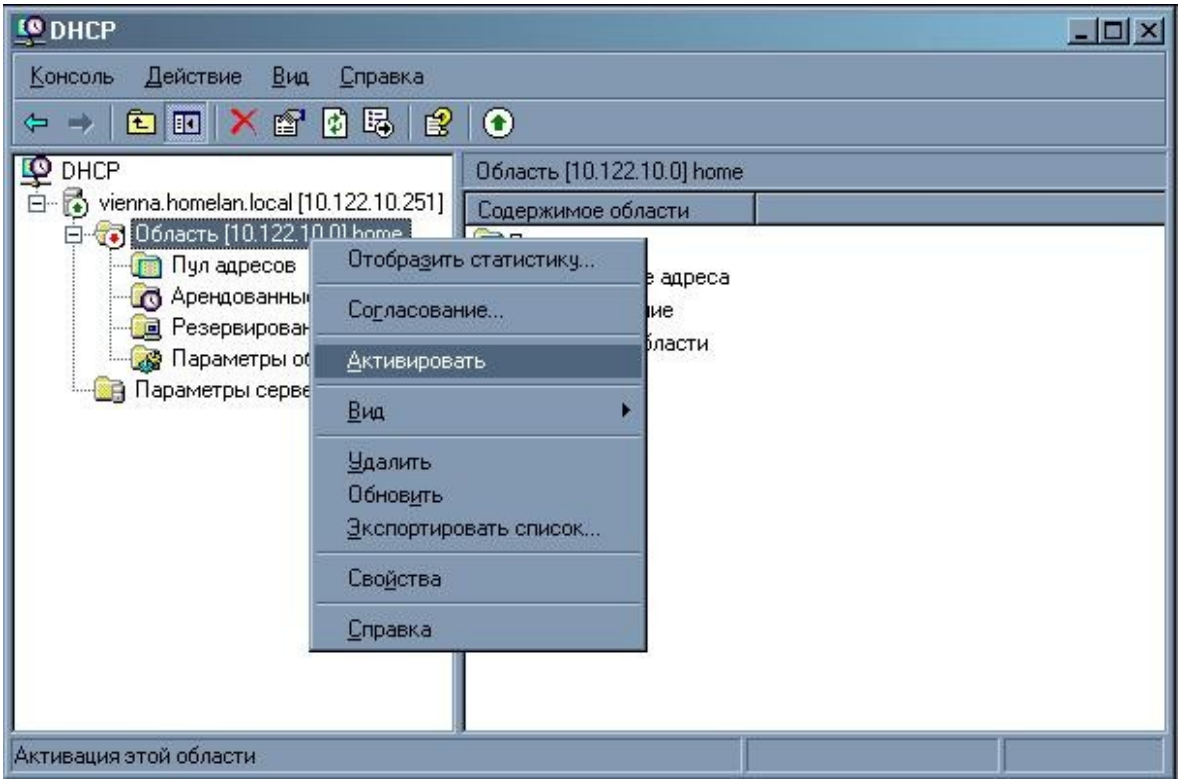

Рис. 19. Активирование созданной области

Диагностические утилиты

Для того чтобы узнать, какие настройки стека протокола мы имеем, следует воспользоваться соответствующими утилитами – `ipconfig`, `arp`, `ping`, `netstat`. Рассмотрим их поподробнее.

Команда ipconfig

Команда `ipconfig` позволяет получить сведения о конфигурации сетевых интерфейсов компьютера, включая его IP-адрес (адреса), маску подсети, основной шлюз и др. Приведем синтаксис команды:

```
ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] |
        /flushdns | /displaydns /registerdns |
        /showclassid адаптер |
        /setclassid адаптер [устанавливаемый_код_класса_dhcp] ]
```

Ключ `/?` позволяет получить подсказку. Остальные ключи означают следующее:

/all - отобразить полную информацию о настройке параметров.
/release - освободить IP-адрес для указанного адаптера.
/renew - обновить IP-адрес для указанного адаптера.
/flushdns - очистить кэш разрешений DNS.
/registerdns - обновить все DHCP-аренды и перерегистрировать DNS-имена
/displaydns - отобразить содержимое кэша разрешений DNS.
/showclassid - отобразить все допустимые для этого адаптера коды (IDs) DHCP-классов.
/setclassid - изменить код (ID) DHCP-класса.

Для ключей /Release и /Renew, если не указано имя адаптера, будет освобожден или обновлен IP–адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

По умолчанию команда отображает только IP-адрес, маску подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Когда команда ipconfig выполняется с параметром /all, она выдает подробный отчет о конфигурации всех интерфейсов, включая все настроенные последовательные порты. Результаты работы команды ipconfig /all можно перенаправить в файл и вставить их в другие документы. Можно также использовать эти результаты для проверки конфигурации TCP/IP на всех компьютерах сети и для выявления причин неполадок TCP/IP-сети.

Например, если компьютер имеет IP-адрес, который уже присвоен другому компьютеру, то маска подсети будет иметь значение 0.0.0.0.

На следующем примере показаны результаты работы команды ipconfig /all на компьютере с Windows XP Professional, настроенном на использование DHCP-сервера для автоматического конфигурирования TCP/IP и WINS- и DNS-серверов для разрешения имен.

```
 Настройка протокола IP для Windows

        Тип узла. . . . . . . . . . . . : гибридный
        IP-маршрутизация включена . . . . : нет
        WINS-прокси включен . . . . . . . : нет

Подключение по локальной сети - Ethernet адаптер:

        Имя компьютера . . . . . . . . . : client1.microsoft.com
        DNS-серверы. . . . . . . . . . . : 10.1.0.200
        Описание . . . . . . . . . . . . : 3Com 3C90x Ethernet Adapter
        Физический адрес . . . . . . . . : 00-60-08-3E-46-07
        DHCP включен . . . . . . . . . . : да
        Автонастройка включена . . . . . : да
        IP-адрес . . . . . . . . . . . . : 192.168.0.112
        Маска подсети. . . . . . . . . . : 255.255.0.0
        Основной шлюз. . . . . . . . . . : 192.168.0.1
        DHCP-сервер. . . . . . . . . . . : 10.1.0.50
        Основной WINS-сервер . . . . . . : 10.1.0.101
        Дополнительный WINS-сервер . . . : 10.1.0.102
        Аренда получена. . . . . . . . . : Среда, 04 сентября, 2019 г. 10:32:13
        Аренда истекает. . . . . . . . . : Пятница, 13 сентября, 2019 г.
10:32:13
```

Проверка соединений с помощью программы ping

Если с конфигурацией TCP/IP все в порядке, следующим шагом должна быть проверка

возможности соединения с другими узлами TCP/IP-сети. Ее можно провести с помощью команды ping. Синтаксис этой команды следующий:

```
ping [-t] [-a] [-n <число>] [-l <размер>] [-f] [-i <TTL>] [-v <TOS>]
   [-r <число>] [-s <число>] [[-j <список_узлов>] | [-k <список_узлов>]]
   [-w <таймаут>] [-R] [-S <источник>] [-4] [-6] <конечный_узел>

  -t      Отправка пакетов на указанный узел, пока вы не прекратите
          опрос узла вручную. Для вывода статистики и продолжения
          опроса нажмите <Ctrl>+<Break>, для прекращения опроса
          нажмите <Ctrl>+<C>.

  -a      Определение имени узла по адресу.

  -n <число>        Число отправляемых запросов.

  -l <размер>       Размер буфера отправки.

  -f                Установка флага, запрещающего фрагментацию пакета

  -i <TTL>          Задание срока жизни пакета ("Time To Live").

  -v <TOS>          Задание типа службы ("Type Of Service")

  -r <число>        Запись маршрута для указанного числа прыжков

  -s <число>        Штамп времени для указанного числа прыжков

  -j <список_узлов> Свободный выбор маршрута по списку узлов

  -k <список_узлов> Жесткий выбор маршрута по списку узлов

  -w <таймаут>      Таймаут для каждого ответа в миллисекундах.
```

С помощью команды ping мы, используя протокол ICMP, отправляем эхо-запрос интересующему узлу, указав его имя или IP–адрес. Используйте команду ping всегда, когда требуется проверить, может ли узел подключаться к сети TCP/IP и ее ресурсам. Команду ping можно также использовать для выявления неполадок сетевых устройств и неправильных конфигураций.

Обычно лучше всего проверять наличие маршрута между локальным компьютером и узлом сети, обращаясь сначала к узлу с помощью команды ping и IP–адреса этого узла. Для этого выполните следующую команду: ping *IP-адрес*

Используя команду ping, следует выполнить перечисленные ниже действия.

1. Обратитесь по адресу замыкания на себя, чтобы проверить правильность настройки TCP/IP на локальном компьютере.
   ping 127.0.0.1
2. Обратитесь по IP-адресу локального компьютера, чтобы убедиться в том, что он был правильно добавлен к сети.
   ping IP-адрес_локального_узла
3. Обратитесь по IP-адресу основного шлюза, чтобы проверить работоспособность основного шлюза и возможность связи с локальным узлом локальной сети.
   ping IP-адрес_основного_шлюза
4. Обратитесь по IP-адресу удаленного узла, чтобы проверить возможность связи через маршрутизатор.
   ping IP-адрес_удаленного_узла

Команда ping использует разрешение имен компьютеров в IP–адреса в стиле Windows Sockets, поэтому если обратиться с ее помощью по адресу удается, а по имени — нет, то проблема кроется в разрешении имен или адресов, а не в сетевом соединении.

Если обращение с помощью команды ping на каком-либо этапе оканчивается неудачей, убедитесь, что:

- после настройки протокола TCP/IP компьютер был перезагружен;
- IP–адрес локального компьютера является допустимым и правильно отображается на вкладке Общие диалогового окна Свойства: Протокол Интернета (TCP/IP);
- включена IP-маршрутизация и связь между маршрутизаторами функционирует нормально.

Команда ping может выполняться с различными параметрами, задающими такие характеристики, как размер пакетов, число отправляемых пакетов и срок жизни пакета (TTL – Time to Live), и определяющими, нужно ли записывать используемый маршрут и нужно ли устанавливать флаг, запрещающий фрагментацию пакетов. Для просмотра этих параметров введите команду ping –?.

На следующем примере показано, как можно отправить два пакета размером по 1450 байт по IP-адресу 172.17.8.1:

```
C:\>ping -n 2 -l 1450 172.17.8.1
Обмен пакетами с 172.17.8.1 по 1450 байт:

Ответ от 172.17.8.1: число байт=1450 время<10мс TTL=32
Ответ от 172.17.8.1: число байт=1450 время<10мс TTL=32

Статистика Ping для 172.17.8.1:
    Пакетов: отправлено = 2, получено = 2, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    наименьшее = 0мсек, наибольшее =  10мсек, среднее =  5мсек
```

По умолчанию команда ping ожидает возврата каждого запроса в течение 4000 мс (4 секунды), а потом выдает сообщение «Превышен интервал ожидания для запроса». Если удаленная система, к которой выполняется обращение, использует соединение, характеризуемое большими задержками, то для возврата запроса может потребоваться большее время. Чтобы задать большее время ожидания, используйте параметр –w.

Обратите внимание, что по умолчанию сетевые интерфейсы компьютеров, работающих под управлением ОС Windows закрыты для команды ping. Чтобы убрать этот запрет нужно разрешить работу протокола ICMP. Сделать это можно как в настройках сетевого адаптера, так и в настройках файервола. Главное — это ни в коем случае не отключать файервол, поскольку его отключение приводит к отказу от защиты компьютера.

Устранение неполадок с аппаратными адресами с помощью программы arp

Как мы уже знаем, протокол ARP (*Address Resolution Protocol*) позволяет узлам определять аппаратные адреса сетевых интерфейсов других узлов, расположенных в той же физической сети, по IP–адресам этих узлов. Напомним, что каждое устройство, предназначенное для работы в локальной сети, должно иметь уникальный аппаратный адрес, присвоенный разработчиком. Для устройств локальных сетей этот адрес называется адресом уровня управления доступом к среде передачи (*MAC–адресом*). Каждый такой аппаратный адрес иден-

тифицирует устройство в физической Ethernet– сети с помощью 6-байтового числа, записанного в ПЗУ сетевого адаптера. Аппаратные адреса обычно представляются в шестнадцатеричном формате, например 00-AA-00-3F-89-4A. Регистрацией и выделением аппаратных адресов занимается институт IEEE (Institute of Electrical and Electronics Engineers). В настоящее время IEEE регистрирует и назначает отдельным изготовителям уникальные числа для первых трех байтов аппаратного адреса. Последние три байта аппаратного адреса каждый изготовитель назначает сетевым адаптерам самостоятельно.

Аппаратные адреса (или MAC–адреса – адреса уровня управления доступом к среде передачи) определяются путем посылки широковещательного сетевого запроса следующего вида: «Какой аппаратный адрес имеет устройство с указанным IP–адресом?». Когда на ARP–запрос отправляется ответ, то отправитель ARP–ответа и запрашивающий узел заносят IP–адреса и аппаратные адреса друг друга в локальную таблицу, называемую кэшем ARP, для дальнейшего использования. Для более эффективного использования ARP каждый компьютер кэширует сопоставления IP–адресов с аппаратными адресами, устраняя тем самым повторяющиеся широковещательные запросы ARP.

Для просмотра и изменения таблицы ARP локального компьютера можно использовать команду `arp`. Команда `arp` служит для просмотра кэша ARP и устранения неполадок с разрешением адресов. Для ознакомления с параметрами команды `arp` выполните команду `arp /?` в командной строке. Обратите внимание, что каждый сетевой адаптер имеет свой кэш ARP.

Команда Netstat

Команда `Netstat` осуществляет вывод статистики протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола TCP/IP.

```
netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал]
```

Параметры у этой команды следующие:

```
-a      Выводит все подключения и сетевые порты. Подключения сервера обычно не
выводятся.

-e      Выводит статистику Ethernet. Возможна комбинация с ключом -s.

-n      Выводит адреса и номера портов в шестнадцатеричном формате (а не имена).

-s      Выводит статистику для каждого протокола. По умолчанию выводится
статистика для TCP, UDP, ICMP и IP. Ключ -p может быть использован для указания
подмножества стандартных протоколов.

-p протокол     Выводит соединения для протокола, заданного параметром протокол.
Параметр протокол может иметь значения tcp или udp. Если используется с ключом
-s для вывода статистики по отдельным протоколам, протокол может принимать
значения tcp, udp, icmp или ip.

-r      Выводит таблицу маршрутизации.

Интервал        Обновляет выведенную статистику с интервалом в интервал секунд.
Нажатие клавиш CTRL+B останавливает обновление статистики. Если этот параметр
пропущен, netstat выводит сведения о текущей конфигурации один раз
```

Лабораторная работа № 1: IP-адресация

Цель работы: изучить теорию и практику назначения IP–адресов, научится устанавливать и конфигурировать DHCP–сервер.

Порядок выполнения лабораторной работы

1. Создайте или импортируйте готовые виртуальные машины. Одна из них будет выступать в роли сервера, а вторая — в роли клиента. Сконфигурируйте обе виртуальные машины таким образом, чтобы их виртуальные сетевые адаптеры были подключены к виртуальной сети. Это означает, что кадры данных (а значит и пакеты данных) будут существовать только в одной из виртуальных сетей, с которой мы работаем. К той же самой виртуальной сети нужно будет подключать и виртуальную машину с Windows XP Professional. Пусть это будет виртуальная сеть Intnet.

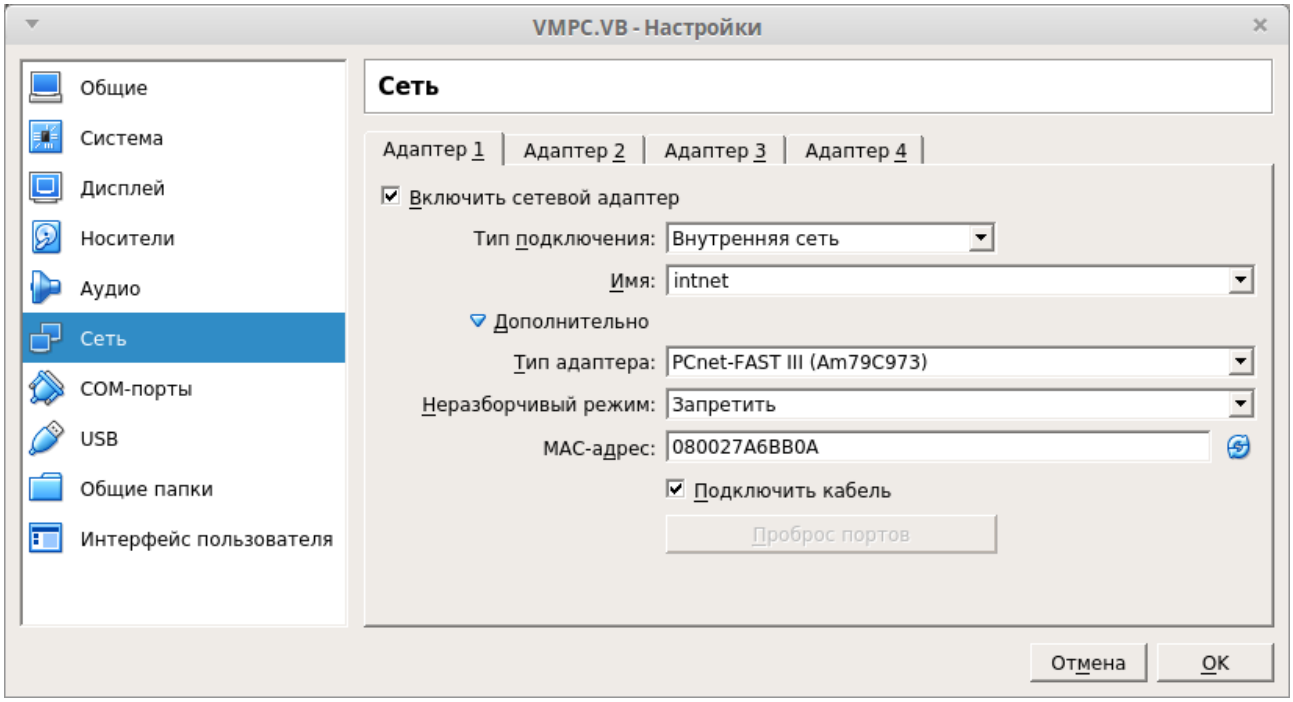

Рис. 20. Настройка виртуального сетевого интерфейса

2. Присвойте вашему серверу имя согласно варианту задания. Установите для сервера статический IP–адрес тоже в соответствии с вариантом вашего задания.

Аналогичным образом сконфигурируйте виртуальную рабочую станцию с системой Windows XP Professional. Проверьте работоспособность стека TCP/IP для этих двух виртуальных машин с помощью диагностических утилит, покажите результаты преподавателю и сделайте соответствующие скриншоты.

3. Установите на сервер с Windows Server службу DHCP. Сконфигурируйте ее согласно вашему варианту задания. Переведите станцию с Windows XP Professional (Windows 7) в статус DHCP–клиента. Добейтесь, чтобы эта станция получала IP–адрес от сервера DHCP. Посмотрите, что среди арендованных IP–адресов присутствует адрес, полученный клиентом. Этот адрес должен быть первым из пула адресов, предоставляемых в аренду. Покажите

преподавателю полученные результаты и работоспособность обоих компьютеров по стеку протоколов TCP/IP с помощью диагностических утилит.

4. Зарезервируйте для клиентской машины фиксированный IP–адрес. С помощью командной строки освободите IP–адрес, занимаемый клиентом. Также с помощью соответствующей команды инициируйте получение клиентским компьютером нового IP–адреса. Удостоверьтесь, что он соответствует зарезервированному. Покажите результат преподавателю.

5. Создайте отчет и сдайте коллоквиум по работе.

Варианты заданий для выполнения лабораторной работы

Имя сервера (имя NetBIOS) должно соответствовать имени Вашего отца, записанному латинскими буквами. Имя рабочей станции должно соответствовать Вашему имени.

Номер сети (подсети) и IP–адрес сервера и рабочей станции должны удовлетворять следующему правилу:

Номер сети	172.(16+N).M.0/24,
где	N – это последняя цифра из номера группы,
	M – ваш порядковый номер по журналу;
IP–адрес сервера	172.(16+N).M.K/24,
где	K – длина Вашей фамилии;
IP–адрес клиента	172.(16+N).M.(100+K)/24.

При настройке DHCP–сервера оставить IP–адрес сервера тем же, а при конфигурировании параметров области нужно выполнить следующие требования:

IP–адрес маршрутизатора 172.(16+N).M.1/24;

IP–адрес DNS– и WINS– серверов пусть соответствуют IP–адресу вашего сервера (конфигурировать эти серверы в данной лабораторной работе не нужно).

Имя домена, которое должны получать клиенты, должно удовлетворять правилу: <family>.gxxxx.local, где family – это Ваша фамилия, записанная латинскими буквами; xxxx-номер группы.

Зарезервированный адрес для клиента должен быть равен 172.(16+N).M.(200+K)/24

Контрольные вопросы

1. Что такое IP–адрес? Что он показывает?
2. Объясните классовую модель IP–адресации.
3. Перечислите диапазоны частных IP–адресов.
4. Что собой представляет сетевая маска? Для чего она нужна?
5. Объясните основной принцип разделения сетей на подсети.
6. На сколько подсетей максимум можно разделить сеть 192.168.0.0?
7. На сколько подсетей максимум можно разделить сеть 172.29.0.0?
8. Что такое DHCP–сервер? Для чего он нужен?
9. Расскажите алгоритм взаимодействия клиента и сервера по протоколу DHCP.
10. Что такое DNS– и WINS– сервер? Для чего они нужны?
11. Что такое область действия DHCP–сервера?
12. Как и для чего резервируются в области действия IP–адреса?
13. Что такое авторизация DHCP–сервера?
14. Какие диагностические утилиты Вы знаете? Расскажите как с ними нужно работать.

Тема № 2: СИСТЕМА ДОМЕННОГО ИМЕНОВАНИЯ

(Domain Name System – DNS)

Краткие теоретические сведения

Система доменных имен (Domain Name System) предназначена для того, чтобы компьютеры, работающие в сети Internet, могли по доменному имени узнать IP-адрес нужной им машины (узла), а также некоторую другую информацию; а по IP-адресу узла могли узнать его доменное имя. Сервис DNS является "служебным" - он обслуживает запросы не только пользователей, но и других программ, которые обслуживают пользовательские запросы. Эту систему в стеке TCP/IP относят к уровню приложений. В числе клиентов DNS имеются и другие программы - серверы, proxy-серверы и т.п. Служба DNS работает для других программ наряду с протоколом ARP, динамической и статической IP-маршрутизацией незаметно для пользователей.

Система доменных имен была разработана для именования машин в глобальной сети, для которой основной особенностью является распределенное администрирование, когда один администратор физически не может уследить за выделением имен для всех компьютеров. Поэтому DNS функционирует на принципе делегирования полномочий - каждый сервер этой системы либо знает ответ на вопрос, поскольку в его базе данных есть искомая информация, либо знает у кого спросить. При правильном функционировании система замкнута, т.е. если запрошенная информация имеется у кого-либо, то она будет найдена и сообщена клиенту; либо, если вопрос не имеет ответа, клиент получит сообщение о невозможности получения ответа на вопрос.

DNS представляет собой иерархическую распределенную систему баз данных с некоторым дублированием информации. "Распределенность" означает, что при правильной настройке каждый из серверов системы, называемый DNS-сервером, содержит либо нужную информацию, либо ссылку на более компетентный источник. На любой запрос система должна давать одинаковый ответ независимо от того, к какому серверу мы обращаемся. "Дублирование информации" происходит путем создания копий, динамически синхронизирующихся с оригиналом. Поэтому все важные ссылки также продублированы.

Все пространство имен разделено на так называемые домены (domain) — множества объектов, которые могут иметь IP-адрес. Объекты домена объединяет принадлежность к домену, на что указывает имя объекта. Имена являются составными и к имени объекта добавляется имя домена, в который он входит. Все пространство имен всех объектов относится к домену высшего уровня иерархии; его называют нулевым уровнем и оно не имеет имени. Домен нулевого уровня иерархии разделён на домены первого уровня иерархии и все эти домены уже имеют уникальные имена. Все они зарегистрированы в домене самого высокого уровня и все серверы нулевого уровня системы доменных имён содержат в себе информацию о доменах первого уровня иерархии. Это так называемые корневые серверы имен, их 13 и они размещены в разных странах и на разных континентах. Домены первого уровня иерархии делят всё пространство имен либо по организационному принципу (для этого используются трехбуквенные имена доменов), либо по территориальному (в этом случае используются двухбуквенные имена, они обозначают страны). Кроме этого существует ещё несколько служебных доменов.

Имя узла получается составным — оно начинается с простого имени, а далее после десятичной точки указывается имя домена, в котором находится узел. Если этот домен сам расположен в домене более высокого уровня иерархии, т. е. выступает как поддомен, то после имени поддомена ставится опять десятичная точка и записывается имя домена, в котором зарегистрирован поддомен. Таким образом можно отобразить всю иерархию доменов. Длина простого имени ограничивается длиной в 63 символа, а общее доменное имя, включающее все десятичные точки, не должно превышать 255 символов. Для указания корневого домена в доменном имени узла используется символ точки (".") на конце имени. Доменные имена, заканчивающиеся точкой, называют абсолютными доменными именами (FQDN — Fully-Qualified Domain Name). Простое доменное имя может состоять из прописных латинских букв, арабских цифр и знака «минус». В последние годы появились расширения для правил составления доменных имен — можно использовать национальные алфавиты, если они зарегистрированы. Доменные имена первого уровня иерархии регистрирует международная организация по присвоению имен и адресов в Интернете (ICANN).

В качестве простого примера рассмотрим имя mail.guap.ru. Это имя почтового сервера в нашем университете. Если выполнить команду `ping mail.guap.ru.` , то получим информацию о прохождении контрольных пакетов от почтового сервера mail.guap.ru. и адрес почтового сервера - он имеет значение 91.151.188.3. (смотри рисунок 21). Этот адрес был получен благодаря работе DNS. Его сообщил нам dns-сервер домена guap.ru. В его локальной базе данных (такие базы данных называются зонными файлами, поскольку в них отображается так называемая зона домена) записано, что компьютер с именем mail.guap.ru имеет ip-адрес 91.151.188.3. Адрес самого dns-сервера guap.ru. 194.226.199.248. Сам домен guap.ru зарегистрирован в домене ru. , а тот, в свою очередь — в корневом домене (.).

```
PING mail.guap.ru (91.151.188.3) 56(84) bytes of data.
64 bytes from ns1.guap.ru (91.151.188.3): icmp_seq=1 ttl=62 time=1.40 ms
64 bytes from ns1.guap.ru (91.151.188.3): icmp_seq=2 ttl=62 time=1.40 ms
64 bytes from ns1.guap.ru (91.151.188.3): icmp_seq=3 ttl=62 time=1.19 ms
64 bytes from ns1.guap.ru (91.151.188.3): icmp_seq=4 ttl=62 time=1.39 ms
64 bytes from ns1.guap.ru (91.151.188.3): icmp_seq=5 ttl=62 time=1.23 ms

--- mail.guap.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.194/1.325/1.408/0.102 ms
```

Рисунок 21. Результат работы команды `ping mail.guap.ru.`

```
PING guap.ru (194.226.199.248) 56(84) bytes of data.
```

```
     64 bytes from 194.226.199.248: icmp_seq=1 ttl=126 time=1.52
ms
     64 bytes from 194.226.199.248: icmp_seq=2 ttl=126 time=1.84
ms
     64 bytes from 194.226.199.248: icmp_seq=3 ttl=126 time=1.54
ms

     --- guap.ru ping statistics ---
     3 packets transmitted, 3 received, 0% packet loss, time
2003ms
     rtt min/avg/max/mdev = 1.521/1.635/1.840/0.145 ms


     Link encap:Ethernet  HWaddr 00:23:54:1A:39:72
                  inet addr:194.226.199.151  Bcast:194.226.199.159
Mask:255.255.255.240
               inet6 addr: fe80::223:54ff:fe1a:3972/64 Scope:Link
               UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:4045705 errors:0 dropped:0 overruns:0
frame:0
                  TX packets:7913060 errors:0 dropped:0 overruns:0
carrier:0
               collisions:0 txqueuelen:0
                           RX bytes:1044031304 (995.6 MiB)    TX
bytes:9553301103 (8.8 GiB)
```

Рисунок 22. Результат работы команды `ping guap.ru`.

Для разрешения имени в IP-адрес DNS-клиент обращается к своему DNS-серверу. Если в его зоне есть искомая информация, то он ответит клиенту. Зоной называют область ответственности DNS-сервера, она представлена в локальном файле системы доменных имен, в котором содержится соответствие между доменными именами текущего локального домена и их IP-адресами. Это текстовый файл, его можно просматривать и его легко редактировать. Совокупность всех локальных зон, связанных друг с другом через зоны, а значит и домены более высокого уровня иерархии, представляет собой всё пространство имен и адресов Интернета. Таким образом, система является иерархической и распределённой одновременно. При отсутствии искомой информации в текущей зоне DNS-сервер либо обращается к вышестоящему DNS-серверу, либо сразу к корневому домену. Поскольку интенсивность обращения к корневому домену очень высока, число корневых DNS-серверов увеличили до 13; они распределены по разным континентам и странам, их IP-адреса Вы можете увидеть в файле cache.dns, который создаётся при установке службы DNS (фрагменты этого файла показаны на рисунке 23).

```
;
;   cache.dns - КЭШ-ФАЙЛ DNS
;
;   Начальные данные для корневых серверов домена.
```

```
;
;   ВАМ НЕБОХОДИМО ИЗМЕНИТЬ:
;   ->  Ничего, если вы подключены к Интернету. Изменяйте этот файл
;       только при выпуске обновленного списка корневых серверов.
;           ИЛИ
;   ->  Если вы не подключены к Интернету, удалите эти записи и замените
;       записями NS и A для DNS-сервера, управляющего корневым доменом
;       для вашего сайта.
;
;
;       Этот файл содержит информацию о корневых серверах имен, необходимых
;       для инициализации кэша серверов доменных имен в Интернете
;       (см. ссылку на этот файл в файле настройки "cache  .  <file>"
;       серверов привязки доменных имен BIND).
;
;       Этот файл был предоставлен службами регистрации InterNIC
;       на анонимном FTP как
;           файл                /domain/named.root
;           на сервере          FTP.RS.INTERNIC.NET
;       -ИЛИ- через Gopher      RS.INTERNIC.NET
;           в меню              InterNIC Registration Services (NSI)
;              подменю          InterNIC Registration Archives
;           файл                named.root
;
;       последнее обновление:   22 августа 1997 г.
;       соответствующая версия корневой зоны: 1997082200
;
;
; ранее - NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; ранее - NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
;
; …..
;
; размещен в Японии, управляется WIDE
;
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
; конец файла
```

Рисунок 23. Файл cache.dns с перечнем корневых DNS-серверов

DNS-сервер может работать либо в рекурсивном режиме, либо в итерационном. При рекурсивном режиме DNS-сервер либо дает ответ на запрос клиента «какой адрес имеет хост с заданным именем?», либо сообщает, что такое имя не зарегистрировано в системе доменных имен. Это означает, что DNS-сервер сам опрашивает всю систему имен. При итерационном режиме DNS-сервер либо возвращает ответ на полученный запрос, найдя его в своих зонах или в кэше, либо сообщает адрес другого DNS-сервера, у которого клиент должен будет дальше запрашивать искомую информацию.

В системе доменного именования определено два типа DNS-серверов: первичные (primary masters) и вторичные (secondary masters). Первичный сервер имен получает данные о зоне, для которой он является полномочным, либо за счет заполнения этой зоны

администратором, либо собирая эти данные от компьютеров, которые централизованно получают IP-адреса от DHCP-сервера. Вторичный сервер имен получает данные о зоне от другого полномочного сервера имен. Когда стартует вторичный сервер, он связывается с полномочным (первичным) сервером зоны и скачивает данные о зоне (получает реплику). Такую процедуру называют передачей зоны (zone transfer). В процессе работы вторичный сервер периодически опрашивает первичный сервер. Если данные на первичном сервере были изменены, то вторичный сервер обновляет свои данные, заново перекачивая все данные зоны с первичного сервера. Параметры передачи новых данных от первичного сервера задаются в главной записи зоны, называемой SOA (Start of Authority). В этой записи (смотри рисунок 24) помимо имени зоны и имени DNS-сервера есть такие параметры как версия зоны (Serial Number), период обновления зоны (Refresh), продолжительность попыток обновить зону (Retry), время актуальности копии зоны (Expire) в случае невозможности связаться с первичным сервером имен, время жизни кэшированных ответов (TTL).

```
;
;  Database file guap.local.dns for guap.local zone.
;      Zone version:  7
;

@                                   IN   SOA router-1.guap.local.
hostmaster.guap.local. (
                            7            ; serial number
                            900          ; refresh
                            600          ; retry
                            86400        ; expire
                            3600       ) ; default TTL

;
```

Рисунок 24. Запись SOA в файле guap.local.dns зоны guap.local.

Обычно для зоны создается один первичный сервер имен и один или несколько вторичных серверов. Сервер имен может быть первичным для некоторой зоны и вторичным для другой зоны.

Данные, содержащие адресную информацию, в пространстве доменных имен индексируются по имени. Поэтому нахождение адреса по данному имени является относительно простой задачей. Но нахождение доменного имени, которому соответствует определенный адрес, в такой модели не является тривиальной задачей, так как требует перебора адресных значений каждого доменного имени в дереве. Для предоставления такого поиска было выбрано довольно простое и эффективное решение. Так как найти данные, индексированные по имени, в дереве имен просто, в пространстве доменных имен Internet был создан специальный домен in-addr.arpa.

Узлы в домене in-addr.arpa именуются по номерам в представлении IP-адресов четырьмя десятичными цифрами, разделенными точками (каждая десятичная цифра находится в диапазоне от 0 до 255). В этом случае домен in-addr.arpa может иметь до 256 поддоменов, каждый из которых соответствует каждому возможному значению первой цифры IP-адреса. Каждый из этих поддоменов может иметь до 256 поддоменов нижнего уровня, соответствующие возможным значениям второй цифры IP-адреса. На последнем

четвертом уровне будут находиться записи о ресурсах, связанные с последней цифрой IP-адреса, которые будут содержать полные доменные имена хост-машин или сетей, соответствующих этим IP-адресам.

Структура домена `in-addr.arpa` поясняется рисунком 25:

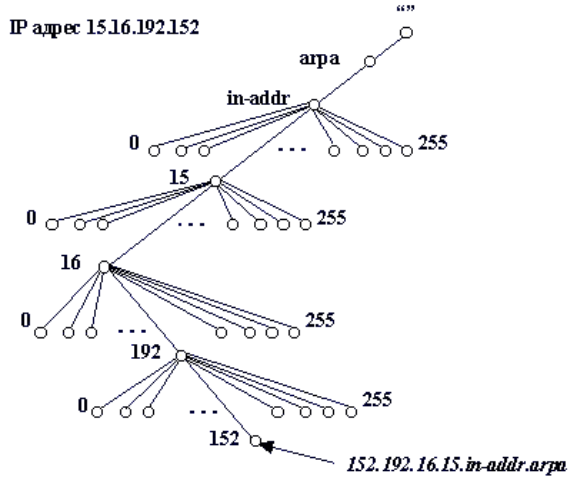

Рисунок 25. Схема структуры доменов для разрешения IP-адреса в доменное имя

Заметим, что когда читается доменное имя из домена in-addr.arpa, IP-адрес представляется в обратном порядке. Например, если хост openit.guap.ru имеет IP-адрес 194.226.199.152 , то соответствующий ему поддомен 199.226.194.in-addr.arpa. должен установить обратное соответствие между узлом 152 в этом поддомене и доменным именем openit.guap.ru. , которое должно храниться в обратной зоне как адрес. Это позволяет единообразно отвечать как на прямой запрос, так и на обратный (то есть искать имя по адресу).

Лабораторная работа № 2: Система доменного именования

Цель работы: изучить теорию и практику назначения IP–адресов, научится устанавливать и конфигурировать DHCP–сервер.

Задание на лабораторную работу

Выполнение лабораторной работы должно включать в себя следующие шаги.

1. С помощью программы Virtual Box создать виртуальную машину Windows Server. Если имеется шаблон этой машины, то сделайте себе копию.
2. Имя компьютера должно соответствовать имени Вашего отца. Должным образом сконфигурировать настройки протокола TCP/IP (IP-адрес взять по правилу 172. (16+N).M.K/24, где N – это последняя цифра из номера группы, M – номер вашего варианта (порядковый номер по журналу), K — длина Вашей фамилии;
3. Установить на этом сервере программное обеспечение для работы DNS-сервера.
4. Создать зону прямого просмотра. Имя зоны должно быть задано по правилу: family.gXXXX.local , где family — Ваша фамилия, XXXX - номер группы.
5. Создать зону обратного просмотра. Создать в зоне прямого просмотра три узла. Имена и адреса этих узлов следующие:

Name-1	172.16.M.N
Name-2	192.168.M.N*2
Name-3	10.44.M.N*3, здесь Name — это Ваше имя, а N —

длина Вашего имени.

6. Создать один узел вручную

MyMother 172.16.M.N и внести вручную в соответствующий зонный файл запись типа указатель для этого узла .

7. Проверить работу DNS-сервера с помощью утилиты nslookup. **Протестировать все имена и адреса, которые Вы занесли в зонные файлы.** В отчете привести скриншот, который бы демонстрировал правильную работу DNS-сервера.

Методические указания к выполнению работы

Прежде чем устанавливать DNS-сервер желательно должным образом настроить клиентскую часть. Для этого нужно выполнить следующее.

- Компьютер, на котором развертывается DNS, должен иметь статический IP-адрес.
- В качестве предпочитаемого DNS-сервера должен быть указан IP-адрес этого компьютера, т.е. он должен указывать на самого себя; поле альтернативного DNS сервера не заполнять.
- В имени компьютера нужно указать DNS-суффикс, который соответствует имени создаваемой зоны. Это необходимо для того, чтобы сервер отвечал не только на полное доменное имя, но и на сокращенное. Также это способствует корректной работе динамического обновления данных сервера (DDNS – Dynamic DNS).

Проделав все вышеперечисленные настройки и перезагрузив компьютер, можно приступать к установке и настройке DNS-сервера.

Порядок выполнения лабораторной работы

1. Создайте или импортируйте готовые виртуальные машины. Одна из них будет выступать в роли сервера, а вторая — в роли клиента. Сконфигурируйте обе виртуальные машины таким образом, чтобы их виртуальные сетевые адаптеры были подключены к одной и той же виртуальной сети. Это означает, что кадры данных (а значит и пакеты данных) будут существовать только в одной из виртуальных сетей, с которой мы работаем. К той же самой виртуальной сети нужно будет подключать и клиентскую виртуальную машину. Пусть это будет виртуальная сеть с именем Intnet.

2. Подготовьте свой виртуальный сервер для выполнения работы, для чего следует создать для него новые уникальный идентификатор и правильное доменное имя, а также присвоить ему IP-адрес.

3. Установите программное обеспечение DNS-сервера и сконфигурируйте зону прямого просмотра для Вашего домена. Это должна быть основная зона. При этом файл зоны создается в каталоге `%SystemRoot%\system32\dns` и его можно там посмотреть.

4. На запрос о разрешении динамического обновления на данном шаге лучше запретить обновления. В созданной зоне должно быть минимум две записи: запись SOA зоны и запись NS зоны. Также там может автоматически прописаться (если правильно настроена клиентская часть) и третья запись типа A с именем и IP-адресом самого сервера. На рисунке 26 приведено окно создания зоны

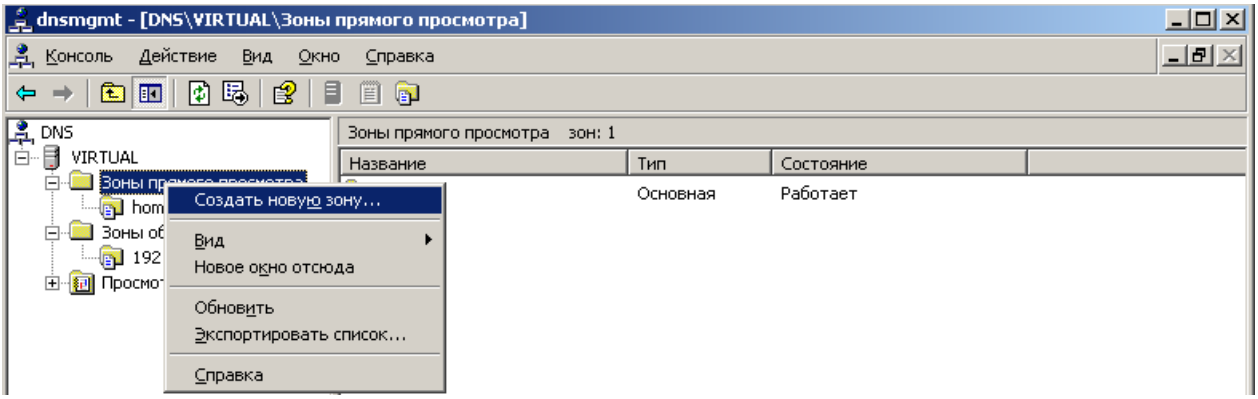

Рисунок 26. Создание зоны прямого просмотра

5. Далее создаем зону обратного просмотра. Выбираем в меню Создать новую зону, указываем что это основная зона. Далее указываем код ID нашей сети (первые три значения IP-адреса в прямом виде), имя зоны и имя файла зоны будет создано автоматически.

На запрос о разрешении динамического обновления на этом этапе выполнения лабораторной работы следует запретить обновления. Обязательно проверьте работу сервера при работе с обратными зонами. Для этого нужно после запуска утилиты nslookup в качестве вопроса задавать ip-адрес; в ответ мы должны получать правильное имя узла.

6. Оформите отчёт и защищайте работу.

Контрольные вопросы

1. Объясните основные принципы построения и работы системы доменного именования.
2. Что такое DNS сервер? Для чего он нужен?
3. Как формируется доменное имя? Что такое доменный суффикс? Какой длины может быть доменное имя?
4. Что такое зона? Чем зона отличается от домена?
5. Что такое primary masters DNS?
6. Что такое secondary masters DNS?
7. Объясните, как происходит преобразование доменного имени в IP-адрес.
8. Объясните, как происходит преобразование IP-адреса в доменное имя.
9. Как осуществляется разрешение доменного имени при рекурсивном режиме обработки запроса к DNS?
10. Как осуществляется разрешение доменного имени при итерационном режиме обработки запроса к DNS?
11. Расскажите о формате файлов конфигурации (dns-файлы).
12. Какие ресурсные записи в зонном файле Вы знаете? Расскажите о них подробнее.

Тема № 3: МАРШРУТИЗАЦИЯ

Краткие теоретические сведения

Сетевой (или межсетевой — InterNet) уровень позволяет передавать данные между любыми, произвольно связанными узлами сети. Реализация протокола сетевого уровня подразумевает наличие в сети специальных устройств — маршрутизаторов. Маршрутизаторы представляют собой либо специализированные сетевые вычислительные машины, либо

обычные компьютеры, но с несколькими сетевыми интерфейсами. В обоих случаях маршрутизация осуществляется за счет специального программного обеспечения, реализующего протоколы маршрутизации. Маршрутизаторы объединяют отдельные сети в общую составную сеть. К каждому маршрутизатору могут быть присоединены несколько сетей (по крайней мере две).

В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. Маршрутом называется путь, по которому пакеты пересылаются от отправителя к получателю. Задачу выбора маршрутов из нескольких возможных решают маршрутизаторы, а также конечные узлы. Помимо объединения сетей в большую составную сеть, маршрутизаторы могут использоваться для разделения сети на небольшие подсети с целью локализации общего трафика, обеспечивая в то же время возможность передачи данных между узлами из разных подсетей. Маршрут, выбираемый на узле, определяет не полный путь, а только сегмент пути от хоста до шлюза (или от шлюза до шлюза), который может переслать пакеты целевому хосту.

С другой стороны, маршрутом можно назвать последовательность маршрутизаторов, через которые должен пройти пакет от узла-отправителя до пункта назначения. Маршрутизатор, расположенный в текущей подсети, является для неё шлюзом, поскольку через него можно попасть в другие подсети. В подсети может быть более одного шлюза. Маршрутизаторы, расположенные в других подсетях, даже если они связаны друг с другом, не являются шлюзами для текущей сети и узлов, в ней расположенных. Маршрутизатор выбирает маршрут на основании своего представления о текущей конфигурации сети и соответствующего критерия выбора маршрута. Обычно в качестве критерия выступает время прохождения маршрута, которое в локальных сетях совпадает с длиной маршрута, измеряемой в количестве пройденных узлов маршрутизации (в глобальных сетях в расчет принимается еще и время передачи пакета по каждой линии связи, т. е. учитывается пропускная способность каналов передачи данных). Список возможных маршрутов хранится в таблице маршрутизации. Процедура выбора маршрута сначала находит все маршруты, соответствующие запросу, а потом выбирает маршрут с минимальной метрикой расстояния. При наличии нескольких маршрутов одинаковой длины выбирается тот маршрут, который задан наиболее точно. Если несколько маршрутов совпадают по обоим критериям, то эти маршруты применяются по-очереди. Описание маршрута содержит такую информацию, как список сетей, достижимых локальным хостом, и список шлюзов для отправки пакетов в удаленные сети. При получении дейтаграммы шлюз ищет в таблицах маршрутизации следующий узел ее маршрута до целевого хоста и отправляет дейтаграмму этому узлу.

Маршрутизация – важнейший процесс в IP-сетях. Чтобы некоторый узел мог найти в сети другой узел, должен быть определен механизм описания того, как осуществить передачу пакетов от произвольного узла к другому заданному узлу. Такой механизм и называется маршрутизацией. Маршрутизация выполняется специальными программными или аппаратно-программными средствами – маршрутизаторами. Маршрутизатор – это сетевое устройство, используемое в компьютерных сетях передачи данных, которое, на основании информации о топологии сети (таблицы маршрутизации) и определенных правил, принимает

решения о пересылке пакетов сетевого уровня их получателю. Маршрутизаторы выпускаются промышленностью, но можно сделать самодельный маршрутизатор, взяв для этой цели компьютер с по крайней мере двумя сетевыми адаптерами и установив на него соответствующее программное обеспечение. Маршрутизация, осуществляемая протоколом IP – это процесс поиска в таблице маршрутизации и определение интерфейса, куда будет послан пакет.

Существует два типа маршрутизации: статическая и динамическая. Статическая маршрутизация осуществляется на основе таблиц маршрутизации, задаваемых администратором. Динамическая маршрутизация организуется автоматически с помощью специальных протоколов, которые сначала собирают информацию об имеющихся маршрутизаторах и существующих между ними связях, а затем строят таблицы маршрутизации. Принцип их использования достаточно прост: маршрутизаторы с помощью устанавливаемого протоколом порядка рассылают определенную информацию из своей таблицы маршрутизации другим и корректируют свою таблицу на основе данных, полученных от других маршрутизаторов. Использование этих протоколов оправдано в случае сложной и часто изменяющейся топологии сети. Поэтому изучение динамической маршрутизации не входит в данную лабораторную работу.

Принцип статической маршрутизации

Как правило, маршрутизатор имеет несколько интерфейсов и одновременно находится в нескольких подсетях. Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Чтобы по адресу сети назначения можно было бы выбрать маршрут дальнейшей пересылки пакета, каждый узел, поддерживающий сетевой уровень, анализирует специальную информационную структуру, называемую таблицей маршрутизации. Простейшая таблица маршрутизации включает в себя информацию об узле (или сети) назначения, маске подсети для узла (сети) назначения, интерфейсе, через который следует направить пакет, и шлюзе – удаленном узле, которому будет передан пакет. Шлюзом называется маршрутизатор, находящийся в той же сети, что и узел, для которого указывается шлюз. Для выбора оптимального маршрута используется метрика. Пример таблицы маршрутизации приведен на рис. 27.

Прокомментируем таблицу маршрутизации, изображенную на этом рисунке. Она построена для сети из двух подсетей. Первая подсеть — это 10.44.7.0/24; к ней сервер, выполняющий функции маршрутизатора, подключен своим первым сетевым адаптером и IP-адрес этого адаптера равен 10.44.7.254/24. Через этот сетевой интерфейс выходят пакеты, адресованные в сеть 10.44.7.0/24 и пришедшие на маршрутизатор через вторую сетевую карту. Второй сетевой адаптер имеет адрес 172.20.7.254/24 и подключен к подсети 172.20.7.0/24. Если нужно добавить маршрут, то можно воспользоваться командой ROUTE ADD. Справку по использованию утилиты ROUTE можно получить по команде `ROUTE /?`

```
IPv4 таблица маршрута
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x10003 ...08 00 27 c1 19 f2 ...... AMD PCNET семейство PCI Ethernet адаптеров
0x10004 ...08 00 27 45 0e 15 ...... AMD PCNET семейство PCI Ethernet адаптеров #2
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
        10.44.7.0    255.255.255.0      10.44.7.254      10.44.7.254     20
      10.44.7.254  255.255.255.255        127.0.0.1        127.0.0.1     20
   10.255.255.255  255.255.255.255      10.44.7.254      10.44.7.254     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1     1
       172.20.7.0    255.255.255.0     172.20.7.254     172.20.7.254     20
     172.20.7.254  255.255.255.255        127.0.0.1        127.0.0.1     20
   172.20.255.255  255.255.255.255     172.20.7.254     172.20.7.254     20
        224.0.0.0        240.0.0.0      10.44.7.254      10.44.7.254     20
        224.0.0.0        240.0.0.0     172.20.7.254     172.20.7.254     20
  255.255.255.255  255.255.255.255      10.44.7.254      10.44.7.254      1
  255.255.255.255  255.255.255.255     172.20.7.254     172.20.7.254      1
===========================================================================
Постоянные маршруты:
  Отсутствует
```

Рис. 27 . Пример таблицы маршрутизации

Как только маршрутизатор (или любой узел сети, поддерживающем сетевой уровень модели TCP/IP) получает IP-пакет, выполняется следующая последовательность действий:

1. Маршрутизатор определяет, является ли узел-получатель пакета локальным (т.е. находится ли он в той же подсети, что и маршрутизатор). Если получатель находится в той же подсети, то пакет направляется ему напрямую.

2. Если узел-получатель находится в другой подсети, то просматривается таблица маршрутизации на предмет пути к этому узлу. При просмотре, сеть узла-получателя сравнивается с записями о сетях в таблице маршрутизации и при обнаружении совпадения пакет направляется маршрутизатору, указанному в соответствующей записи.

3. Если маршрут в таблице маршрутизации не найден, то пакет отправляется шлюзу по умолчанию, указанному на маршрутизаторе.

4. Если запись о шлюзе по умолчанию отсутствует, то пакет уничтожается. Для указания шлюза по умолчанию, в таблице существует специальная запись default. Запись default указывает, на какой узел должен быть направлен пакет, если совпадений его места назначения в таблице не найдено.

Для объединения подсетей в единую сеть в простейшем случае используется маршрутизация по умолчанию. Она организуется посредством шлюзов. Схема такой маршрутизации выглядит следующим образом: задан адрес шлюза по умолчанию. При попытке отправки пакета в сеть, узел проверяет совпадение подсети назначения пакета с подсетью узла. Если подсети разные, то пакет отправляется на шлюз. В простейшем случае, шлюз сравнивает сеть IP-адреса назначения с номерами сетей на своих интерфейсах и в

случае совпадения, направляет пакет узлу назначения через этот сетевой интерфейс. В противном случае он отправляет пакет узлу, указанному в качестве шлюза по умолчанию на самом шлюзе. Если такового нет, то пакет теряется.

Лабораторная работа № 3: Маршрутизация

Цель работы: изучить теорию и практику маршрутизации пакетов и построения маршрутизируемых IP-сетей.

Порядок выполнения лабораторной работы

В работе нужно последовательно выполнить 2 задания.

Задание № 1

Необходимо построить сеть из двух подсетей, соединенных с помощью маршрутизатора. В каждой подсети нужно разместить по узлу, в роли которых можно взять рабочую станцию с операционной системой Microsoft Windows Professional. Функцию маршрутизатора пусть выполняет компьютер с операционной системой Micosoft Windows Server; очевидно, что этот компьютер должен иметь минимум две сетевые карты. Обратите особое внимание на то, к каким виртуальным сетям будут подключены сетевые адаптеры виртуальных машин и постарайтесь не перепутать IP-адреса у этих адаптеров.

Первая подсеть должна определяться по правилу: 10.GG.N.0/24, где GG— это последние две цифры из номера Вашей группы, а N — это Ваш порядковый номер по журналу. Имя рабочей станции в первой подсети должно быть следующим: Name-1, где Name — это Ваше имя.

Вторая подсеть должна определяться по правилу: 172.16+G.N.0/24. Имя рабочей станции в этой подсети должно быть следующим: Name-2.

Имя сервера-маршрутизатора должно соответствовать имени Вашего отца. Поскольку по умолчанию маршрутизация отключена, ее нужно включить и настроить. Проще всего это сделать с помощью добавления роли маршрутизатора и сервера удаленного доступа и соответствующей настройки маршрутов. Помимо мастера конфигурирования можно воспользоваться утилитой ROUTE, которая работает в режиме командной строки; изучите эту утилиту. Хотя можно не использовать мастер конфигурирования сервера, а просто открыть оснастку управления службами и запустить маршрутизацию; настроить ее следует с помощью утилиты ROUTE.

Покажите в отчете, что с помощью утилиты PING пакеты ходят между рабочими станциями. Приведите в отчете таблицу маршрутизации и будьте готовы ее объяснить.

Задание № 2

Необходимо к построенной ранее сети (в рамках выполнения первого задания) из двух подсетей добавить третью подсеть, подсоединив ее ко второй подсети с помощью второго маршрутизатора. Имя этого второго маршрутизатора должно соответствовать имени Вашей матери. IP-адреса третьей сети должны соответствовать правилу: 192.168.N.0/24. Кроме

сервера-маршрутизатора разместите в этой третьей сети клиента с именем Name-3. Обратите внимание, что теперь в VirtualBox должны быть использованы три внутренних виртуальных сети. Настройте все сетевые интерфейсы и таблицы маршрутизации таким образом, чтобы было обеспечено прохождение эхо-пакетов между любыми виртуальными компьютерами в Вашей сети.

Помимо утилиты PING при настройке и проверке маршрутизации очень часто используют утилиту TRACERT. В операционных системах UNIX (Linux) вместо TRACERT используется команда (утилита) traceroute. Эта утилита позволяет проследить путь, который проходят пакеты в процессе достижения ими указанного хоста. Этот путь пролегает через маршрутизаторы (если сеть маршрутизируемая), и они перечисляются при выводе результатов . В процессе своего выполнения утилита TRACERT отправляет к удаленному хосту по протоколу ICMP специальные эхо-пакеты с различным уровнем жизни (параметр TTL — Time To Live). Первый пакет имеет TTL, равный единице, и с каждой новой отправкой следующего эхо-пакета его время жизни увеличивается на единицу. Принцип работы утилиты TRACERT основывается на том факте, что при прохождении через маршрутизатор пересылаемого пакета его TTL уменьшается на единицу. И когда время жизни пакета становится равным нулю, то отправителю посылается соответствующее сообщение. Утилита TRACERT получает эти сообщения и на их основании выводит информацию о пути следования пакета.

Многие считают, что основная польза этой утилиты заключается в определении маршрута. Не будем это оспаривать, но другим важным ее достоинством является то, что в ней по умолчанию указывается не IP-адрес удаленного узла, а его имя. Как правило, имя узла преобразуется в IP-адрес с помощью DNS-сервера. Если Вы правильно настроите не только маршрутизаторы, но и DNS-сервер, который в данной лабораторной работе должен быть размещён на первом маршрутизаторе, то можно будет проводить трассировку и «пингование», обращаясь к удаленным узлам по их именам.

Другим важным достоинством утилиты TRACERT является то, что она позволяет обнаружить участки задержки пакетов, а иногда и возможные потери пакетов, что помогает локализовать проблему и перейти к ее устранению.

Утилита имеет следующий формат:

```
tracert [-d] [-h maximum_hops] [-j host-list] 9-w timeout]
[-R] [-S srcaddr] [-4] [-6] target_name
```

Ключи и параметры в этой команде имеют следующее значение:

- -d — по умолчанию утилита, предоставляя информацию о проходимых пакетами маршрутизаторах, указывает не только IP-адреса, но и их доменные имена. Использование этого ключа предписывает утилите TRACERT не производить преобразование IP-адресов в доменные имена, что позволяет сократить время ее выполнения;
- -h maximus_hops — использование утилиты с данным ключом позволяет ограничить допустимое число переходов (maximus_hops)из одной сети в

другую в процессе отслеживания маршрута;

- -w timeout — ключ позволяет явно определить максимальное время ожидания ответа от удаленного маршрутизатора (параметр timeout, который задается в милисекундах);
- -R — этот ключ предписывает осуществлять трассировку пути по алгоритму Round Trip и действует только для стека протоколов TCP/IP v.6;
- -S — ключ, который тоже используется только для стека TCP/IP v.6 и указывает адрес источника пакетов;
- ключи -4 и -6 указывает версию стека протоколов;
- target_name — определяет имя удаленного хоста, маршрут к которому необходимо проследить.

Пример работы утилиты при выполнении лабораторной работы приведен на рисунке 28.

```
C:\Documents and Settings\Admin>tracert client-1

Трассировка маршрута к client-1.guap.local [10.44.7.1]
с максимальным числом прыжков 30:

  1     1 ms    <1 ms    <1 ms  route-2.guap.local
[192.168.7.254]
  2     1 ms     1 ms     1 ms  router-1.guap.local
[172.20.7.254]
  3     2 ms     1 ms     1 ms  client-1.guap.local
[10.44.7.1]

Трассировка завершена.

C:\Documents and Settings\Admin>
```

Рисунок 28. Пример работы утилиты TRACERT

В отчете по лабораторной работе приведите схемы маршрутизируемой сети с IP-адресами узлов и маршрутизаторов, их именами, и все необходимые скриншоты от утилит PING и TRACERT, которые будут демонстрировать работоспособность маршрутизаторов и правильную настройку сервера DNS. Кроме этого приведите таблицы маршрутизации.

Контрольные вопросы

1. Что такое шлюз? Для чего он нужен?
2. Объясните основной принцип разделения сетей на подсети.
3. Как можно объединить две сети? Как можно объединить две подсети?
4. Какой маршрутизатор называют шлюзом?
5. Что такое шлюз по умолчанию? Для чего он нужен?

6. Расскажите про возможности утилиты ROUTE.
7. Объясните механизм статической маршрутизации.

Тема № 4: **ФУНКЦИОНИРОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ И ИХ МОДЕЛИРОВАНИЕ**

Принципы работы вычислительных сетей заключаются в том, что компьютеры и, соответственно, программы, работающие в них, могут связываться друг с другом с помощью специальных устройств ввода-вывода и соответствующего программного обеспечения. Эти устройства, называемые сетевыми адаптерами или сетевыми картами[5], являются внешними по отношению к центральной части компьютера, скорость их работы на несколько порядков меньше, чем работа центральной части. Но зато они могут передавать данные на существенно большее расстояние, чем между основными компонентами, расположенными в компьютере. Сетевые адаптеры могут прочитать данные из оперативной памяти компьютера и послать их по среде передачи данных другому сетевому устройству или компьютеру, у которого тоже есть сетевой адаптер. Сетевой адаптер, подключенный к среде передачи данных, принимает их и отправляет в оперативную память другого компьютера.

Различают проводные (кабельные) среды передачи данных и беспроводные (с использованием волновых принципов; прежде всего — радиоволн). В любом случае сигналы по общей среде передачи данных могут проходить без существенных искажений только в том случае, если они идут от одного передатчика и никакие другие сигналы от других сетевых устройств не искажают друг друга. Естественно, что имеет место быть явление затухания сигналов, поэтому они распространяются на ограниченные расстояния. Главным способом избежать искажения передаваемых сигналов, а значит и данных, которые эти сигналы передают по среде, является разделение этой среды во времени между абонентами. Хотя в ряде случаев идут на создание двух сред: по одной среде сигналы идут от первого абонента ко второму, а по другой — в обратную сторону. В этом случае говорят о дуплексной связи. В любом случае протяженность распространения сигналов, даже если обеспечить им монопольное предоставление, ограничена и для увеличения дальности передачи данных используют специальные технические средства; обычно их называют повторителями (репитерами — repeater). Репитеры принимают данные, а затем передают их дальше. В случае обнаружения ошибок в порции принятых данных (эту последовательность передаваемых битов называют кадром) репитер запрашивает данные повторно. В настоящее время при подключении к одной общей среде передачи данных (к так называемой сетевой инфраструктуре) множества абонентов - компьютеров с сетевыми адаптеров - в роли репитеров используют так называемые коммутаторы. Это устройства, к которым подключаются компьютеры и иные сетевые устройства, каждый своим кабелем.

Локальные сети, с которыми мы чаще всего сталкиваемся при использовании различных вычислительных систем, характеризуются тем, что они объединяют вместе компьютеры, расположенные относительно недалеко друг от друга. Это могут быть

5 Сетевые карты остались в основном в прошлом. Это были дополнительные устройства, вставляемые в один из слотов материнской платы. В настоящее время сетевые адаптеры распаиваются на материнскую плату, а часть этого адаптера входит в контроллер вводы-вывода (Input-Output Controller Hub).

компьютеры, находящиеся от нескольких десятков метров до нескольких километров. В последнем случае обычно используют оптоволоконные соединения или беспроводные технологии. Благодаря этому в локальных сетях применяются такие сетевые технологии, которые могут обеспечить достаточно большие скорости передачи данных. Чаще всего в них используют кабельные соединения, хотя в последние годы многие мобильные устройства, в том числе и ноутбуки, подключаются к сети посредством беспроводных соединений. Для знакомства с такими технологиями можно воспользоваться специально для этого разработанными программами моделирования сетей. Одной из таких программ является NetEmul, разработанная студентами нашего университета Павлом Семёновым и Анастасией Омилаевой. Программа NetEmul была создана ими для визуализации работы компьютерных сетей, для облегчения понимания происходящих в ней процессов. Программа NetEmul свободно распространяется по лицензии GPL. Также следует отметить, что она является кросс-платформенной и свободно может быть использована в операционных системах Windows, Linux и MacOS.

NetEmul - это программа для моделирования локальных вычислительных сетей, причем работающих по принципам Ethernet. Эта сетевая технология использует идею разделения среды передачи данных случайным образом и её связывают с методом CSMA/CD — Carrier Sence Multiple Access with Collision Detection, т. е. множественный случайный доступ с прослушиванием несущей частоты и обнаружением коллизий. Этот метод оказался относительно несложным для технической реализации, но достаточно эффективным при небольшом количестве сетевых устройств, подключённых к среде передачи данных. Основная среда передачи данных в настоящее время — это медные кабели типа «витая пара», оптоволоконные кабели и беспроводные технологии типа Wi-Fi [ ]. Для кабельных сетей используется топология типа «звезда». Отдельные кабели присоединяют сетевые адаптеры компьютеров к концентраторам или коммутаторам. Кстати, коммутаторы можно присоединять к другим коммутаторам и получать достаточно разветвленные соединения. Коммутаторы — это более сложные устройства нежели концентраторы. Если концентратор получает от сетевой карты порцию данных (напомним, что эту порцию называют кадром, она представляет собой множество информационных битов, у которых есть заголовок, описывающий кадр и указывающий адреса отправителя и получателя, и контрольная сумма, позволяющая обнаруживать искажения в полученной последовательности битов), то он передаёт этот кадр на все кабели, подключённые к нему. В отличие от концентратора, коммутатор запоминает адреса отправителей и со временем отправляет принятые кадры не всем устройствам, а только получателю. Это существенно снижает уровень коллизий, время от времени возникающих в среде из-за случайной природы посылки кадров сетевыми устройствами.

Помимо компьютеров с сетевыми адаптерами, концентраторов и коммутаторов программа NetEmul позволяет представить в модели вычислительной сети такие сложные сетевые устройства как маршрутизаторы. Все эти устройства могут иметь по несколько разъёмов, к которым могут быть присоединены виртуальные кабели, поэтому построение модели сети заключается в выборе нужных устройств, размещении их на плоскости создаваемой модели, и в связывании компонентов сети соединениями. После чего можно задать параметры сетевых устройств и наблюдать за функционированием созданной модели.

С помощью программы NetEmul можно не только наглядно увидеть как функционируют построенные Вами сети, но и протестировать их. Задав все необходимые параметры "смонтированному" вами сетевому оборудованию, можно проверить и своими глазами увидеть работу сети. Можно сказать, что эта программа открывает широкие возможности для экспериментов и их наглядного отображения. Помимо изучения основ функционирования локальных вычислительных сетей, её можно использовать и для выполнения некоторых лабораторных работ, и прежде всего — для закрепления знаний о маршрутизации.

Можно сказать, что эта программа затрагивает только канальный и сетевой уровни модели взаимодействия открытых систем OSI (Open System Interconnection). Это, соответственно, 2-й и 3-й уровни упомянутой семиуровневой модели OSI. А если взять стек TCP/IP, то это уже относится к 4-ому и 3-ему уровням [. Уровни приложений (7-й), представления данных (6-й), сеансовый (5-й) и транспортный (4-й) здесь не рассматриваются. Хотя при моделировании есть возможность указать какой из протоколов транспортного уровня стека TCP/IP будет использоваться — TCP или UDP ? Оба эти протокола относятся ко второму уровню модели TCP/IP, т. е. к транспортному.

Программа NetEmul имеет встроенное руководство, поэтому описывать работу с ней здесь не будем.

Лабораторная работа № 4: Моделирование маршрутизируемой сети

Цель работы: изучить программу NetEmul для моделирования вычислительных сетей и получить навыки построения маршрутизируемых IP-сетей.

Порядок выполнения лабораторной работы

1. Взять второе задание из предыдущей лабораторной работы согласно своему варианту и построить модель своей сети в программе NetEmul. Сделайте скриншот этой модели, он должен выглядеть подобно тому, как это показано на рисунке 29 . В этой сети в итоге мы должны иметь два маршрутизатора (с двумя сетевыми адаптерами каждый) и три компьютера, размещенных в своих сетях и подключенных к маршрутизаторам через коммутаторы.

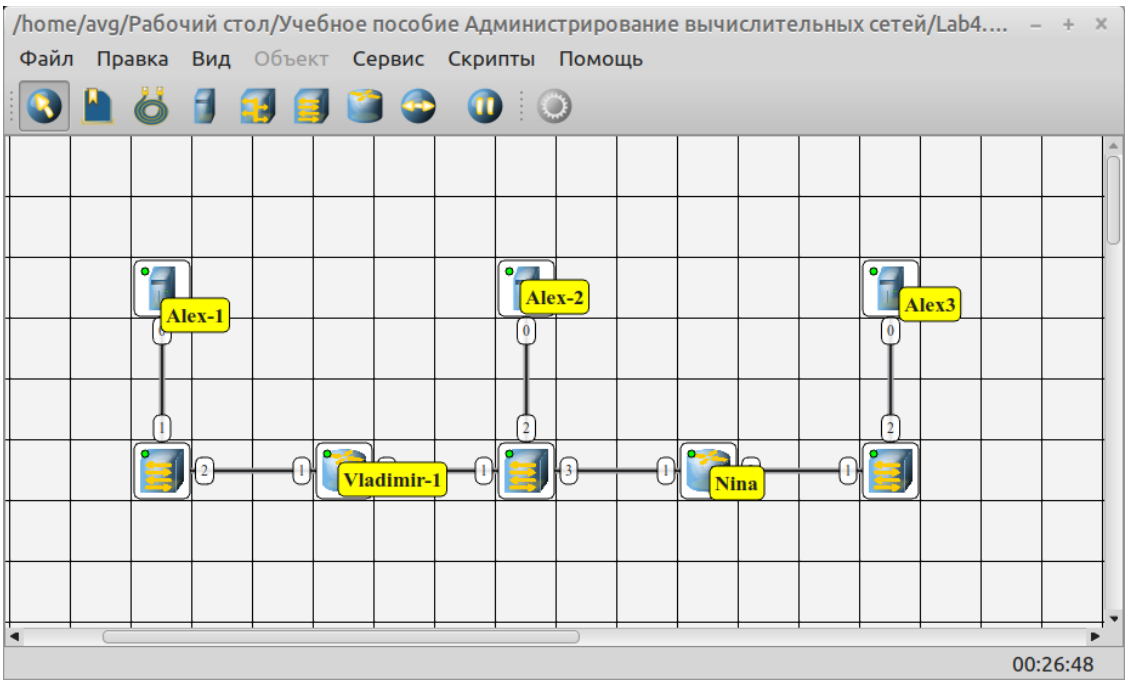

Рисунок 29. Модель маршрутизируемой сети.

2. Задайте все необходимые IP-адреса. Задайте маршруты движения пакетов. Для большего удобства можно IP-адреса вывести в качестве комментариев.

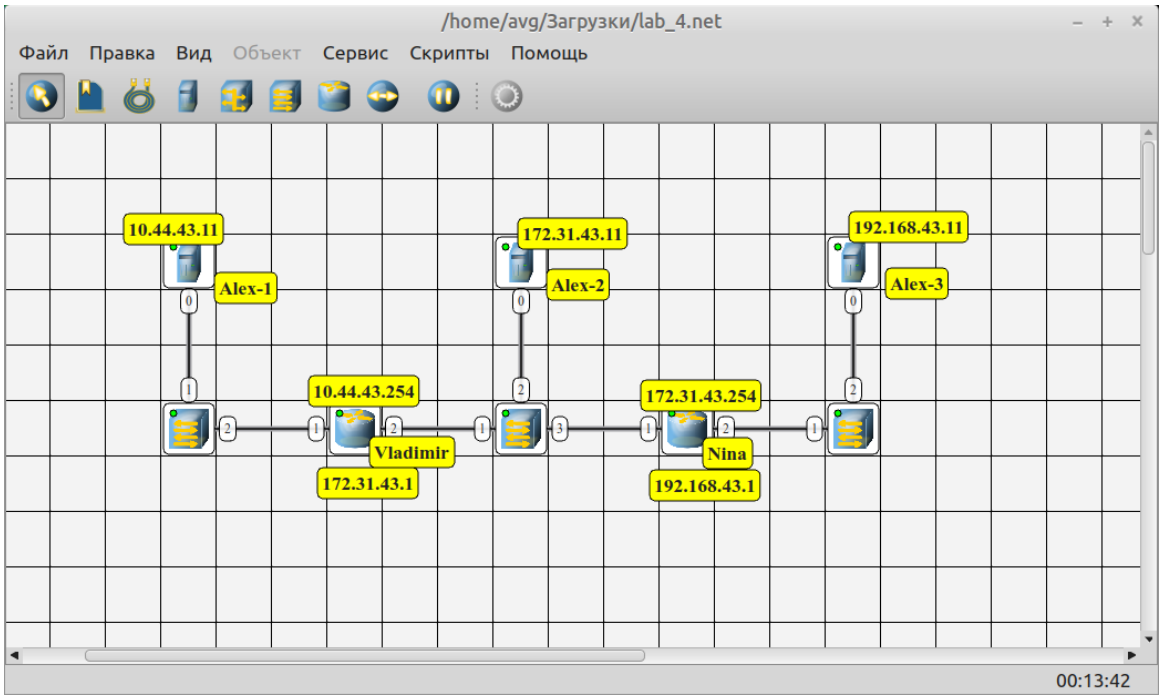

Рисунок 30. Комментарии на схеме создаваемой модели сети

Проверяем работоспособность сети, выбрав параметр «Send data», тип пакетов – UDP, далее выбираем отправителя и получателя данных.

Помимо визуализации процесс передачи пакетов отражается в журнале. Для его просмотра достаточно по правой кнопке мыши на выбранном компьютере (или маршрутизаторе) выбрать пункт «Показать журнал». Например, при передаче данных от

хоста с IP-адресом 192.168.43.11 к хосту с IP-адресом 172.31.43.11 в журнале маршрутизатора формируются записи, отраженные на рисунке 31. Так как хост-получатель находится в другой сети, сначала хост-отправитель, отправляя ARP-запрос, ищет маршрутизатор, через который передача данных становится возможна. Получив ARP-ответ от маршрутизатора, хост отправляет пакет – запрос на соединение (установлен флаг SYN), затем получает ответ «соединение установлено» (флаг SYN, ACK), после чего отправляется пакет – подтверждение (флаг ACK), затем хост начинает передачу данных.

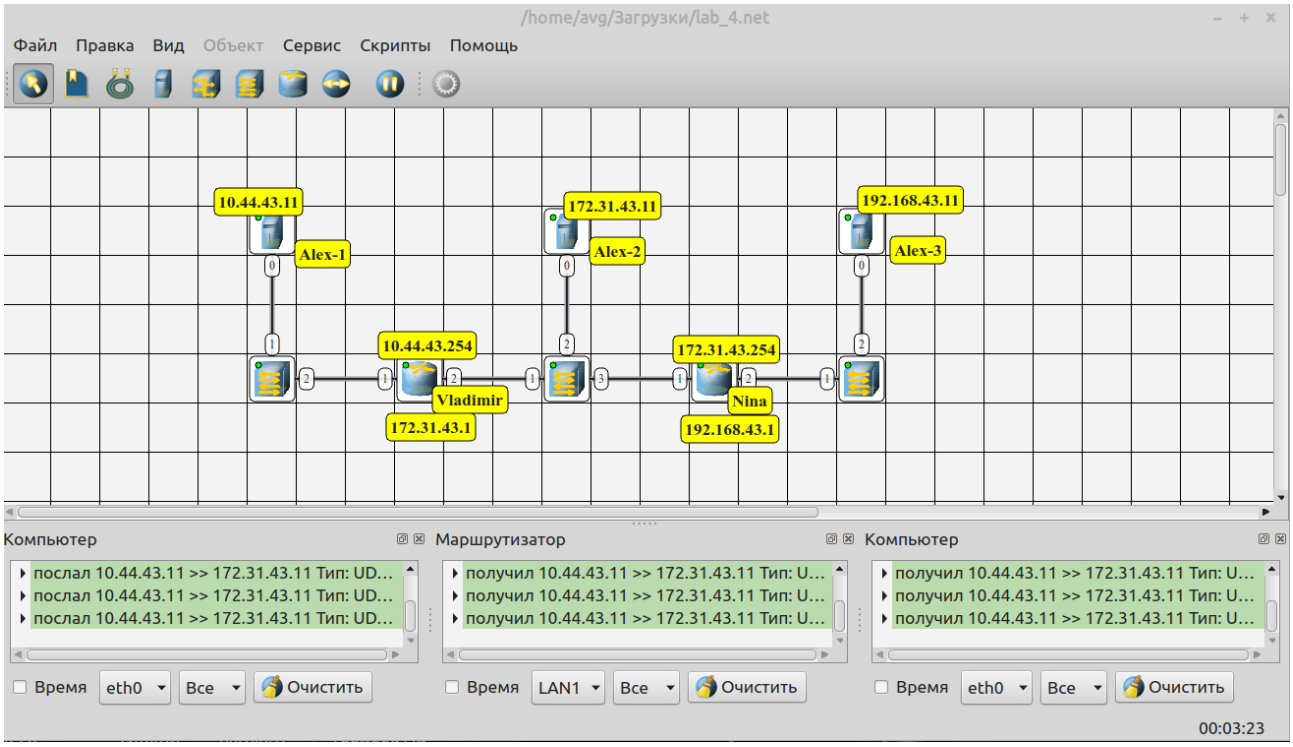

Рисунок 31. Работа созданной модели маршрутизируемой сети

Итогом правильно настроенной сети является сеть, в которой доступны для приема и передачи данных все рабочие станции.

3. Приведите в отчете скриншоты или содержимое просмотренного журнала и включите в него соответствующие пояснения.

Тема № 5: **СЛУЖБА УДАЛЕННЫХ РАБОЧИХ СТОЛОВ**

Краткие теоретические сведения

Выполнение вычислений непосредственно на компьютере пользователя при условии доступа к обрабатываемым файлам когда они находятся на сервере, как правило, приводит к достаточно большому трафику. Во-вторых, к компьютеру пользователя порой должны быть предъявлены достаточно серьёзные требования по производительности, поскольку приложения могут быть ресурсоёмкими. Наконец, на каждом пользовательском компьютере, на котором выполняются приложения, должны быть лицензии для использования этих приложений. Эти приложения должны быть соответствующим образом установлены, время от времени их нужно обновлять, что приводит к ощутимым затратам на администрирование. Альтернативой такому использованию выступает подход, при котором приложения выполняются не на пользовательских компьютерах, а на специальных серверах (возможно, что даже на тех же, где хранятся необходимые для них файлы чтобы минимизировать сетевой трафик и ускорить время доступа к файлам). А для управления приложениями пользователю на его дисплей передаётся с сервера окно приложения или даже весь «рабочий стол». Сервер, на котором выполняется приложение, позволяет запускать и исполнять удалённые от пользователя приложения, инициированные с клиентской машины. При этом приложения выполняются непосредственно на сервере, а на клиентскую машину передаются либо только результаты вычислений, либо, если вычисления осуществляются в диалоговом режиме, на дисплее отображается процесс вычислений. Всё управление вычислениями, происходящими на сервере приложений, осуществляется с машины-клиента. При правильной организации таких вычислений это позволяет сократить объём трафика. А главное — снизить затраты на компьютеры пользователей, затраты на лицензирование и на администрирование.

Наиболее известное программное обеспечение, предназначенное для организации сервера приложений, было разработано компанией Citrix Inc. Она называет свой сервер приложений терминальным сервером, поскольку клиентская машина в этом случае выступает в роли терминала. Вначале это были простые алфавитно-цифровые терминалы, а затем они стали поддерживать полноценный графический режим. Компания Citrix разработала несколько версий своего терминального сервера и соответствующих клиентов. Имеются варианты и для платформы Microsoft Windows, и для UNIX-систем, в том числе и для Linux. В девяностые годы компания Microsoft приобрела у компании Citrix лицензии на включение их программного обеспечения в состав дистрибутива своих серверных операционных систем класса NT и так же стала называть свои серверы приложений терминальными серверами. В последнее время службу терминального сервера (Windows Terminal Service — WTS) стали называть службой удалённых рабочих столов (Remote Desktop Service - RDS).

Итак, Terminal Service позволяет нескольким клиентам обращаться к приложениям, работа которых полностью происходит на терминальном сервере. Между сервером и клиентом передаются только экранные данные и события клавиатуры или мыши. Приложение, с помощью которого клиент может работать с терминальным сервером, сейчас называется «Подключение к удалённому рабочему столу» и представлено файлом mstsc.exe (Microsoft Terminal Services Client), см. рисунок 32 .

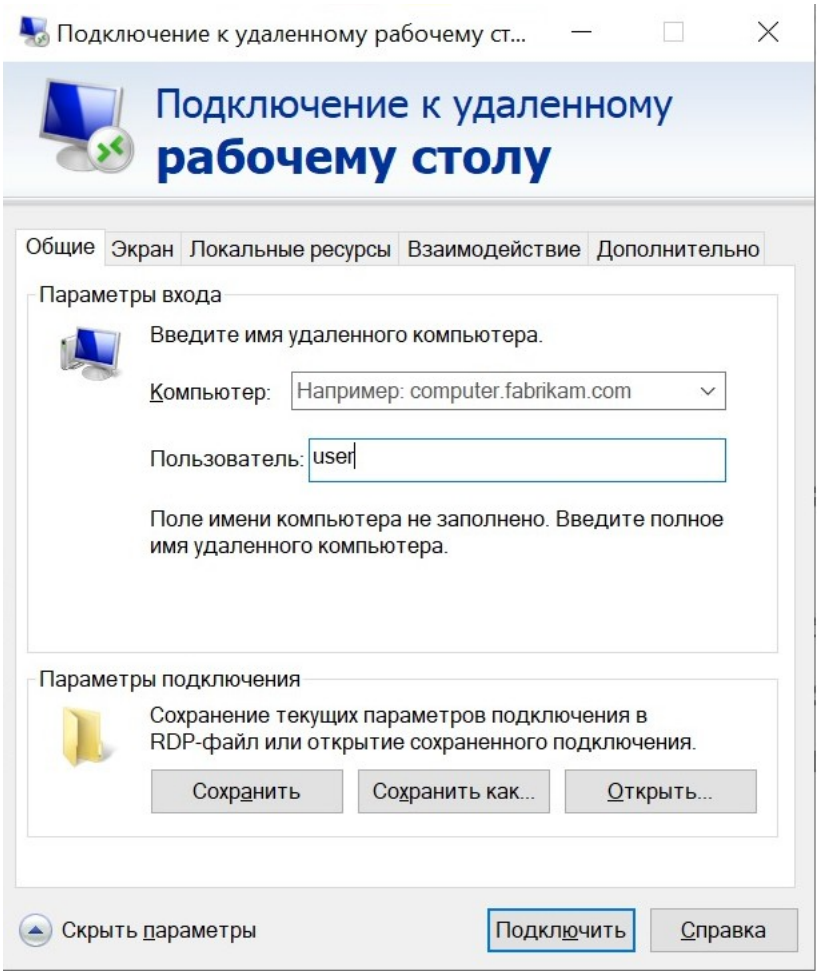

Рисунок 32. Главное окно клиента подключения к удаленному рабочему столу

Помимо штатных средств удаленного доступа к рабочему столу имеется несколько других программных решений. Среди наиболее популярных можно назвать такие как AnyDesk от компании AnyDesk Software GmbH и TeamViewer от компании TeamViewer GmbH [5, 6]. Обе программы предполагают, что они должны быть установлены как на компьютере, который будет выступать в роли сервера, так и на компьютерах, которые будут выступать в роли клиента. Наиболее интересным и важным свойством этих средств является их кроссплатформенность

Рассмотрим подробнее штатную службу терминального сервера, которую предоставляет компания Microsoft в своих операционных системах Windows. Внешние данные (экранная графика, данные, поступающие от пользователя) передаются между сервером терминальных служб и клиентом с помощью протокола RDP (Remote Desktop Protokol), который, в свою очередь, использует стек протоколов TCP/IP. Remote Desktop Protocol (RDP) — протокол удалённого рабочего стола — это протокол для служб распределенного представления, управляющий передачей экранных данных и данных, вводимых пользователем, между клиентом и сервером терминальных служб.

Windows Terminal Service в Windows 2000 поддерживала протокол RDP версии 5.0. В Windows Server 2003 основным стал протокол RDP 5.2, в Windows Server 2008 использовался RDP 6.1, а в Windoows Server 2012 уже используется протокол версии 8. С каждой новой версией увеличиваются возможности по передаче не только качественной

графики, но и по передаче на сервер ресурсов, доступных пользователю при такой удалённой работе.

Передачу данных RDP между сервером и клиентом можно разделить на три основных этапа:

• передача графической информации от сервера клиенту;

• передача данных от мыши и клавиатуры клиента на сервер;

• передача данных от подключённых к компьютеру пользователя устройств, т. е. их виртуализация на удалённом сервере.

Каждый сеанс подключения пользователя Terminal Server, который осуществляется с помощью специального приложения mstsc.exe[6], работает совершенно независимо от других. Память и другие ресурсы, выделенные одному сеансу, недоступны для других. Можно сказать, что для удаленных вычислений на терминальном сервере создается своеобразная виртуальная машина, причем никакие ресурсы нескольких виртуальных машин не пересекаются. С целью обеспечения такого режима предоставления ресурсов для клиентов терминального сервера даже установка приложений осуществляется иначе. Установку приложений на терминальном сервере следует осуществлять через апплет Установка и удаление программ, либо можно воспользоваться командой CHANGE USER. По команде CHANGE USER /INSTALL система переводится в режим установки программных продуктов, а по команде CHANGE USER /EXECUTE – в режим выполнения приложений. Правильно установленные на терминальном сервере приложения становятся реентерабельными, т. е. код приложения размещается при запуске первого процесса в единственном экземпляре и далее разделяется между другими процессами, выполняющими ту же самую программу. При этом каждый процесс выполнения такой реентерабельной программы имеет свои собственные, не разделяемые ни с каким другим процессом, данные. Если же запускать на терминальном сервере приложения, которые были на нём установлены до перевода сервера в режим терминального сервера, то они не будут реентерабельными и запуск нескольких процессов с таким кодом уже не будет выполняться корректно. Заметим, что на создание одного сеанса выделяется минимум 20 МБ оперативной памяти; обычно выделяется больше памяти, т. к. в этом сеансе запускаются приложения и порой они требуют существенные ресурсы.

В Windows 2000 Server было два режима использования Terminal Services:

- ***Режим сервера приложений*** (*Application Server Mode*) с классическими функциями Terminal Services. В режиме сервера приложений планировщик задач операционной системы выделяет больше процессорного времени на взаимодействие с пользователем и на выполнение активных задачам. В этом режиме приложения, предназначенные для использования клиентами, устанавливаются особым образом, чтобы обеспечить изолирование виртуальных машин, запускаемых от имени клиента, и корректное исполнение кода в каждом из вычислительных процессов. Очевидно, что ресурсы, необходимые для организации одного сеанса работы прежде всего зависят от приложений. Однако из практики можно сказать, что в среднем на одну виртуальную

6 mstsc — MicroSoft Terminal Services Client

машину, выполняющую вычисления для клиента сервера терминалов необходимо около 60-80 Мбайт оперативной памяти.

- Специальный режим управления, называемый ***режимом удаленного администрирования*** (*Remote Administration Mode*). В этом режиме только члены группы Администраторы могут подключиться к серверу терминалов, причем поддерживается не более двух сеансов. В режиме удаленного администрирования планировщик задач операционной системы выделяет больше времени на выполнение фоновых процессов. Для работы с Terminal Server в режиме удаленного администрирования не требуется специальных лицензий, в отличие от режима сервера приложений.

Начиная с Windows Server 2003, эти режимы в явном виде не упоминаются, но по факту при установке программного обеспечения службы терминального сервера (эта служба установлена на сервер изначально, но работает только в режиме удалённого администрирования) сервер переводится в режим терминального сервера. В последнее время установка этих служб осуществляется с помощью специального мастера (Wizard) «Управление данным сервером» посредством добавления ролей. В Windows Server 2003 это называется «Сервер терминалов». А в Windows Server 2008 та же технология стала называться по имени основного используемого протокола, т. е. «Служба удалённого рабочего стола».

В Windows 2008 помимо уже названных средств появились новые службы. Это Узел виртуализации удаленных рабочих столов (Remote Desktop Virtualization Host), который работает в сочетании со штатным сервером Hyper-V. Последний обеспечивает возможность на одном компьютере одновременно запускать несколько виртуальных машин, часть или все из которых могут работать как сервер удаленного рабочего стола. Кроме этого, появился так называемый Шлюз удаленных рабочих столов (Remote Desktop Gateway). Это служба, которая позволяет обращаться к сервису удаленных рабочих столов удаленно, через брендмауэр, который по умолчанию блокирует такие соединения из соображений безопасности. При этом не важно — служба удаленного рабочего стола работает на виртуальном сервере или на реальном. Клиенту важно получить обслуживание и не он решает какой из конкретных серверов его обслуживает. Такой трафик проходит через SSL-ретрансляцию, т. е. через виртуальную частную сеть. Другими словами, для передачи трафика RDP шлюз RD применяеттуннель HTTP Secure Sockets Layer/Transport Layer Security (SSL/TSL). Соответственно, используется механизм сертификации и в сети должен быть сервис сертификации, который должен работать на клиентов, выдавая им доверенные сертификаты. Для успешной работы этой технологии администратор сети должен обеспечить следующие дополнительные требования:

- Должна быть установлена служба удаленного вызова процедур через HTTP Proxy (Remote Procedure Call over HTTP Proxy.
- Для успешного функционирования RPC over HTTP Proxy должен быть установлен и запущен Web-Server Internet Information Services.
- На сервере, выполняющем роль шлюза RD должна быть установлена и сконфигурирована служба сетевых политик (Network Policy Server.

Важно отметить, что для полноценного использования службы удаленного рабочего стола необходимо приобретать дополнительные лицензии. Бесплатно она может использоваться только в режиме удаленного администрирования. Однако для изучения этой службы можно воспользоваться тем, что компания Microsoft допускает ее использование в тестовом режиме (в течение 90 дней), что снимает проблему в рамках учебного процесса.

При работе с сервером терминалов у пользователя имеется возможность завершить сеанс или отключиться от сеанса. Для завершения работы в сеансе Terminal Server меню Start системы Windows содержит команды:

• Logoff (Завершение сеанса);

• Disconnect (Отключение сеанса);

• Shutdown (Завершение работы);

• Restart (Перезагрузка компьютера).

Список операций зависит от прав пользователя. Обычным пользователям доступны только операции Logoff и Disconnect. Администраторы и члены группы Power Users получают доступ к операциям Shutdown и Restart.

Команда Disconnect позволяет пользователю разорвать подключение к серверу терминальных служб, оставив активным сеанс на сервере, пока не возникнет одно из следующих событий:

• Пользователь заново регистрируется на этом же сервере терминальных

служб и при этом автоматически подключается к прерванному сеансу.

• Истечет время ожидания для отключенных сеансов. Тогда сервер автоматически завершит сеанс.

• Администратор вручную завершит сеанс.

Команда Disconnect полезна в процессе регистрации в Terminal Server при удаленном доступе к сети. Если период ожидания выбран с расчетом на это, вы можете запустить программу на сервере терминальных служб, отключиться, а позже вернуться и проверить результат. Поддерживать подключение к серверу не нужно: процесс все равно завершится успешно.

Недостаток команды Disconnect заключается в том, что многие пользователи не понимают разницы между завершением сеанса и отключением от сервера. Многие заканчивают работу, используя команду Disconnect вместо Logoff. Если период ожидания выбран неправильно, на сервере терминальных служб может остаться много отключенных сеансов, отнимающих ресурсы, которые могли бы использоваться активными пользователями. Нужно следить, чтобы период ожидания позволял исключить лишние отключенные сеансы. Следует отметить, что если просто закрыть окно сеанса работы с сервером приложений, то это как раз и означает отключение сеанса. Виртуальная машина при отключении от сеанса продолжает функционировать и потреблять соответствующие ресурсы.

В операционных системах GNU/Linux тоже есть клиенты удаленного рабочего стола, т. е. имеется возможность выполнять приложения не на своем компьютере с ОС Linux, а с помощью специального клиентского приложения через RDP попасть на компьютер с установленной на него службой удаленного рабочего стола. В случае удаленного запуска приложений на Linux-системах необходимости использовать RDP уже нет, т. к. для Linux можно воспользоваться возможностями X-Window. Напомним, что X-Window — это клиент-серверная технология организации графического режима работы (графического интерфейса). На компьютере с X-Window работают одновременно и клиент, и сервер. Поскольку X-клиент может быть запущен на другом компьютере, то мы автоматически получаем возможность работать с удаленным рабочим столом. Поэтому для работы с удаленной системой Linux достаточно через ssh (Secure Shell) , который обеспечивает безопасное соединение и шифрование передаваемых данных, запустить графический режим. Например, после ввода через интерфейс командной строки команды `ssh -XCA user@server` , где user — это Ваш логин на удаленном компьютере, а server — это имя компьютера-сервера[7], дать команду `startx`, то Вы получите рабочий стол сервера. Правда, тут есть несколько нюансов. Так, если на сервере и на клиентском компьютерах работает графический менеджер окон Xfce, то запускать нужно именно его; в этом случае графический режим будет работать наиболее корректно.

Лабораторная работа № 5 Служба удаленных рабочих столов

Цель работы: изучить службу удаленных рабочих столов и получить начальные умения по ее администрированию.

Для управления службой удаленного рабочего стола имеются специальные средства. Прежде всего, это соответствующие оснастки (snap-in) — Terminal Services Manager (Диспетчер служб терминалов) и Terminal Services Configuration (Настройка служб терминалов). При выполнении лабораторной работы вам необходимо будет освоить оба эти средства. Остальные инструменты нужны в случае использования таких служб как RD Gateway, RD Virtual Host, и другие. Так же надо знать, что для работы в сеансе удаленного рабочего стола у пользователя должны быть соответствующие права. Лучше всего их получить за счет того, что администратор добавит Вашу учетную запись в специальную Группу пользователей удаленного рабочего стола. Необходимо отметить, что права пользователей определяются членством во встроенных локальных группах. После установки на сервер службы удаленного рабочего стола на нем появляется локальная группа Пользователи удаленного рабочего стола, а в свойствах учетной записи пользователя на таком сервере появляются новые вкладки с параметрами, определяющими работу в сеансе на этом сервере. Речь идет о вкладках «Сеансы» - устанавливает параметры таймаутов и переподключения, «Среда» - определяет приложение, которое запускается при открытии сеанса, «Удаленное управление» - разрешает или запрещает доступ к сеансу работы пользователя и взаимодействие с ним. Эти же вкладки доступны через оснастку Terminal Services Configuration, но здесь они конфигурируют общие свойства, т. е. они распространяются на всех, кто зашел на сервер через RDP и использует службу RDS. А в

7 Можно указать вместо имени сервера его IP-адрес, например `ssh -XCA user@10.22.7.103`

учетной записи пользователя они касаются только конкретного пользователя. Имейте это ввиду при выполнении своего варианта работы.

Порядок выполнения лабораторной работы и варианты заданий

1. Установить на виртуальной машине (сервере) службу терминального сервера. Имя этого сервера должно соответствовать Вашему имени. IP-адрес этой машины должен быть назначен согласно правилу:

172.(16+N).M.K /24,

где N - это последняя цифра из номера группы;

M – ваш порядковый номер по журналу;

K – длина Вашей фамилии.

Клиентом для этого сервера должна быть виртуальная машина с IP-адресом 172.(16+N).M.(100+K) /24.

2. Создать на сервере терминалов две учетные записи (с именем Вашего отца и Вашей матери), включить их в группу Пользователи удаленного рабочего стола.

Установить на сервере терминалов какую-нибудь программу, которой нет на клиентской машине.

3. Сконфигурировать свойства клиентского приложения mstsclient таким образом, чтобы при его запуске запускалось установленное Вами на сервере терминалов приложение и сохранить эти настройки, создав ярлык этого приложения на рабочих столах созданных пользователей на клиентской машине. Проверить работу программы.

4. В свойствах учетных записей сделайте такие настройки, чтобы для одной из них можно было наблюдать за действиями пользователя на сервере терминалов, а для другой — можно было бы управлять его работой в сеансе. Покажите это преподавателю.

Контрольные вопросы

1. Расскажите о назначении службы терминального сервера.
2. Какие дополнительные новые службы появились в системах Windows для расширения потенциала службы Windows Terminal Service?
3. В каких режимах может работать Terminal Server ? Объясните различия в этих режимах.
4. Могут ли пользователи домена получить доступ к Terminal Server ?
5. Поясните принцип работы службы терминалов.
6. Что означает понятие «Удаленное управление» ? Как оно реализуется?
7. Чем отличаются завершение сеанса от отключения сеанса (команды Shutdown и Disconnect) ?
8. На что влияет параметр «ограничение на продолжительность сессии» ?
9. На что влияет параметр «ограничение на неактивность» ?
10. Почему приложения на терминальном сервере должны устанавливаться после включения службы терминального сервера?

Тема № 6: **ОДНОРАНГОВЫЕ И КОРПОРАТИВНЫЕ СЕТИ. УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ И ОБЩИЙ ДОСТУП К ФАЙЛАМ**

Краткие теоретические сведения

В самом общем случае для организации сетевого взаимодействия на разных компьютерах (платформах) необходимо обеспечить трансляцию запросов от приложений к платформе таким образом, чтобы эти запросы были правильно поняты и выполнены на другом компьютере. Напомним, что приложения создаются для выполнения на определенной платформе и что под платформой мы понимаем вычислительную систему как совокупность аппаратного и системного программного обеспечения, которая создаёт так называемую операционную среду [4]. Приложения выполняются в этой среде и взаимодействие между приложением и операционной средой осуществляется через соответствующий интерфейс, называемый Application Program Interface (API) — интерфейс прикладного программиста. Поскольку платформы могут быть разными, то для для организации взаимодействия между ними системный запрос на API одной платформы (обозначим его как API_1) должен быть сначала преобразован в некий сетевой API (NetAPI), который может быть правильно интерпретирован на другой платформе, связанной с первой через сетевое соединение, и потому может быть преобразован в запрос на API_2, который будет корректно выполнен второй платформой. Первая трансляция $API_1 \rightarrow$ NetAPI осуществляется с помощью модуля, называемого «клиент». А вторая трансляция (обратная) NetAPI $\rightarrow API_2$ осуществляется модулем, который называют «сервер». После второй трансляции запрос от приложения передается в операционную систему второй платформы и она исполняет этот запрос. Тем самым обеспечивается то самое сетевое взаимодействие между платформами, которое позволяет не только разделять ресурсы, но и выполнять различные клиент-серверные взаимодействия. Системы, которые могут общаться с внешним миром, в том числе и с другими платформами, называются открытыми [3]. Это межплатформенное общение (сетевое взаимодействие компьютеров) в общем случае наиболее полно описывается моделью взаимодействия открытых систем — Open Systems Interconnection (OSI), которая была принята международной организацией стандартизации International Standardt Organization (ISO). Модель OSI ISO описывает систему взаимодействия в процессах обмена сообщениями и данными между прикладными программами, которые выполняются на разных компьютерах (платформах). Она является наиболее проработанной с функциональной точки зрения полноты набора стандартов и определения их совместимости друг с другом. При разработке модели использовался известный метод разбиения сложной задачи на подзадачи, поэтому модель получилась многоуровневой[8]. На практике мы предпочитаем использовать другой открытый стек протоколов взаимодействия между открытыми системами; речь идёт о стеке TCP/IP. Главным образом потому, что этот стек появился на несколько лет раньше и смог продемонстрировать свою работоспособность и эффективность.

Если мы на одном компьютере захотим предоставить какие-нибудь его ресурсы в общий доступ, то на другом компьютере должны быть механизмы получения об этом

8 Модель OSI ISO официально насчитывает семь уровней, хотя второй уровень, называемый канальным, разбит на два подуровня: это LLC-sublayer (подуровень логического соединения, на котором пакеты данных преобразуются в кадры данных. В частности, один пакет может быть разбит на несколько кадров) и MAC-sublayer (подуровень управления доступом к среде передачи данных, на котором осуществляется передача кадров).

сведений — какие ресурсы, где они расположены, кому и на каких условиях ими можно пользоваться. Это можно сделать с помощью так называемого «сетевого браузера», который за счет посылки специальных запросов собирает информацию о ресурсах, имеющихся в сети, и представляет ее в виде базы данных виртуальных сетевых ресурсов. Эти сетевые ресурсы могут быть использованы пользователями и приложениями, которые они запускают на своём компьютере. В том случае, когда приложения обращаются к локальным ресурсам компьютера, запросы на API_1 передаются в операционную систему и должным образом обрабатываются. А обращения к сетевым виртуальным ресурсам должны перенаправляться на модуль «клиент» с целью их трансляции в NetAPI и пересылки на другой компьютер, на котором и расположены запрашиваемые ресурсы. Этот анализ запросов со стороны приложений осуществляются модулем, который чаще всего называют «редиректором». Редиректор умеет читать базу данных сетевых виртуальных ресурсов и сортирует запросы от любого приложения к операционной системе, перенаправляя их при необходимости на модуль «клиент».

Итак, мы перечислили следующие главные компоненты сетевого взаимодействия, которое обеспечивается операционными системами. Это модули «клиент», «сервер», «сетевой браузер» и «редиректор». Не все эти компоненты должны быть установлены одновременно на компьютере. Если на всех компьютерах, связанных сетевыми коммуникациями, установлены все упомянутые четыре компонента, то такую сеть обычно называют «одноранговой». В такой сети любой из компьютеров может выступить и в роли клиента, и в роли сервера. Это самые простые сетевые системы, но они эффективны только в том случае, когда компьютеров мало. Множество компьютеров в одноранговой сети образуют так называемую «рабочую группу». Можно сказать, что «рабочая группа» - это группа компьютеров, отнесенных к некоторой одноранговой сети с заданным именем (названием). С ростом числа компьютеров в одноранговых сетях ими становится очень трудно управлять, они не поддерживают централизованного управления. Обычно такие сети содержат не более 10 - 25 компьютеров. Стоит сказать, что операционные системы Windows Home могут работать только в одноранговых сетях[9], а системы Windows Professional изначально настроены на работу в них, но могут быть переведены в другой режим, для которого и предназначены.

Если на одном или на нескольких компьютерах установлены только модуль «сервер» и их основная роль — это предоставление своих ресурсов пользователям и их приложениям, работающих на других компьютерах, на которые установлены модули «клиент», «браузер» и «редиректор», то такие сети принято называть «клиент — сервер». Есть даже операционные системы, которые изначально могут работать только как серверы в сетевом взаимодействии. Хотя большинство операционных систем, у которых в названии присутствует слово «сервер», считают себя и клиентом, и сервером, и размещены в «рабочую группу». При этом они могут быть отнесены к сетям «клиент — сервер» и выполнять либо роль выделенного сервера, либо клиента, либо даже стать основой построения корпоративной клиент-серверной сети.

При разработке операционных систем, предназначенных для работы в сетях «клиент-

9 Одним из разновидностей рабочих групп являются домашние группы. Они имеют механизмы информационной безопасности — стать членом домашней группы можно только в случае знания пароля, который указывается при создании такой группы.

сервер» и из-за необходимости организовать управление доступом к ресурсам, в системах Microsoft Windows уделялось пристальное внимание обеспечению информационной безопасности. При этом была реализована модель безопасности с дискреционным разграничением доступа, делающая операционную систему более надежной и в то же время достаточной простой в управлении. Суть дискреционного метода управления доступом рассмотрим чуть позже.

Модель безопасности систем Windows класса NT[10] предполагает глубокую интеграцию средств защиты с операционной системой. Подсистема безопасности осуществляет контроль за тем, кто и какие действия совершает в процессе работы, к каким объектам пытается получить доступ. Все действия пользователя, в том числе и обращения ко всем объектам, как нетрудно догадаться, на самом деле могут быть совершены только через соответствующие запросы к операционной системе. Операционная система использует этот факт и имеет все необходимые механизмы для тотального контроля всех запросов к ней. Это обеспечивается с помощью механизмов, использующих понятие *учетной записи*. Учетная запись или аккаунт (account) — это информационная структура, с которой работает операционная система. Главное поле в учетной записи — это идентификатор пользователя, по которому система может идентифицировать (распознавать) пользователя всё время его работы на компьютере. Когда он регистрируется в системе, то по имени входа пользователя — так называемому логину (login от сочетания log in, т. е. зарегистрироваться в журнале) система находит соответствующую ему учетную запись. Если такая учетная запись есть, то проверяется пароль пользователя (на самом деле сверяется значение вычисленной хеш-функции пароля со значением, хранящемся в этой учетной записи). В случае успешной проверки (проверка подлинности пользователя называется *аутентификацией* - authentication) создается сеанс пользователя и ему присваивается идентификатор пользователя. В системах Microsoft Windows этот идентификатор называют Secure Identifier, сокращенно SID. SID-ы пользователей уникальны, они имеют длину 128 бит и генерируются при создании новой учетной записи по алгоритму, схожему с UUID (Universally Unique Identifier). Помимо логина, идентификатора и значения хеш-функции пароля в учетной записи содержатся сведения о членстве в групповых учетных записях (в учетной записи пользователя перечислены SIDы групп, к которым он имеет отношение, т. е. является членом группы). Совокупность этих идентификаторов, полученная из учётной записи, образует так называемый *маркер доступа* — Access Token, который сопровождает все вычислительные процессы, порожденные (запущенные) пользователем, и этот маркер содержится во всех запросах к операционной системе.

Теперь о дискреционном методе управления доступом. Каждый объект в операционной системе, особенно если она и ресурсы, которыми она управляет, установлены на томах с файловой системой NTFS, имеют *список управления доступом* — Access Control List (ACL). Элемент списка представляет собой запись, в которой полю с SID-ом сопоставлена так называемая *маска доступа* — Access Mask. В общем случае эта битовая маска доступа может быть представлена как матрица из двух строк и N столбцов. Первая строка, обозначаемая Deny (Отказывать), указывает какие элементарные действия с объектом

10 NT — New Technology, т. е. новые технологии. Дело в том, что до этого компания Microsoft не имела операционных систем, которые могли бы работать в корпоративном секторе.

запрещены, в то время как вторая строка, обозначаемая словом Allow (Разрешено), указывает на «действия», которые разрешены к выполнению. Столбцы таких матриц как раз и соответствуют этим «действиям». Точнее сказать, что это так называемые Permissions (Разрешения). Состав этих пермиссий (разрешений) зависит от класса объекта и тем элементарным действиям, которые могут применяться с объектами данного класса. Например, если объектом является принтер, то на нем можно или нельзя распечатывать документы, можно или нельзя его конфигурировать (администрировать), можно или нельзя удалить или создать, стать его владельцем и т. д. Очевидно, что для объектов типа «файл» имеются другие разрешения («пермиссии»). Файл можно или нельзя читать, можно или нельзя узнать или изменить значения его аргументов и/или значения расширенных аргументов, можно или нельзя читать список управления доступом к файлу (разрешения на файл) и т.д. И подсистема безопасности операционной системы, получив запрос на какую-нибудь операцию над тем или иным объектом, получает маркер доступа, и перечень запрашиваемых пермиссий, сопровождающих запрос на выполнение той или иной операции над этим объектом. Подсистема безопасности берет ACL объекта и последовательно перебирает SID-ы из маркера доступа, анализируя маски доступа соответствующих элементов списка управления доступом. Запрошенное действие будет выполнено только в том случае, если при анализе разрешений в элементах списка не будет ни одного запрета и если найдется требуемое разрешение. В противном случае запрошенное действие не будет выполняться. Очевидно, что если ACL объекта пустой, т.е не содержит ни одного элемента, то никакие действия с этим объектом невозможны, т.к. подсистема безопасности не получит разрешения на выполнение запрашиваемых действий над объектом. И наоборот, если в списке разрешения доступа к объекту есть единственный элемент для группы Все (Everyone), в котором маска доступа содержит разрешение Allow для всех пермиссий, имеющих отношение к этому объекту, то любой пользователь будет иметь возможность выполнять любое действие над таким объектом. Среди возможных разрешений (пермиссий) есть разрешение на изменение разрешений (Change Permissions) и разрешение на смену владельца объекта (Take Ownership). Кстати, владелец объекта (как правило, это создатель объекта) может изменять ACL даже если такое действие ему запрещено в явном виде. Описанный механизм и представляет собой дискреционный метод управления доступом.

Итак, запрашиваемые у операционной системы операции и обращения к конкретным объектам разрешаются, только если у пользователя для этого имеются необходимые *права* и/или *разрешения*. При этом следует различать эти понятия.

Права (Rights) определяют уровень полномочий при работе в системе. Например, если нет права форматировать диск, то выполнить это действие пользователь не сможет. Кстати, конкретно таким правом при работе с Windows обладают только члены группы Администраторы. Можно говорить и о праве изменения настроек дисплея, и о праве работать на компьютере. Очевидно, что перечень прав является достаточно большим. Права могут быть изменены посредством применения соответствующих политик.

Термин *разрешение* (permission) обычно применяют по отношению к конкретным объектам, таким как файлы и каталоги, принтеры и некоторые другие. Можно говорить о разрешениях на чтение, на запись, на исполнение, на удаление и проч. Например, можно иметь разрешения на чтение и запуск некоторой программы, но не иметь разрешений на ее переименование и удаление.

Важно, что права имеют приоритет перед разрешениями. Например, если у некоторого пользователя нет разрешения «стать владельцем» того или иного файлового объекта, но при этом мы дадим ему право стать владельцем любого объекта, то он, дав запрос на владение упомянутым объектом, получит его в свою собственность. Таким правом обладают члены группы Администраторы.

Модель безопасности Windows NT гарантирует, что не удастся получить доступ к ее объектам без того, чтобы предварительно пройти аутентификацию и *авторизацию*. Под авторизацией (Authorization) понимают получение полномочий; она осуществляется посредством получения информации о членстве во встроенных локальных группах системы.

Учетные записи хранятся в базе данных учетных записей, которая представлена файлом SAM (Security Account Management). Это так называемые локальные учетные записи, поскольку они могут быть идентифицированы только на том компьютере, где они имеются. Строго говоря, если мы для некоторого пользователя создадим ему учетную запись на двух компьютерах с Windows NT, то это будут две разные учетные записи — у них будут разные SIDы. Это потому, что SID пользователя, присутствующий в маркере доступа, идентифицируется не по имени пользователя, а по идентификатору, который находится в учетной записи. Подсистема безопасности гарантирует уникальность идентификаторов безопасности. Они генерируются при создании новых учетных записей и никогда не повторяются.

Как мы уже говорили, маркер доступа несёт в себе информацию о типе учетной записи, т.к. учетные записи могут быть объединены в группы, а в учетных записях пользователей перечислены учетные записи групп, в которые он включён.

К встроенным учетным записям относятся записи администратора и гостя, а также учетные записи для следующих групп:

Администраторы (Administrators) – имеют полные, ничем не ограниченные права доступа к компьютеру

Пользователи (Users) – пользователи не имеют прав на изменение параметров системы. Они не могут запускать многие несертифицированные приложения, однако они могут иметь свои личные настройки параметров рабочего стола и папку Мои документы.

Опытные[11] пользователи (Power Users) – обладают большинством прав, но с некоторыми ограничениями. В частности, они могут запускать любые, а не только сертифицированные приложения, создавать учетные записи и управлять ими, управлять сетевым доступом.

Гости (Guests) – имеют минимальные права при работе на компьютере, не могут иметь свои настройки рабочего стола.

Операторы архива (Backup Operators) – члены этой группы могут создавать архивы из системных и пользовательских файлов и восстанавливать файлы их архивов в случае такой необходимости.

Репликатор (Replicator) – предназначена для создания учетных записей, которые смогут осуществлять репликации файлов и баз данных.

Учетные записи имеют и компьютеры. Есть такая учетная запись System, которая получает свой SID при установке операционной системы.

11 Неудачный перевод термина Power Users. На самом деле речь идет о пользователях, обладающих существенно большими правами по сравнению с обычными пользователями.

Принадлежность учетной записи к одной из встроенных локальных групп определяет полномочия (права, привилегии) пользователя при работе на этом компьютере. Например, члены встроенной группы Администраторы имеют максимально возможные права при работе на компьютере (встроенная учетная запись администратора практически равносильна учетной записи суперпользователя в UNIX-системах, хотя механизм прав в UNIX-системах существенно отличается).

Помимо перечисленных выше встроенных групп администратор системы может создать любое количество групп пользователей и предоставить им необходимый набор прав и разрешений. Вновь создаваемые учетные записи групп (их называют группами безопасности) используются для определения разрешений на доступ к тем или иным объектам. Как мы уже знаем, для этого любому объекту может быть специально создан сконфигурирован свой ACL. При использовании файловой системы NTFS помимо обычного ACL, который может быть создан для каталога, каждый файл (в том числе и файлы-каталоги) имеется ещё два списка. Это список *DACL* (Discretionary Access Control List). Он порождается вместе с новым файловым объектом. Помимо DACL каждый файл в NTFS может иметь ещё список SACL (System Access Control List — системный ACL), который используется подсистемой аудита для контроля работы со списком DACL.

Рекомендуется составлять списки управления доступом, пользуясь не учетными записями пользователей, а учетными записями групп. Во-первых, это позволяет существенно сократить список управления доступом, поскольку групп обычно намного меньше, чем пользователей. Как результат, список будет намного короче, понятнее и удобнее для последующего редактирования. Во-вторых, в последующем можно будет создавать новых пользователей и добавлять их в соответствующие группы, что практически автоматически определит их разрешения на те или иные объекты как членов определенных групп. Наконец, в-третьих, список будет быстрее обрабатываться операционной системой.

Очевидно, что каждый пользователь должен быть членом, как минимум, одной встроенной группы и может быть членом нескольких групп безопасности, создаваемых в процессе эксплуатации операционной системы. Итоговые разрешения на доступ к объектам, имеющим списки управления доступом, вычисляются как сумма разрешений, определенных для каждой из групп. И только явный запрет на разрешение перечеркивает сумму разрешений, которая получается для данного пользователя.

Операционные системы Microsoft Windows обеспечивают вышеописанный механизм безопасности и управление доступом к ресурсам прежде всего на локальном уровне. Это означает, что механизмы защиты работают на каждом компьютере с такой операционной системой. Однако это имеет и обратную сторону. Дело в том, что учетные записи пользователей и групп локальны: они идентифицируются и потому правильно работают только на том компьютере, где их создали. Если же есть необходимость обратиться к общим ресурсам компьютера через сеть, нужно, чтобы для пользователя, который выполняет такое обращение к удаленным объектам, была создана такая же учетная запись. При этом точно такой она, естественно, быть не может, т. к. алгоритм генерации SID обеспечивает их уникальность. Поэтому в рабочих группах применяют упрощенный способ контроля доступа через сеть — не через SIDы учетных записей, а через проверку логина и пароля. В этом

случае достаточно обеспечить, чтобы для некоего пользователя у него на разных компьютерах были учетные записи с одинаковым логином и паролем.

Поскольку становится затруднительным обеспечить наличие учетных записей для каждого пользователя на всех тех компьютерах, с ресурсами которых ему необходимо работать, пользуясь вычислительной сетью, в свое время была предложена технология корпоративных (доменных) сетей. В *домене*, который представляет собой множество компьютеров, должен быть выделен сервер со всеми учетными записями этого домена (на контроллерах домена, работающих под управлением Windows Server, база с учетными записями домена находится в файле NTDS.DIT, поскольку организация доменов в этих операционных системах возможна только при установке службы Active Directory). Такой сервер называют *контроллером домена*. Учетные записи домена в отличие от локальных учетных записей, имеющихся на каждом компьютере с операционной системой типа Windows, являются глобальными. Это означает, что они могут быть идентифицированы на любом компьютере, входящем в состав домена. В результате, имея множество компьютеров, объединенных в домен, и контроллер домена, на котором созданы все необходимые учетные записи, мы можем использовать эти учетные записи для управления доступом к различным ресурсам. Более того, мы можем контролировать использование этих ресурсов и регистрировать попытки несанкционированного доступа к тем или иным объектам.

Лабораторная работа № 6. Общий доступ к файлам

Цель работы: Целью работы является получение знаний о проблемах администрирования учетных записей и управления общим доступам к файлам и папкам в одноранговых сетях.

Краткие теоретические сведения

Одна из широко используемых функций операционных систем – предоставление папок с файлами для общего доступа. Однако неверное использование этой возможности может служить причиной нарушения политики доступа и привести к негативным последствиям.

Для управления папками общего доступа используются различные средства. Делать папки общими можно непосредственно из программы “Проводник”, выбирая нужную папку или диск и специальным образом редактируя её (его) свойства доступа. Другая возможность – использование специальной оснастки для консоли управления Microsoft – fsmgmt.msc (от File Sharing management – Общие файлы). Управление общими файлами входит в группу оснасток под названием Управление компьютером (Панель управления → Администрирование → Управление компьютером). Наконец, для управления доступом к файлам через сеть возможно использование команд NetBIOS.

При управлении общим доступом к папкам с использованием “Проводника” для выбранной папки необходимо в контекстном меню, открывающимся по правой кнопке мыши, выбрать пункт “Свойства”. В открывшемся диалоговом окне выбрать вкладку “Доступ” (см. рисунок). По умолчанию для папки включена радиокнопка «Отменить общий ресурс». Для организации общего доступа к папке необходимо выбрать радиокнопку «Открыть общий доступ». При этом станут доступны характеристики общего доступа.

В окне Сетевое имя указывается имя ресурса. Это имя NetBIOS, поэтому если папка,

предоставляемая в общий доступ, имеет длинное имя, да еще и с использованием кириллицы, рекомендуется указать сетевое имя латиницей и не делать его длинным. Имя NetBIOS может быть длиной до 15 символов, но для того, чтобы старое системное программное обеспечение смогло правильно работать с сетевыми именами, рекомендуется делать его не длиннее 8 символов. Например, если папка на диске имела имя Общие файлы, то при предоставлении ее в общий доступ по сети можно дать ей имя либо COMMON, либо FILES, либо еще какое-нибудь понятное и короткое имя. При этом в окне Комментарий следует разместить необходимые пояснения. Соответствие между сетевыми именами и локальными именами фиксируется в реестре операционной системы. Следует знать, что если сетевое имя оканчивается на символ «доллар» ($), то такой ресурс не будет виден при обзоре сети; его не покажет и команда NET VIEW интерфейса NetBIOS. Для получения доступа к невидимому сетевому ресурсу можно воспользоваться либо командой NET USE интерфейса NetBIOS, либо подключая сетевой диск.

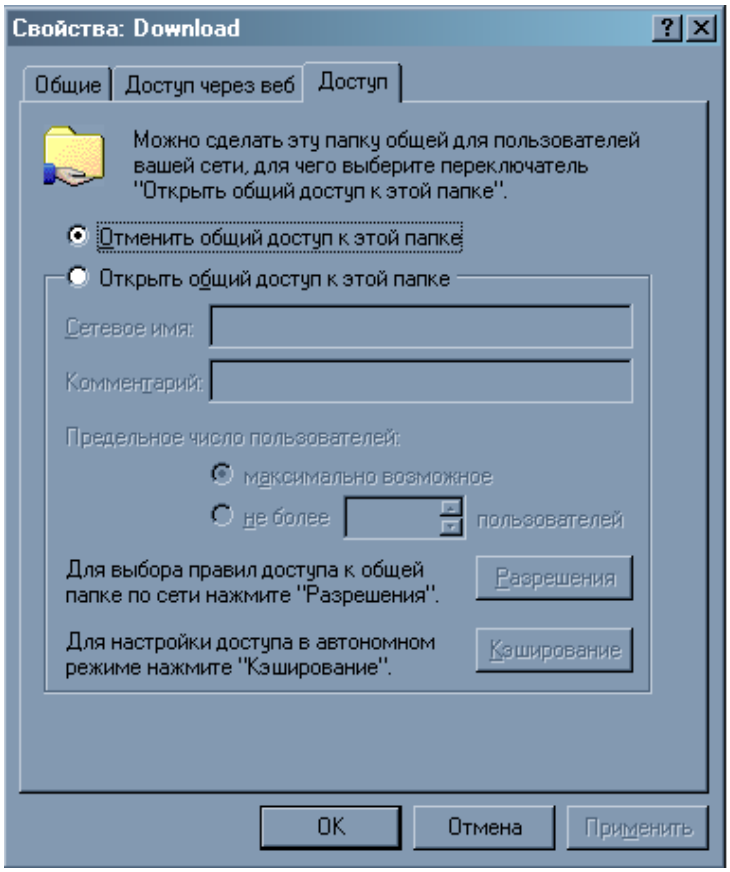

Рисунок. 33 Окно управления общим доступом

Следующая важная кнопка – это Разрешения. Если открыть окно управления разрешениями доступа, то мы увидим то, что показано на рисунке 34. Это разрешения доступа, которые система устанавливает по умолчанию.

Однако в таком случае информация в этой папке становится доступной всем пользователям, работающим в сети, причем это максимально возможные разрешения доступа. Легко догадаться, что это далеко не всегда является желательным фактом. Для более безопасной работы рекомендуется, как минимум ограничить доступ к папке, задав иные разрешения доступа. Рассмотрим поподробнее процедуру составления иного списка

управления доступом.

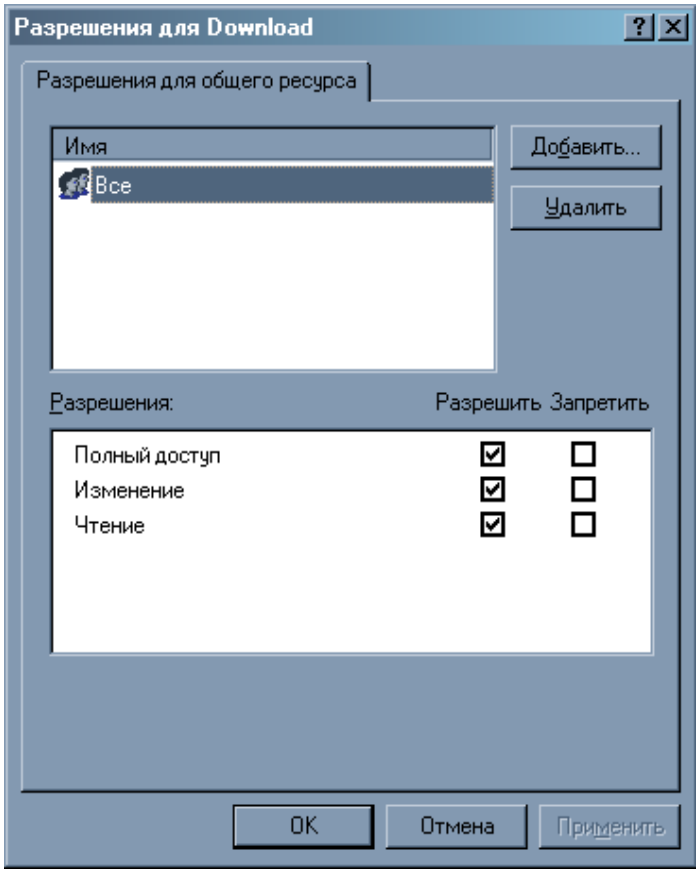

Рисунок 34 . Диалоговое окно «Разрешения доступа»

В верхней части окна Разрешения для … необходимо сформировать перечень тех групп и/или пользователей, доступ которых к папке предполагается. При этом группу «Все» возможно следует и вовсе удалить, чтобы исключить доступ к файлам, расположенным в папке, нежелательным лицам. Для формирования списка управления доступом следует использовать кнопки Добавить (Add) и Удалить (Delete). В случае нажатия на кнопку Добавить открывается окно Выбор … с перечнем пользователей и групп (см. рис. 35). Здесь следует остановиться и рассмотреть эти учетные записи. Они образованы из встроенных учетных записей, из учетных записей пользователей и групп, которые были сделаны членами группы Администраторы и/или членами группы Опытные пользователи. Наконец, в этом списке можно увидеть особые группы. Состав членов этих особых групп нельзя просмотреть или модифицировать. Однако представлять, кто может быть членами этих групп, необходимо.

- ВСЕ (Everyone) — объединяет все возможные обращения к системе с запросами на те или иные ресурсы. Включает в себя не только те учетные записи, которые могут быть идентифицированы системой, но и вообще любые запросы.
- Прошедшие проверку – объединяет всех тех пользователей, которые прошли аутентификацию.
- АНОНИМНЫЙ ВХОД (Anonimous) – для учетных записей, которые могут обращаться к ресурсам компьютера не указывая свой пароль.
- СЕТЬ (Network) — объединяет всех пользователей, получивших доступ к данному ресурсу по сети (в отличие от пользователей, получивших доступ к ресурсу локально).
- УДАЛЕННЫЙ ДОСТУП – пользователи, получающие доступ через модемные

соединения.

- ИНТЕРАКТИВНЫЕ (Interactive) — объединяет всех пользователей, получивших доступ к данному ресурсу, зарегистрировавшись локально на компьютере, где находится этот ресурс. Для сетевого доступа эта группа не имеет значения, но при формировании дискреционных списков управления доступом, который имеет отношение к разрешениям NTFS, эта группа может быть востребована.
- SYSTEM (система) – ядро операционной системы.
- СЛУЖБА (Services) – управляющие и обрабатывающие модули операционной системы, имеющие статус процесса. Вызываются из ядра операционной системы.
- ПАКЕТНЫЕ ФАЙЛЫ
- И некоторые другие группы. Их наличие или отсутствие в списке зависит от операционной системы и установленных в ней сервисов.

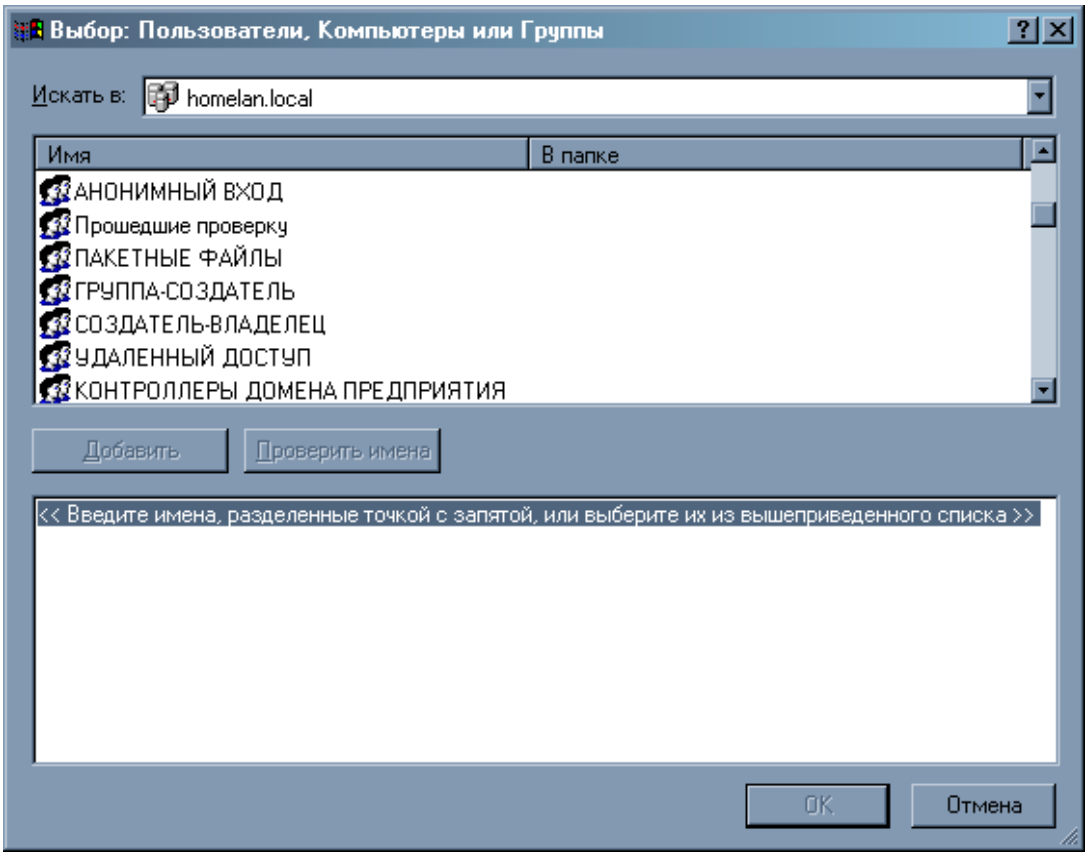

Рис. 35. Диалоговое окно «Выбор пользователей и групп»

В окне Разрешения для … устанавливаются соответствующие разрешения. Обратите внимание, что имеется возможность выбрать одну из трех комбинаций:

- поставить галочку в столбце Разрешить (Allow). В этом случае говорят, что данный пункт разрешен;
- поставить галочку в столбце Запретить (Deny). Следует считать, что соответствующее действие *запрещено*.
- оставить неотмеченными и столбец Разрешить, и столбец Запретить. Это будет означать, что разрешение *не запрещено.*

Таким образом, разрешения могут быть в явном виде разрешены или запрещены, а могут быть и не запрещены. Если мы заменяем примитивный список вида: «Все имеют полный доступ» на какой-нибудь иной, то вычисляются итоговые разрешения доступа. Если

некий пользователь является членом нескольких групп, то в списке разрешений для него может оказаться несколько правил. Разрешения суммируются, однако запрет имеет приоритет перед разрешением. Не рекомендуется указывать запрет для групп, и уж тем более никогда нельзя ставить запрет для группы Все. Очевидно, что те пользователи и группы, которые не были указаны в списке разрешений доступа, не получат доступа к ресурсу. Поэтому правильно составленный список может и не иметь ни одного запрета. Очень важно отметить, что не следует в списке управления доступом использовать встроенные учетные записи групп, за исключением группы Администраторы, для которых, как правило, всегда указывается разрешение полного доступа.

Разрешение Чтение (Read) предполагает возможность чтения файлов и, если файл является исполняемым, выполнение соответствующей программы. Разрешение Изменение (Change) означает, что помимо чтения и запуска программ можно изменять файлы и папки – создавать, переименовывать, изменять и удалять файловые объекты. Если установить галочку напротив разрешения Изменение, но удалить галочку напротив разрешения Чтение, то изменять файлы и папки, со всей очевидностью, будет нельзя.

Разрешение Полный доступ отличается от разрешения Изменение тем, что при полном доступе можно управлять разрешениями. Поэтому если папки с общими файлами располагаются на дисках с NTFS, то использование разрешения Изменение позволяет лишить пользователей возможности изменять разрешения NTFS, даже если пользователи и являются собственниками файлов. Напомним, что владелец файлов имеет право изменять разрешения NTFS даже в отсутствие разрешения на изменение разрешений.

Следует отметить, что разрешения общего доступа к файлам отличаются от разрешений NTFS, предоставляемых на вкладке Безопасность свойств папки. Их часто используют совместно для управления доступом, но в данной лабораторной работе мы изучаем только разрешения общего доступа.

Для управления доступом к таким сетевым ресурсам как файлы в системах Windows помимо обычного проводника сделана специальная консоль. Подробно описывать ее не будем, поскольку ее изучение предполагается выполнить самостоятельно. Для этого необходимо запустить на выполнение файл FSMGMT.MSC и нажать на клавишу {F1} или указать на символ «?» в панели управления открывшегося окна. Следует внимательно и полностью прочитать имеющиеся справочную информацию и подсказки.

Обратите внимание, что консоль управления Общие файлы помимо управления сетевым доступом к общим файлам позволяет получить полный перечень сетевых файловых ресурсов. Кроме этого, с ее помощью можно управлять сетевым доступом к папкам с файлами на удаленных компьютерах, если Вы имеете на удаленном компьютере соответствующие права. Наконец, с ее помощью можно получить информацию о том, кто сейчас использует через механизмы сетевого доступа имеющиеся на компьютере общие файлы, и какие конкретно файлы в каком режиме используются.

Если внимательно посмотреть на имеющиеся сетевые ресурсы, то можно увидеть, что кроме тех общих папок с файлами, которые были сделаны администраторами и/или членами группы Power Users, существуют специальные ресурсы, имена которых составлены из имени логического диска и дописанного к нему символа $ (доллар), и другие общесистемные ресурсы: Admin$ и IPC$. Эти ресурсы, за исключением IPC$ предназначены исключительно

для членов группы Администраторы. Аббревиатура IPC означает межпроцессное взаимодействие. Речь идет о канале обмена данными между процессами, которые выполняются на разных компьютерах. В случае отключения этого ресурса (это можно сделать, например, путем редактирования реестра) перестанет работать связь между модулями клиент и сервер, работающими по протоколу SMB (Server Message Blocks).

Использование команд NetBIOS для администрирования общего доступа

NetBIOS – это протокол, предоставляющий право удаленного доступа к файлам и папкам. Этот протокол предоставляет ряд команд, которые могут использоваться для администрирования общего доступа и подключения к общим файлам и папкам на других компьютерах в сети. Ниже приведена краткая справка по командам, использование которых может понадобиться в данной лабораторной работе:

Подключение и отключение общих ресурсов и вывод сведений о подключениях:
NET USE [диск: | *] [\\компьютер\каталог [пароль | ?]] [/SAVEPW:NO] [/YES] [/NO]
NET USE [порт:] [\\компьютер\принтер [пароль | ?]] [/SAVEPW:NO] [/YES] [/NO]

NET USE диск: | \\компьютер\каталог /DELETE [/YES]
NET USE порт: | \\компьютер\принтер /DELETE [/YES]
NET USE * /DELETE [/YES]

NET USE диск: | * /HOME

Диск Имя диска, назначаемое общему каталогу.
* Эквивалент следующего свободного имени диска. При использовании совместно с ключом /DELETE производится отключение сразу всех ресурсов.
Порт Имя параллельного (LPT) порта, назначаемое общему принтеру.
Компьютер Имя компьютера, на котором расположен общий ресурс.
Каталог Сетевое имя общего каталога.
Принтер Сетевое имя общего принтера.
Пароль Пароль для доступа к общему ресурсу (если он имеется).
? Пароль для доступа к ресурсу запрашивается интерактивно. Этот режим может понадобиться лишь в том случае, когда ввод пароля необязателен.
/SAVEPW:NO Использование этого ключа позволяет предотвратить запись пароля в файл со списком паролей. В этом случае при каждом подключении к ресурсу пароль надо будет вводить заново.
/YES Выполнение команды NET USE без предварительного запроса данных или подтверждения.
/DELETE Отключение общего ресурса.
/NO Выполнение команды NET USE с автоматической выдачей отрицательных (NO) ответов на все запросы, относящиеся к подтверждению действий.
/HOME Подключение к личному (HOME) каталогу, если сведения о нем имеются в учетной записи LAN Manager или Windows NT.

Команда NET USE без параметров выводит список всех подключенных ресурсов.

Для просмотра выводимых сведений с паузами между отдельными экранами используются команды: NET USE /? | MORE и NET HELP USE | MORE

Вывод текущих параметров рабочей группы NET CONFIG [/YES]

/YES Выполнение команды NET CONFIG без предварительного запроса данных или подтверждения.

Создание и удаление общих ресурсов NET SHARE имя_ресурса

имя_ресурса=диск:путь [/USERS:число | /UNLIMITED][/REMARK:"текст"] [/CACHE:Manual | Automatic | No][/CACHE:Manual | Documents| Programs | None]
имя_ресурса [/USERS:число | /UNLIMITED] [/REMARK:"текст"][/CACHE:Manual | Documents | Programs | None]{имя_ресурса | имя_устройства | диск:путь} /DELETE

Эта команда позволяет управлять общим доступом - создавать или отменять доступ к общим файлам. Когда она дается без параметров, то выдает информацию обо всех ресурсах компьютера, которые могут быть получены по сети. Синтаксис команды зависит от того, в какой операционной системе мы работаем. Для сервера он будет следующим:

NET SHARE sharename
sharename=drive:path [/GRANT:user,[READ | CHANGE | FULL]]
[/USERS:number | /UNLIMITED]
[/REMARK:"text"]
[/CACHE:Manual | Documents| Programs | None]
sharename [/USERS:number | /UNLIMITED]
[/REMARK:"text"]
[/CACHE:Manual | Documents | Programs | None]
{sharename | devicename | drive:path} /DELETE

Нетрудно заметить, что здесь имеется возможность указать разрешения доступа, в то время как при выполнении этой команды на рабочей станции не представляется возможным составить перечень разрешений.

Вывод сведений о командах и сообщениях NET команда /?

NET HELP [суффикс]
NET HELP код_ошибки

Команда Определяет команду Microsoft NET, сведения о которой следует получить.

Суффикс Определяет второе слово интересующей команды. Например суффикс команды NET VIEW - слово VIEW.

код_ошибки Задает номер интересующего сообщения об ошибке.

Чтобы получить краткое описание всех команд Microsoft NET, введите команду NET HELP без параметров.

Порядок выполнения лабораторной работы и варианты заданий

1. Подготовьте две виртуальных машины, которые будут содержаться в одной сети (с адресами 172.(16+N).M.K /24, где N - это последняя цифра из номера группы; M – ваш порядковый номер по журналу; K – длина Вашей фамилии и 172.(16+N).M.100+K /24 и могут общаться друг сдругом. Первая машина — это сервер, его имя должно соответствовать имени Вашего отца. Вторая машина будет выполнять роль клиента.
2. С помощью менеджера учетных записей создайте на сервере группу безопасности, которая задается в виде: G<№группы>_<№варианта>, где №группы – номер группы

студента, выполняющего лабораторную работу[12].

3. Создайте учетные записи пользователей и добавить их в группу. Наименование учетной записи задается в виде U<№группы>_<Фамилия>[13]. Помните, что созданные учетные записи обязательно должны принадлежать одной из встроенных групп.
4. Создайте общие ресурсы. Имя общей папки должно соответствовать Вашей фамилии. Настроить доступ на изменение для созданных ранее пользователей к этому ресурсу в и на чтение всем.
5. Создайте на клиентской машине такие же учетные записи. Проверьте работу с созданными ресурсами. Покажите преподавателю результаты.
6. Напишите .bat файлы, который бы выполнял те же действия используя команды NetBios. Напишите bat файл, который бы отменял общие ресурсы, сделанные в соответствии с пунктом 3. Показать преподавателю результаты.
7. Поменяйте на одном из компьютеров пароли учётным записям. Проверьте работу с ресурсами сервера. Сделайте выводы.
8. Оформите отчет.

Контрольные вопросы

1. Объясните модель безопасности, применяемую в системах Microsoft Windows класса NT.
2. Объясните назначение встроенных локальных групп.
3. Что такое административные общие файловые ресурсы? Как отключить административные общие ресурсы?
4. Что такое IPC$? Что будет, если отключить IPC$?
5. Как обеспечить общий доступ к файлам и папкам?
6. Какие команды NetBIOS используются для подключения к общим файлам и папкам?
7. Какие команды NetBIOS используются для администрирования общих файлов и папок?
8. С помощью какой команды можно получить перечень сетевых ресурсов, расположенных на удаленном компьютере, имя которого Вы знаете?
9. Как можно узнать, кто сейчас подключен к вашим общим файлам? Как можно предупредить пользователей о том, что им необходимо отключиться от общих файлов Вашего компьютера?

12 Например, студент с 3-им вариантом задания из группы 4061 должен создать группу с наименованием «G4061_3».

13 Если по заданию требуется создать несколько учетных записей, то их наименования должны быть в виде U<№группы>_<Фамилия>_<Имя>.

Тема № 7: **КОРПОРАТИВНЫЕ СЕТИ. СЛУЖБА КАТАЛОГА**

Краткие теоретические сведения

Как мы уже отмечали, для сетей с большим количеством компьютеров и, соответственно, пользователей, вместо рабочих групп используют доменную организацию. Под доменом понимают множество компьютеров с общей базой учетных записей компьютеров и пользователей этого домена и единой политикой защиты. Среди компьютеров домена должен быть специально сконфигурированный сервер, являющийся держателем всех учетных записей домена. Такой сервер называют контроллером домена. На контроллере домена осуществляется аутентификация пользователей домена.

Доменные учетные записи пользователей являются глобальными. Это означает, что такая запись может быть идентифицирована на любом компьютере домена. Очевидно, что это существенно облегчает работу администраторов, поскольку достаточно создать для пользователя всего одну учетную запись, которая будет находиться на контроллере домена. Для повышения надежности доменной сети в ней создается несколько контроллеров домена. Каждый контроллер домена имеет копию базы данных с учетными записями. Идентичность баз данных обеспечивается механизмом репликаций, т.е. рассылкой на все контроллеры домена вносимых изменений в базу данных домена. По умолчанию пользователи, работающие на компьютерах, которые не входят в состав домена, не имеют доступа к ресурсам этого домена.

Служба каталога

В больших корпоративных сетях пользователи при поиске сетевых ресурсов начинают испытывать определенные проблемы. Дело в том, что каждый компьютер, на котором установлена служба «сервер», может выступать в этой роли. Как следствие, сетевые ресурсы при большом числе серверов действительно порой нелегко найти. А если администратор решит переместить общие каталоги с одного сервера на другой, то возникают проблемы: как донести до всех пользователей эти и многие другие изменения в сети? Гораздо удобнее было бы, если бы пользователи могли видеть некий перечень (возможно, структурированный тем или иным образом) всех сетевых ресурсов, пользуясь которым можно было бы получить доступ к этим ресурсам (если это разрешено) без поиска вручную того сервера, на котором располагаются эти ресурсы. Поэтому в больших сетях стали использовать так называемую *службу каталога*. Служба каталога (Directory Service) представляет собой базу данных, хранящую сведения и о сетевых ресурсах домена, и о пользователях, и о политиках, с помощью которых определяются права пользователей, и многое другое. Можно сказать что *каталог, как база данных, хранит значения атрибутов для некоторого множества объектов и позволяет получать информацию по запросу*. Находить объекты можно по его атрибутам. Объектами сети являются пользователи, компьютеры, файлы, приложения, принтеры, факс-серверы, базы данных, и многое другое.

Впервые службу каталога реализовала компания Banyas. Однако в нашей стране сетевое программное обеспечение этой фирмы не получило широкого распространения. Следующей была всем известная компания Novell. Ее операционные системы, начиная с

Netware 4.0, использовали службу каталога, названную NetWare Directory Services (NDS). Это позволяло строить сети корпоративного масштаба и предоставлять пользователям ресурсы, которые могли быть расположены на любом из серверов сети. Служба каталога NDS - это распределенная и дублируемая база данных по именам. Причем пользователи в такой сети могут не знать реальное месторасположение ресурсов, которые они используют.

Наконец, в канун 2000 года компания Microsoft также выпустила сетевую операционную систему, использующую идеи службы каталога. Это было семейство серверов Windows 2000. Свою службу каталога Microsoft назвала Active Directory. Эта служба каталогов позволяет отобразить иерархическую организацию компании и ее вычислительной сети. Active Directory обеспечивает наращиваемость и расширяемость, а также функции распределенной безопасности. Эта служба для именования и поиска объектов каталога использует систему доменного именования DNS. Поэтому она легко интегрируется с Интернетом, позволяет использовать простые и интуитивно понятные имена объектов, пригодна для использования в организациях любого размера и легко масштабируется. Если говорить коротко, то служба каталогов Active Directory предоставляет следующие возможности:

- *Единую регистрацию в сети*. Пользователи могут регистрироваться в сети со своим именем и паролем и при этом получать доступ ко *всем* сетевым ресурсам (серверам, принтерам, приложениям, файлам и т. д.) независимо от их расположения в сети.
- *Безопасность информации.* Средства аутентификации и управления доступом к ресурсам, встроенные в службу Active Directory, обеспечивают централизованную защиту сети. Права доступа можно определять не только для каждого *объекта* каталога, но и каждого *свойства* (атрибута) объекта.
- *Централизованное управление.* Администраторы могут централизованно управлять всеми корпоративными ресурсами. Рутинные задачи администрирования не нужно повторять для многочисленных объектов сети.
- *Администрирование с использованием групповых политик*. При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в объектах групповых политик (GPO) и "привязываются" к сайтам, доменам или организационным единицам. Групповые политики определяют, например, права доступа к различным объектам каталога или ресурсам, а также множество других "правил" работы в системе.
- *Гибкость изменений.* Служба каталогов гибко следует за изменениями структуры компании или организации. При этом реорганизация каталога не усложняется, а может и упроститься. Кроме того, службу каталога можно связать с Интернетом для взаимодействия с деловыми партнерами и поддержки электронной коммерции.
- *Масштабируемость.* Служба Active Directory может охватывать как один домен, так и множество доменов, один контроллер домена или множество контроллеров домена ≈ т. е. она отвечает требованиям сетей любого масштаба. Несколько доменов можно объединить в дерево доменов, а несколько деревьев доменов можно связать в лес.
- *Репликация информации.* В службе Active Directory используется репликация служебной информации в схеме *со многими ведущими (multi-master)*, что позволяет модифицировать каталог на любом контроллере домена. Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость и возможность распределения сетевой нагрузки.
- *Гибкость запросов к каталогу*. Пользователи и администраторы сети могут быстро находить объекты в сети, используя *свойства* объекта (например, имя пользователя

или адрес его электронной почты, тип принтера или его местоположение и т. п.). Это, в частности, можно сделать при помощи команды Пуск → Поиск (Start → Search), папку Мое сетевое окружение (My Network Places) или оснастку Active Directory - пользователи и компьютеры (Active Directory Users and Computers). Оптимальность процедуры поиска достигается благодаря использованию глобального каталога.

- *Интеграция с DNS.* Служба Active Directory тесно связана с DNS. Этим достигается единство в именовании ресурсов локальной сети и сети Интернет, в результате чего упрощается подключение пользовательской сети к Интернету.
- *Стандартные интерфейсы.* Для разработчиков приложений служба каталогов предоставляют доступ ко всем возможностям (средствам) каталога и поддерживают принятые стандарты и интерфейсы программирования (API). Служба каталогов тесно связана с операционной системой что позволяет избежать дублирования в прикладных программах функциональных возможностей системы, например, средств безопасности.

Active Directory использует информационную модель X.500, а в качестве протокола доступа — стандартный протокол доступа к каталогам LDAP (Lightweight Directory Access Protocol). Опираясь на этот открытый протокол, можно создавать необходимое программное обеспечение для работы с этой базой данных.

Каталог Active Directory позволяет создавать иерархические структуры данных, упрощающие управление учетными данными и другими параметрами безопасности, а также облегчающие для пользователя процедуру поиска таких сетевых ресурсов, как файлы и принтеры. Она поддерживает ряд протоколов проверки подлинности, таких как Kerberos V5, Secure Sockets Layer (SSL) v3 и Transport Layer Security (TLS) с сертификатами X.509 v3, а также группы безопасности, объединяющие несколько доменов.

Возможности по объединению каталогов и их структурированию позволяет организовать и упростить процедуру управления данными о пользователях, компьютерах, приложениях и устройствах, а также упростить поиск нужных сведений для пользователей. Интерфейсы, основанные на протоколе LDAP, позволяют воспользоваться преимуществами поддержки синхронизации и обеспечить соблюдение определенных требований к объединению. Возможности каталога Active Directory упрощают настройку конфигурации и управление приложениями и другими внесенными в каталог сетевыми компонентами. Используется технология индексирования и усовершенствованная техника репликации, которые повышают быстродействие.

Активным этот каталог назвали скорее всего потому, что это не только база данных, к которой обращаются с тем или иным запросом для получения необходимой информации. Эта служба сама, по своей инициативе, а не по запросу может посылать на компьютеры домена некоторую информацию. Прежде всего, в качестве такой информации можно рассматривать групповые политики, которые определяют, как должны работать компьютеры и пользователи домена (или его части, называемой подразделением).

База данных Active Directory основана на иерархической модели. Это позволяет легко и достаточно эффективно отображать структуру организации и вносить относительную независимость в функционирование каждого подразделения и, вместе с тем, проводить единую политику безопасности и использования вычислительных и информационных

ресурсов.

Создавая инфраструктуру Active Directory, необходимо построить модель организации и продумать структуру пространства имен. Это позволит в дальнейшем упростить пользователям и администраторам осуществлять поиск объектов каталога. Поскольку пространства имен Active Directory и DNS имеют одинаковую структуру, правильное планирование пространства имен играет важную роль при развертывании Active Directory. Пространство имен AD использует три основных структурных уровня: домены, деревья доменов и леса. Действительно, поскольку Active Directory использует систему доменных имен, появляется возможность в некотором домене создать дочерние домены (они станут подчиненными доменами). Таким образом, при необходимости можно создать целое доменное дерево. Имеется возможность объединять доменные деревья в один лес. Для однозначного определения статуса вновь создаваемого домена администратор обязательно должен указать следующие сведения:

- новый домен является дочерним для некоторого домена или он является начальным (корневым) доменом в новом доменном дереве?
- новое доменное дерево будет входить в уже существующий доменный лес, или же лес пока будет состоять из одного единственного дерева?
- Режим работы контроллера домена (или модель совместимости с пред-Windows 2000 серверами.

При установке службы каталога необходимо указать – будет ли домен содержать контроллеры домена на базе Windows NT 4.0 server, либо в нем таких контроллеров не будет. В первом случае домен будет работать в так называемом *смешанном режиме* (*mixed mode*). В этом режиме учетные записи хранятся в виде, который доступен для контроллеров домена на базе ОС Windows NT 4.0 server. Если же в домене нет и не будет контроллеров домена на базе этой или еще более ранней ОС, то лучше выбрать так называемый *основной режим* (*native mode*). При использовании основного режима работы появляются дополнительные возможности, позволяющие проще и эффективнее выполнять некоторые задачи администрирования. Но при этом не стоит упускать из внимания, что будет невозможно использовать средства администрирования, созданные другими компаниями (не Microsoft), и совместимости с другими контроллерами домена уже не будет.

Домены в AD, как и в системах на базе Windows NT 4.0 Server, допускают к ресурсам только членов домена и в этом смысле являются границей общей области безопасности. Кроме того, домен служит границей репликации: AD допускает репликацию объектов домена только на контроллеры данного домена. Между родственными доменами (принадлежат одному лесу или дереву[14]) автоматически устанавливаются *отношения доверия*. *Отношения доверия* (часто говорят: «доверительные отношения») *позволяют доверять процедуре аутентификации, которая прошла домене, которому мы доверяем*, и предоставлять разрешения доступа к тем или иным ресурсам, опираясь на полученные сведения о пользователях, группах и компьютерах.

Наиболее простой структурой домена для администрирования является одиночный домен. При создании корпоративной сети следует начинать с создания одиночного домена, а

14 Чаще всего доменный лес состоит из одного единственного дерева, которое, в свою очередь, редко когда насчитывает более одного домена.

затем добавлять дополнительные домены, когда модель одиночного домена более не будет удовлетворять поставленным требованиям. Компания Microsoft рекомендует всегда, когда это только возможно, организовывать одиночный домен, и только в исключительных случаях - строить домен как часть леса. Один домен может располагаться в нескольких сайтах и содержать миллионы объектов. Структуры сайта и домена гибкие и существуют отдельно. Одиночный домен может располагаться в нескольких географических сайтах, а одиночный сайт может содержать пользователей и компьютеры, принадлежащие нескольким доменам.

Не требуется создавать раздельные деревья доменов только для отображения структуры отделов и подразделений предприятия. В домене для этих целей можно использовать подразделения. Затем можно настроить групповую политику и включить пользователей, группы и компьютеры в подразделения.

Существует несколько причин для создания более одного домена.

- Различные требования к паролям для отделов и подразделений.
- Большое количество объектов.
- Различные имена доменов в Интернете.
- Расширенные возможности управления репликацией.
- Децентрализованное администрирование сети.

Хотя использование одиночного домена для всей сети имеет несколько преимуществ, для удовлетворения дополнительных требований к масштабируемости, безопасности или репликации можно создать один или более доменов для предприятия. Ознакомление с принципами репликации данных каталога между контроллерами домена поможет спланировать количество доменов, необходимых данной организации. Несколько доменов может понадобиться, если имеется децентрализованная сеть, в которой различные подразделения управляются абсолютно разными администраторами. При наличии нескольких доменов каждая группа администраторов может устанавливать собственные политики безопасности, которые не зависят от политик других доменов. Кроме того, для международных организаций может быть легче обеспечить администрирование пользователями и ресурсами на языке каждой страны.

Все домены леса имеют один и тот же глобальный каталог, и прошедшие проверку пользователи каждого домена получают доступ к ресурсам в других доменах леса. Деревья доменов в основном используются для установки раздельных пространств имен. Все домены в дереве имеют связанное пространство DNS-имен. Если текущая сеть относится к связанному пространству DNS-имен, может понадобиться объединить все домены в одно дерево доменов. Также можно объединить организации с уникальными именами доменов в лес. Каждое дерево в составе леса имеет собственное уникальное пространство имен.

Дочерний домен следует создавать, когда требуется создать домен, имеющий общее связанное пространство имен с одним или несколькими доменами. Это означает, что имя нового дочернего домена содержит полное имя родительского домена. Например, домен `filial.firma.spb.ru` будет дочерним для домена `firma.spb.ru.` Для иерархической

организации доменов в организации следует использовать данную структуру дерева доменов.

Для создания домена, имя которого не связано с остальными доменами леса, следует создавать корень нового дерева доменов. Создавать новые деревья доменов необходимо, если требуется включить домены различных отделов организации в один лес и оставить их собственные имена доменов в Интернете неизменными.

Если в определенном домене уже имеется один контроллер домена, можно добавить дополнительные контроллеры в данный домен для увеличения доступности и надежности сетевых служб. Наличие более одного контроллера в домене позволяет функционировать домену в случае отказа одного из контроллеров домена, либо в случае необходимости отключения одного из контроллеров по какой-либо причине. Наличие нескольких контроллеров домена также может повысить производительность, облегчая клиентам Windows подключение к контроллеру домена при входе в сеть.

Если сеть разделена на сайты, рекомендуется иметь хотя бы один контроллер домена в каждом сайте. Частью процесса входа клиентов в сеть является подключение к контроллеру домена. Если клиентам требуется осуществлять доступ к контроллеру домена через медленное сетевое подключение, то процесс входа в сеть может занять неприемлемое количество времени. Размещение контроллера домена в каждом сайте позволяет выполнять процесс входа в сеть внутри сайта без использования медленных подключений между сайтами.

Основные контрольные вопросы

1. Что такое домен? Какие преимущества перед рабочими группами имеет доменная организация вычислительной сети?
2. Чем отличается главный контроллер домена (PDC) от резервного (BDC)? Сколько главных контроллеров домена может быть в домене? Сколько резервных контроллеров домена может быть в домене?
3. Что такое служба каталога? Какие преимущества по сравнению с обычными доменными сетями имеют сети на основе службы каталога? Какие сетевые операционные системы, основанные на идеях службы каталога Вы знаете?
4. Объясните следующие понятия: домен, доменное дерево, лес.
5. Что такое сайт и что такое подразделение? Для чего домен иногда разбивают на сайты и для чего – на подразделения? Можно ли домен разделять и на сайты, и на подразделения?
6. В чем заключаются основные различия между смешанным режимом (mixed mode) работы Active Directory и основным режимом (native mode)?
7. Что означают слова «один домен доверяет другому»? Каким свойством обладают домены, принадлежащие одному лесу?
8. Кто имеет право добавлять рабочие станции в домен? Может ли не администратор домена подключить свой компьютер в домен, если для этого компьютера уже есть учетная запись в активном каталоге?

Рекомендуемая литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 5-е изд. - СПб.: Питер, 2016. - 944 с.
2. Таненбаум Э. Компьютерные сети. 5-е изд. - СПб.: Питер, 2012. - 992 с.
3. Гордеев А.В. Открытые системы. Текст лекций. - СПб.: ГУАП, 2017. - 111с.
4. Гордеев А.В. Операционные системы. Учебник. - СПб: Питер, 2009. - 416с.
5. https://anydesk.com/ru
6. https://www.teamviewer.com/ru/

Содержание