**Лекция 6. АДРЕСАЦИЯ В IP-СЕТЯХ**

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

**6.1. Физический адрес**

**Физический,**или**локальный адрес узла** определяется технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети, это МАС-адрес сетевого адаптера или порта маршрутизатора.

В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Понятно, что столько сетевых адаптеров никогда не будет выпущено.

С тем, чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса (рис. 6.1).

I/G

U/L

OUI (уникальный идентификатор)

OUA (уникальный адрес)

1 бит

1 бит

22 бита

24 бита

UAA (46 бит)

Рис. 6.1.  Структура 48-битного стандартного MAC-адреса

Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) – ***уникальный адрес***. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, то есть каждый изготовитель может выпустить 16 миллионов сетевых адаптеров.

Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) – ***уникальный идентификатор***. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей. Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.

Два старших разряда адреса управляющие, они определяют тип адреса, способ интерпретации остальных 46 разрядов. Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46-ю младшими разрядами. Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

Для широковещательной передачи (то есть передачи всем абонентам сети одновременно) применяется специально выделенный ***сетевой адрес***, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

Данной системы адресов придерживаются такие популярные сети, как Ethernet, Fast Ethernet, Token-Ring, FDDI, 100VG-AnyLAN. Ее недостатки – высокая сложность аппаратуры сетевых адаптеров, а также большая доля служебной информации в передаваемом пакете (адреса источника и приемника вместе требуют уже 96 битов пакета или 12 байт).

Во многих сетевых адаптерах предусмотрен так называемый циркулярный режим. В этом режиме адаптер принимает все пакеты, приходящие к нему, независимо от значения поля адреса приемника. Такой режим используется, например, для проведения диагностики сети, измерения ее производительности, контроля ошибок передачи. При этом один компьютер принимает и контролирует все пакеты, проходящие по сети, но сам ничего не передает. В данном режиме работают сетевые адаптеры мостов и коммутаторы, которые должны обрабатывать перед ретрансляцией все пакеты, приходящие к ним.

**6.2. Сетевой адрес**

***6.2.1. Представление IP-адреса***

Адрес IP представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемые **октетами**. Например, 00010001 11101111 00101111 01011110.

Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками. Таким образом, приведенный выше IP-адрес можно записать в следующей форме: 17.239.47.94.

Следует заметить, что максимальное значение октета равно 111111112 (двоичная система счисления), что соответствует в десятичной системе 25510. Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, а 172.16.123.256 – несуществу-ющий адрес, поскольку 256 выходит за пределы допустимого диапазона: от 0 до 255.

IP-адрес состоит из двух логических частей – ***номера подсети*** (IDподсети) и ***номера узла*** (ID хоста) в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом: ID подсети 172.16.0.0; ID хоста 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно *N*, то общее количество узлов равно 2*N* – 2. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно 216 – 2 = 65534 узла.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа: с помощью классов и с помощью масок.

***Общее правило****:* под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Рассмотрим конфигурирование IP-адресации (v4) в операционных системах типа *Windows.*

*Пример 1.* Рассмотрим настройку протокола TCP/IP v4.

1. [Запустите папку *Сетевые подключения*](http://technet.microsoft.com/ru-ru/library/cc771878%28WS.10%29.aspx). Для этого в операционных системах типа Windows Seven необходимо нажать кнопку «Пуск», ввести в строке поиска начальные буквы слова «Центр». Из списка выберите пункт «Центр управления сетями и общим доступом» (рис. 6.2).

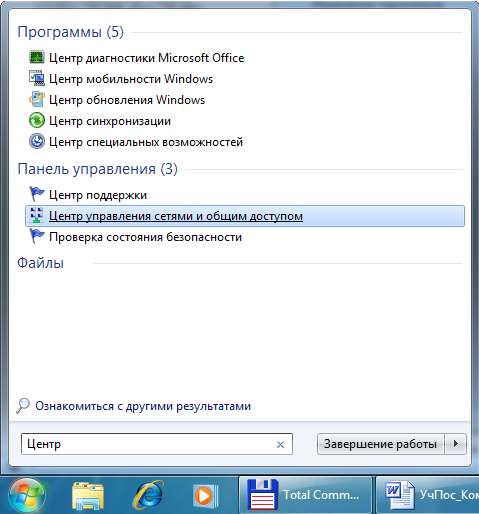


Рис. 6.2. Пример вызова Центра управления сетями и общим доступом

2. В окне Центра управления сетями и общим доступом щелкните по *изменению параметров адаптера* (рис. 6.3). Далее откроется окно с сетевыми подключениями (рис. 6.4).

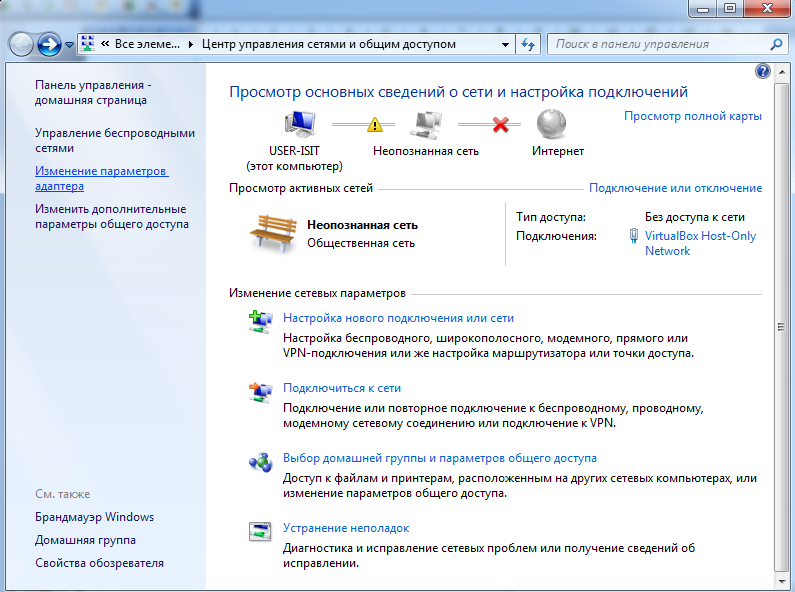


Рис. 6.3. Общий вид центра управления сетями и общим доступом

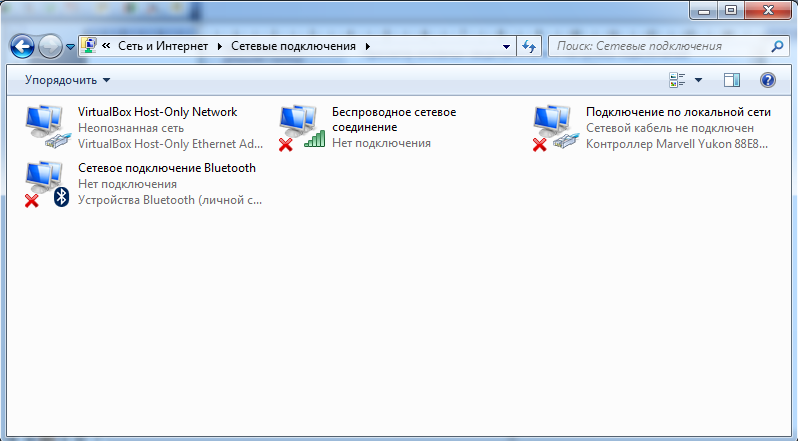


Рис. 6.4. Общий вид папки Сетевые подключения

3. Щелкните правой кнопкой мыши по подключению, которое требуется настроить, а затем выберите команду *Свойства*. Если появится диалоговое окно *Управление учетной записью пользователя*, убедитесь, что действие, указанное в окне, совпадает с тем, которое вы хотите выполнить, и нажмите *Продолжить*.

4. Далее выполните одно из указанных ниже действий:

* + в случае подключения по локальной сети на вкладке *Общие* в списке *Компоненты*, используемые этим подключением, выберите пункт *Протокол Интернета версии 4 (TCP/IPv4)* и нажмите кнопку *Свойства*;
  + в случае подключения удаленного доступа, VPN-подключения или высокоскоростного подключения на вкладке *Сеть* в списке *Компоненты*, используемые этим подключением, выберите пункт *Протокол Интернета версии 4 (TCP/IPv4)* и нажмите кнопку *Свойства*. В результате откроется окно с настройками протокола TCP/IP (рис. 6.5).

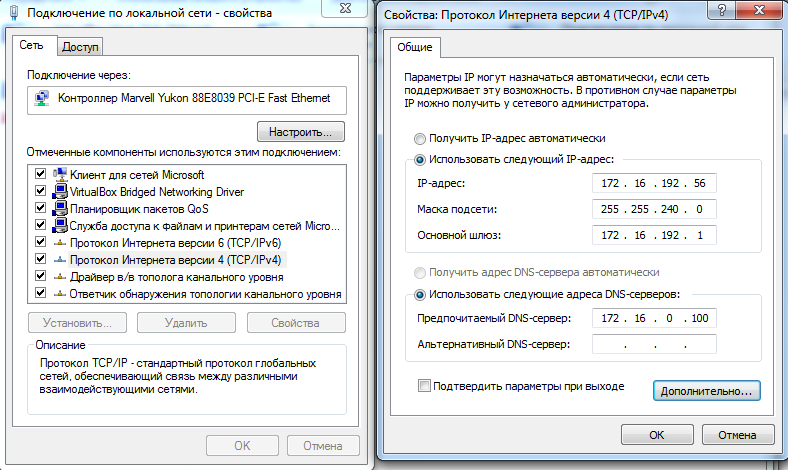


Рис. 6.5. Свойства Протокола Интернета версии 4 (TCP/IPv4)

5. Выполните далее одно из указанных ниже действий:

* + если необходимо, чтобы параметры IP-адреса назначались автоматически, выберите пункт Получить IP-адрес автоматически и нажмите кнопку ОК;
  + если необходимо указать IP-адрес IPv4 или адрес DNS-сервера, выполните следующие действия:

1. выберите пункт *Использовать следующий IP-адрес* и в поле *IP-адрес* введите IP-адрес, соответствующую маску подсети и адрес шлюза по умолчанию (в примере на рис. 6.5 IP адрес: 172.16.192.56; маска подсети: 255.255.240.0; основной шлюз: 172.16.192.1);
2. выберите пункт *Использовать следующие адреса DNS-серверов* и в полях *Предпочитаемый DNS-сервер и Альтернативный DNS-сервер* введите адреса основного и дополнительного DNS-сервера (в примере на рис. 65.5. IP-адрес предпочитаемого DNS сервера: 172.16.0.100;
3. для настройки параметров DNS, WINS и IP нажмите кнопку *Дополнительно* (рис. 6.6).

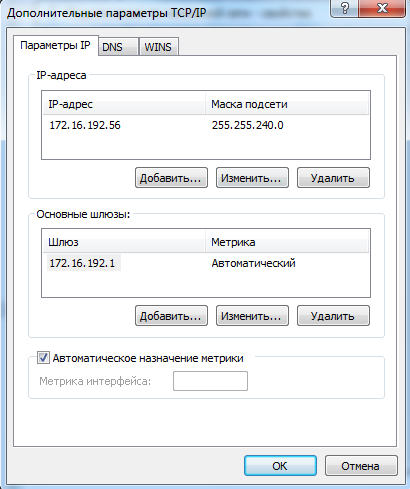


Рис. 6.6. Окно с дополнительными параметрами TCP/IP

6. В подключении по локальной сети при выборе параметра *Получить IP-адрес автоматически* включается вкладка *Альтернативная конфигурация*. Если компьютер используется более чем в одной сети, используйте эту вкладку для ввода альтернативных параметров IP-адреса. Для настройки параметров DNS, WINS и IP откройте вкладку *Настраиваемый пользователем или Альтернативная конфигурация.*

*Дополнительные рекомендации.* Если это возможно, используйте автоматическую настройку параметров протокола IP (DHCP), поскольку при этом устраняется необходимость настройки таких параметров, как IP-адрес, адрес DNS-сервера и адрес WINS-сервера.

Параметры *Альтернативная конфигурация* определяют второй набор параметров протокола IP, который используется при недоступности DHCP-сервера. Это весьма полезно для пользователей портативных компьютеров, которые часто перемещаются между двумя различными сетевыми средами (например, между средой со службой DHCP и средой со статическими IP-адресами).

Отметим, что аналогично осуществляется конфигурирование TCP/IPv6 (используются *свойства* *Протокол Интернета версии 6 (TCP/IPv6)*).

***6.2.2. Классы IP-адресов***

Существует пять классов IP-адресов: *A, B, C, D* и *E* (рис. 6.7).

Номер узла

Номер сети

0

1 байт

3 байта

4 байта

Номер узла

Номер сети

1

2 байта

2 байта

0

Номер узла

Номер сети

1

3 байта

1 байт

0

0

Адрес группы Multicast

1

0

0

0

Зарезервирован

1

0

0

0

0

Класс A

Класс B

Класс C

Класс D

Класс E

Рис. 6.7. Классы IP-адресов

За принадлежность к тому или иному классу отвечают первые биты IP-адреса. Деление сетей на классы описано в RFC 791 (документ описания протокола IP).

Целью такого деления являлось создание малого числа больших сетей (***класса А***), умеренного числа средних сетей (***класс* *В***) и большого числа малых сетей (***класс С***).

Если адрес начинается с 0, то сеть относят к *классу А* и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. Сетей класса А немного, зато количество узлов в них может достигать 224 – 2, то есть 16 777 214 узлов.

Если первые два бита адреса равны 10, то сеть относится к *классу В.* В сетях класса В под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса В является сетью средних размеров с максимальным числом узлов 216 – 2, что составляет 65 534 узлов.

Если адрес начинается с последовательности 110, то это сеть *класса С.* В этом случае под номер сети отводится 24 бита, а под номер узла – 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 28 – 2, то есть 254 узлами.

Адрес, начинающийся с 1110, обозначает особый, **групповой адрес** *(*multicast*).* Пакет с таким адресом направляется всем узлам, которым присвоен данный адрес.

Адреса *класса Е* в настоящее время не используются (зарезервированы для будущих применений).

Характеристики адресов разных классов представлены в табл. 6.1.

Таблица 6.1

**Характеристики IP-адресов разных классов**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Класс | Первые биты | Наименьший номер сети | Наибольший номер сети | Количество сетей | Максимальное число узлов в сети |
| *А* | 0 | 1.0.0.0 | 126.0.0.0 | 126 | 224 – 2 = 16777214 |
| *В* | 10 | 128.0.0.0 | 191.255.0.0 | 16384 | 216 – 2 = 65534 |
| *С* | 110 | 192.0.0.0 | 223.255.255.0 | 2097152 | 28 – 2 = 254 |
| *D* | 1110 | 224.0.0.0 | 239.255.255.255 | Групповой адрес | |
| *Е* | 11110 | 240.0.0.0 | 247.255.255.255 | Зарезервирован | |

Применение классов удовлетворительно решало задачу деления на подсети в начале развития Интернета. В 90-е годы с увеличением числа подсетей стал ощущаться дефицит IP-адресов. Это связано с неэффективностью распределения при классовой схеме адресации. Например, если организации требуется тысяча IP-адресов, ей выделяется сеть класса В, при этом 64 534 адреса не будут использоваться.

Существует два основных способа решения этой проблемы:

* более эффективная схема деления на подсети с использованием масок (RFC 950);
* применение протокола IP версии 6 (IPv6).

***6.2.3. Использование масок***

**Маска подсети**(subnet mask) – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети.

Для стандартных классов сетей маски имеют следующие значения:

* *класс А* – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
* *класс В* – 11111111.11111111.00000000. 00000000 (255.255.0.0);
* *класс С* – 11111111.11111111.11111111.00000000 (255.255.255.0).

Маска подсети записывается либо в виде, аналогичном записи IP-адреса, например 255.255.255.0, либо совместно с IP-адресом с помощью указания числа единичных разрядов в записи маски, например 192.168.1.1/24, т. е. в маске содержится 24 единицы (255.255.255.0).

При использовании масок можно вообще отказаться от понятия классов.

*Пример 2.* Пусть задан IP-адрес 17.239.47.94, маска подсети 255.255.0.0 (другая форма записи: 17.239.47.94/16).

Требуется определить ID подсети и ID хоста в обеих схемах адресации.

1) *Адресация с использованием классов*. Двоичная запись IP-адреса имеет вид:

00010001.11101111.00101111.01011110.

Так как первый бит равен нулю, адрес относится к *классу А*. Следовательно, первый байт отвечает за ID подсети, остальные три байта – за ID хоста:

ID подсети: 17.0.0.0. ID хоста: 0.239.47.94.

2) *Адресация с использованием масок*. Запишем IP-адрес и маску подсети в двоичном виде:

IP-address: 17.239.47.94 = 00010001.11101111.00101111.01011110 ,

Subnet mask: 255.255.0.0 = 11111111.11111111.00000000.00000000 .

Вспомнив определение маски подсети, можно интерпретировать номер подсети как те биты, которые в маске равны 1, т. е. первые два байта. Оставшаяся часть IP-адреса будет номером узла в данной подсети.

ID подсети: 17.239.0.0. ID хоста: 0.0.47.94.

Номер подсети можно получить другим способом, применив к IP-адресу и маске операцию логического умножения или *конъюнкции* (AND):

AND 00010001. 11101111. 00101111. 01011110

11111111. 11111111. 00000000. 00000000 .  
 00010001. 11101111. 00000000. 00000000  
 17 239 0 0

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8.

*Пример 3.* Задан IP-адрес 192.168.89.16, маска подсети – 255.255.192.0 (другая форма записи: 192.168.89.16/18).

Требуется определить ID подсети и ID хоста. Воспользуемся операцией AND:

IP-address: 192.168.89.16 = AND11000000.10101000.01011001.00010000  
Subnet mask: 255.255.0.0 =  11111111.11111111.11000000.00000000.  
subnet ID: 11000000.10101000.01000000.00000000

192 168 64 0

Чтобы получить номер узла, нужно в битах, отвечающих за номер подсети, поставить нули:

Host ID: 00000000.00000000.00011001.00010000 = 0.0.25.16.

*Ответ:* ID подсети = 192.168.64.0, ID хоста = 0.0.25.16.

*Для масок существует важное правило: разрывы в последовательности единиц или нулей недопустимы.*

Например, не существует маски подсети, имеющей следующий вид:

11111111.11110111.00000000.00001000 (255.247.0.8),

так как последовательности единиц и нулей не являются непрерывными.

С помощью масок администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей.

*Пример 4.* Допустим, организации выделена сеть класса *В*: 160.95.0.0 (рис. 6.8).

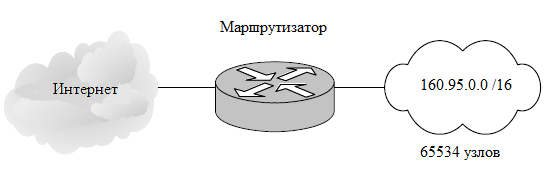


Рис. 6.8. Сеть класса В до деления на подсети

В такой сети может находиться до 65 534 узлов. Однако организации требуется 3 независимые сети с числом узлов в каждой не более 254. В этой ситуации можно применить деление на подсети с помощью масок. Например, при использовании маски 255.255.255.0 третий байт адреса будет определять номер внутренней подсети, а четвертый байт – номер узла (рис. 6.9).

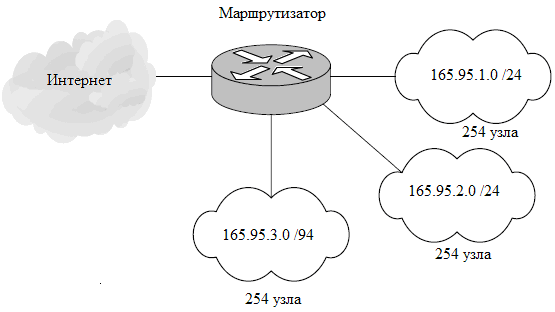


Рис. 6.9. Сеть класса В после деления на подсети

Маршрутизаторы во внешней сети (Интернет) ничего «не знают» о делении сети 160.95.0.0 на подсети, все пакеты направляются на маршрутизатор организации, который переправляет их в требуемую внутреннюю подсеть.

***5.2.4. Протокол IPv6***

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов. Для преодоления ограничений IPv4 был разработан ***протокол IP 6-й версии***– ***IPv6***(RFC 2373, 2460).

Протокол IPv6 имеет следующие основные особенности:

* длина адреса 128 бит – такая длина обеспечивает примерно 3,4×1038 адресов; такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;
* автоматическая конфигурация – протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;
* встроенная безопасность – для передачи данных является обязательным использование *протокола защищенной передачи* IPsec (протокол IPv4 также может использовать IPsec, но не обязан этого делать).

В настоящее время многие производители сетевого оборудования включают поддержку протокола IPv6 в свои продукты, однако преобладающим остается протокол IPv4. Связано это с тем, что IPv6 обратно несовместим с IPv4 и процесс перехода сопряжен с определенными трудностями.

***6.2.5. Особые IP-адреса***

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей.

1. Если первый октет ID сети начинается с 127, такой адрес считается адресом машины-источника пакета. В этом случае пакет не выходит в сеть, а возвращается на компьютер-отправитель. Такие адреса называются **loopback**(«**петля**», «замыкание на себя») и используются для проверки функционирования стека TCP/IP.
2. Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.
3. Если все биты IP-адреса равны 1, адрес называется ***ограниченным широковещательным***(limited broadcast).Пакеты, направленные по такому адресу рассылаются всем узлам той подсети, в которой находится отправитель пакета.
4. Если все биты ID хоста равны 1, адрес называется ***широковещательным***(broadcast);пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
5. Если все биты ID хоста равны 0, адрес считается **идентификатором подсети** (subnet ID).

Наличие особых IP-адресов объясняет, почему из диапазона доступных адресов исключаются два адреса – это случаи, когда все биты ID хоста равны 1 или 0. Например, в сети *класса* *С* не 256, а 254 узлов.

***6.2.6. Автоматизация назначения IP-адресов узлам сети – протокол DHCP***

Как уже было сказано, IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети, и должны поэтому полагаться на администраторов.

Протокол Dynamic Host Configuration Protocol (DHCP) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Служба DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра «продолжительности аренды», который определяет, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от сервера DHCP в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Рассмотрим пример настройки DHCP-сервера (в ОС Windows 2003 Server).

*Пример 5*

*1. Установка и авторизация сервера DHCP*

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

Для авторизации сервера DHCP необходимо запустить появившуюся в разделе *«Администрирование»* консоль управления службой DHCP с правами пользователя, являющегося членом группы *«Администраторы»*. Если текущая рабочая учетная запись не входит в данную группу, то для запуска консоли с соответствующими полномочиями необходимо щелкнуть правой кнопкой мыши на ярлыке консоли и выбрать пункт меню *«Запуск от имени…»* (рис. 6.10), после чего указать имя пользователя, являющегося членом группы *«Администраторы»* и ввести его пароль.

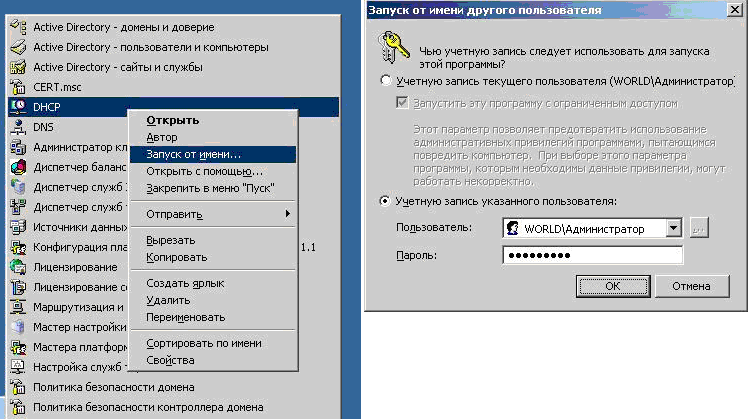


Рис. 6.10. Запуск службы DHCP

Для авторизации сервера необходимо в консоли DHCP выбрать сервер, щелкнуть на имени сервера правой кнопкой мыши и выбрать пункт меню *«Авторизовать»* (рис. 6.11).

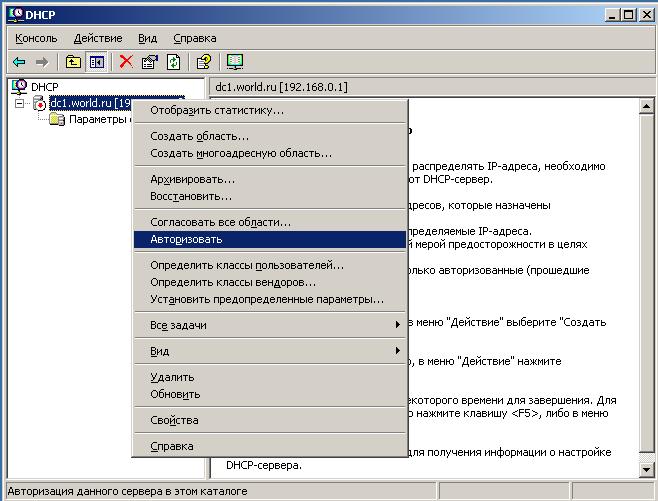


Рис. 6.11. Авторизация DHCP сервера

Когда авторизация будет завершена, значок у имени сервера изменится – вместо красной стрелки, направленной вниз, появится зеленая стрелка, направленная вверх.

*2. Настройка параметров DHCP-сервера*

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

*Имя и описание области*. В больших сетях именование областей и задание их краткого описания облегчает работу администратора за счет более наглядного отображения в консоли всех созданных областей (рис. 6.12).

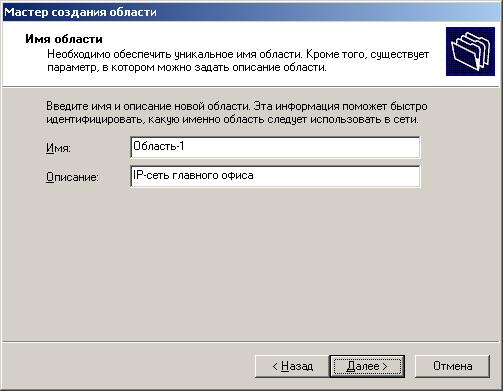


Рис. 6.12 Создание области DHCP-сервера

*Определение диапазона* IP-адресов и маски подсети (рис. 6.13).

*Добавление исключений*. На данном шаге задаются диапазоны IP-адресов, которые будут исключены из процесса выдачи адресов клиентам.

*Срок действия аренды*. Стандартный срок действия – 8 дней. Если в вашей сети редко происходят изменения (добавление или удаление сетевых узлов, перемещение сетевых узлов из одной подсети в другую), то срок действия можно увеличить, это сократит количество запросов на обновление аренды. Если же ваша сеть более динамичная, то срок аренды можно сократить, это позволит быстрее возвращать в пул IP-адреса, которые принадлежали компьютерам, уже удаленным из данной подсети.

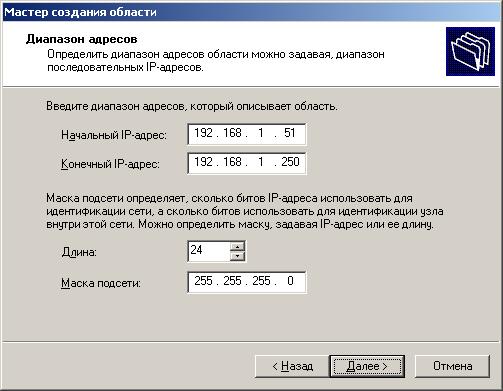


Рис. 6.13. Создание диапазона адресов области

Далее мастер предложит настроить параметры, специфичные для узлов IP-сети, относящихся к данной области: маршрутизатор (основной шлюз; рис. 6.14); адрес DNS-сервера (можно назначить несколько адресов; рис. 6.15); адрес WINS-сервера (аналогично серверу DNS; можно также назначить несколько адресов).

*Запрос на активацию области*. IP-адреса, заданные в созданной области, не будут выдаваться клиентам, пока область не будет активирована (рис. 6.16).

Нажимаем кнопку *«Готово»* и завершаем работу мастера. Область готова к использованию. Если какие-либо параметры (например, адреса серверов DNS или WINS) являются общими для всех областей, управляемых данным DHCP-сервером, то такие параметры лучше определить не в разделе параметров каждой области, а в разделе параметров самого сервера (рис. 6.17). Нажимаем кнопку *«Готово»* и завершаем работу мастера. Область готова к использованию.

Если какие-либо параметры (например, адреса серверов DNS или WINS) являются общими для всех областей, управляемых данным DHCP-сервером, то такие параметры лучше определить не в разделе параметров каждой области, а в разделе параметров самого сервера (рис. 6.17).

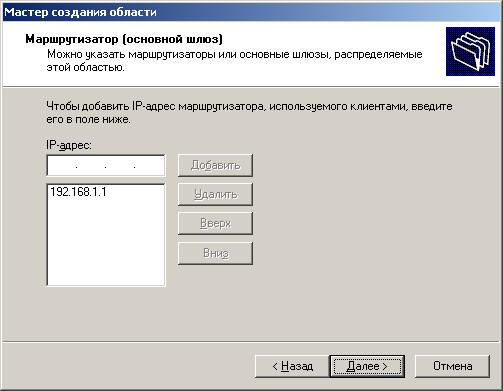


Рис. 6.14. Добавление адреса шлюза, распределяемого областью

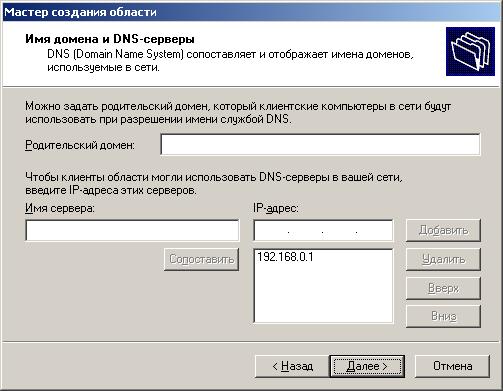


Рис. 6.15. Добавление адреса DNS-сервера, распределяемого областью

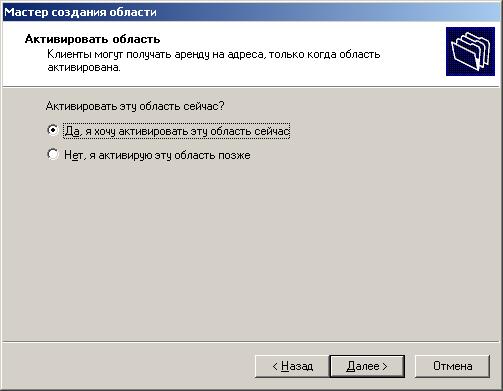


Рис. 6.16. Запрос на активацию области DHCP-сервера

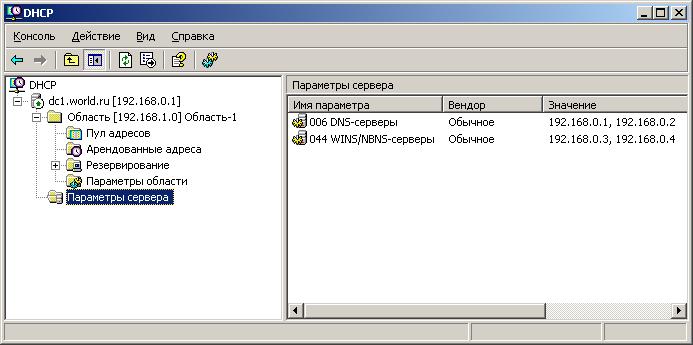


Рис. 6.17. Общие параметры DHCP-сервера

Протокол DHCP использует модель клиент-сервер. Во время старта системы компьютер – клиент DHCP, находящийся в состоянии «инициализация», посылает сообщение discover (исследовать), которое широковещательно распространяется по локальной сети и передается всем DHCP-серверам частной интерсети. Каждый DHCP-сервер, получивший это сообщение, отвечает на него сообщением offer (предложение), которое содержит IP-адрес и конфигурационную информацию.

Компьютер-клиент DHCP переходит в состояние «выбор» и собирает конфигурационные предложения от DHCP-серверов. Затем он выбирает одно из этих предложений, переходит в состояние «запрос» и отправляет сообщение request (запрос) тому DHCP-серверу, чье предложение было выбрано.

Выбранный DHCP-сервер посылает сообщение DHCP-acknowledgment (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, DHCP-сервер посылает параметры сетевой конфигурации. После того, как клиент получит это подтверждение, он переходит в состояние «связь», находясь в котором он может принимать участие в работе сети TCP/IP. Компьютеры-клиенты, которые имеют локальные диски, сохраняют полученный адрес для использования при последующих стартах системы. При приближении момента истечения *срока аренды адреса* компьютер пытается обновить параметры аренды у DHCP-сервера, а если этот IP-адрес не может быть выделен снова, то ему возвращается другой IP-адрес.

Однако использование DHCP несет в себе и некоторые проблемы. Во-первых, это проблема согласования информационной адресной базы в службах DHCP и DNS. Как известно, DNS служит для преобразования символьных имен в IP-адреса. Если IP-адреса будут динамически изменятся сервером DHCP, то эти изменения необходимо также динамически вносить в базу данных сервера DNS.

Во-вторых, нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов. Аналогичные проблемы возникают и при конфигурировании фильтров маршрутизаторов, которые оперируют с IP-адресами.

Наконец, централизация процедуры назначения адресов снижает надежность системы: при отказе DHCP-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации. Последствия такого отказа могут быть уменьшены путем использовании в сети нескольких серверов DHCP, каждый из которых имеет свой пул IP-адресов.

***6.2.7. Распределение IP-адресов***

Поскольку каждый узел сети Интернет должен обладать уникальным IP-адресом, то, безусловно, важной является задача координации распределения адресов отдельным сетям и узлам. Такую координирующую роль выполняет Интернет-корпорация по распределению адресов и имен (The Internet Corporation for Assigned Names and Numbers, ICANN).

Естественно, что ICANN не решает задач выделения IP-адресов конечным пользователям и организациям, а занимается распределением диапазонов адресов между крупными организациями-поставщиками услуг по доступу к сети Интернет (Internet Service Provider), которые, в свою очередь, могут взаимодействовать как с более мелкими поставщиками, так и с конечными пользователями. Так, например функции по распределению IP-адресов в Европе ICANN делегировал Координационному Центру RIPE (RIPE NCC, The RIPE Network Coordination Centre, RIPE – Reseaux IP Europeens). В свою очередь, этот центр делегирует часть своих функций региональным организациям.

* + 1. ***Частные адреса***

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных сетей три блока адресов:

10.0.0.0 – 10.255.255.255 (маска 255.0.0.0);

172.16.0.0 – 172.31.255.255 (маска 255.255.0.0);

192.168.0.0 – 192.168.255.255 (маска 255.255.255.0).

Будем называть первый блок 24‑битовым, второй – 20‑битовым, а третий – 16‑битовым. Отметим, что первый блок представляет собой не что иное, как одну сеть класса *А*, второй блок – 16 последовательных сетей класса *В*, а третий блок – 256 последовательных сетей класса *С*.

Любая организация может использовать IP‑адреса из этих блоков без согласования с ICANA или Internet‑регистраторами. В результате эти адреса используются во множестве организаций. Таким образом, уникальность адресов сохраняется только в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов. В такой сети каждая рабочая станция может обмениваться информацией с любой другой рабочей станцией частной сети.

Если организации требуются уникальные адреса для связи с внешними сетями, такие адреса следует получать обычным путем через регистраторов Internet. Такие адреса никогда не будут входить ни в один из указанных выше блоков частных адресов.

Перед распределением адресов из частного и публичного блоков следует определить, какие из рабочих станций сети должны иметь связь с внешними системами на сетевом уровне.  Для таких рабочих станций следует использовать публичные адреса, остальным же – можно присваивать адреса из частных блоков, это не помешает им взаимодействовать со всеми рабочими станция частной сети организации, независимо от того, какие адреса используются (частные или публичные). Однако прямой доступ во внешние сети для рабочих станций с адресами из частного блока невозможен. Для организации их доступа во внешние шлюзы придется использовать прокси-серверы.

Перемещение рабочей станции из частной сети в публичную (и обратное) связано со сменой IP-адреса, соответствующих записей DNS и изменением конфигурационных файлов на других рабочих станцях, которые их идентифицируют по IP-адресам. Поскольку частные адреса не имеют глобального значения, маршрутная информация о частных сетях не должна выходить за пределы этих сетей, а пакеты с частными адресами отправителей или получателей не должны передаваться через межсетевые каналы. Предполагается, что маршрутизаторы в публичных сетях (особенно маршрутизаторы провайдеров Internet) будут отбрасывать маршрутную информацию из частных сетей. Если маршрутизатор публичной сети получает такую информацию, ее отбрасывание не должно трактоваться как ошибка протокола маршрутизации.

**6.3. Символьный адрес**

***6.3.1. DNS-имена***

**DNS** (Domain Name System) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.

*Служба DNS* предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, разрешающих имена компьютеров в IP-адреса.

**Протокол DNS** является служебным протоколом прикладного уровня. Этот протокол несимметричен – в нем определены DNS-серверы и DNS-клиенты.

**DNS-серверы** хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес. Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет – то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого **доменным пространством имен**, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены.

**Имя домена** идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

*Корень базы данных DNS* управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны отвечать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

* ***com*** – коммерческие организации (например, microsoft.com);
* ***edu*** – образовательные (например, mit.edu);
* ***gov*** – правительственные организации (например, nsf.gov);
* ***org*** – некоммерческие организации (например, fidonet.org);
* ***net*** – организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой ***домен*** на ***поддомены*** и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню.

Рассмотрим пример организации DNS-адресации в локальной сети.

*Пример 6.* Для организации DNS-адресации необходимо выполнить определенные действия на двух серверах (с именами DC1 и DC2) и клиенте.

*1.* *Установка DNS-сервера*

Установка службы DNS производится достаточно просто с помощью мастера установки компонент Windows:

* откройте *«Панель управления»*;
* выберите пункт *«Установка и удаление программ»*;
* нажмите кнопку *«Установка компонентов Windows»* (рис. 6.18);
* выберите *«Сетевые службы»* – кнопка *«Дополнительно»* (ни в коем случае не ставьте галочку у названия *«Сетевые службы»*);
* отметьте службу DNS;
* кнопка *«ОК»*, кнопка *«Далее»*, кнопка *«Готово»* (если система попросит указать путь к дистрибутиву системы, введите путь к папке с дистрибутивом).

Выполним данные действия на обоих серверах.

*2. Создание основной зоны прямого просмотра*

На сервере DC1 создадим стандартную основную зону с именем world.ru:

* откройте консоль DNS;
* выберите раздел «Зоны прямого просмотра»;
* запустите мастер создания зоны (тип зоны – «Основная», динамические обновления – разрешить, остальные параметры – по умолчанию);
* введите имя зоны – world.ru;
* разрешите передачу данной зоны на любой сервер DNS (Консоль DNS – зона world.ru – Свойства – Закладка «Передачи зон» – Отметьте «Разрешить передачи» и «На любой сервер»).

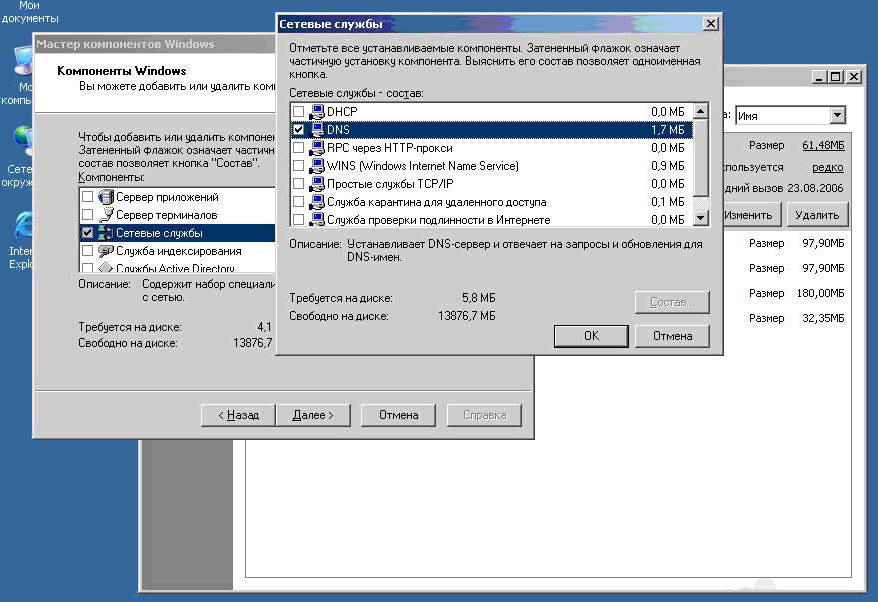


Рис. 6.18. Установка службы DNS

*3.* *Создание дополнительной зоны прямого просмотра*

На сервере DC2 создадим стандартную дополнительную зону с именем world.ru:

* откройте консоль DNS.;
* выберите раздел «Зоны прямого просмотра»;
* запустите мастер создания зоны (выберите: тип зоны – «Дополнительная», IP-адрес master-сервера (с которого будет копироваться зона) – адрес сервера DC1, остальные параметры – по умолчанию);
* введите имя зоны – world.ru.

*4.* *Настройка узлов для выполнения динамической регистрации на сервер DNS*

Для выполнения данной задачи нужно выполнить ряд действий как на сервере DNS, так и в настройках клиента DNS.

Насервере *DNS* необходимо:

* создать соответствующую зону;
* разрешить динамические обновления.
* На клиенте DNS необходимо сделать следующее:
* указать в настройках протокола TCP/IP адрес предпочитаемого DNS-сервера – тот сервер, на котором разрешены динамические обновления (в нашем примере – сервер DC1);
* в полном имени компьютера указать соответствующий DNS-суффикс (рис. 6.19) (в нашем примере – world.ru). Для этого последовательно инициировать: «Мой компьютер» – «Свойства» – Закладка «Имя компьютера» – Кнопка «Изменить» – Кнопка «Дополнительно» – в пустом текстовом поле вписать название домена world.ru – кнопка «ОК» (3 раза)).

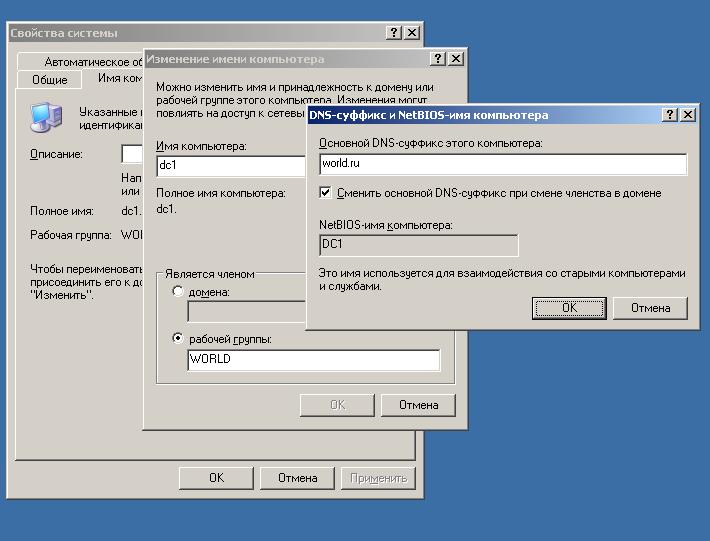


Рис. 6.19. Установка DNS-суффикса в полном имени компьютера

После этого система предложит перезагрузить компьютер. После выполнения перезагрузки на сервер DNS в зоне world.ru автоматически создадутся записи типа A для наших серверов (рис. 6.20).

*5.* *Создание зоны обратного просмотра* выполняется по следующим шагам:

* откройте консоль DNS;
* выберите раздел «Зоны обратного просмотра»;
* запустите мастер создания зоны (выберите: тип зоны – *«Основная»*, динамические обновления – разрешить, остальные параметры – по умолчанию);

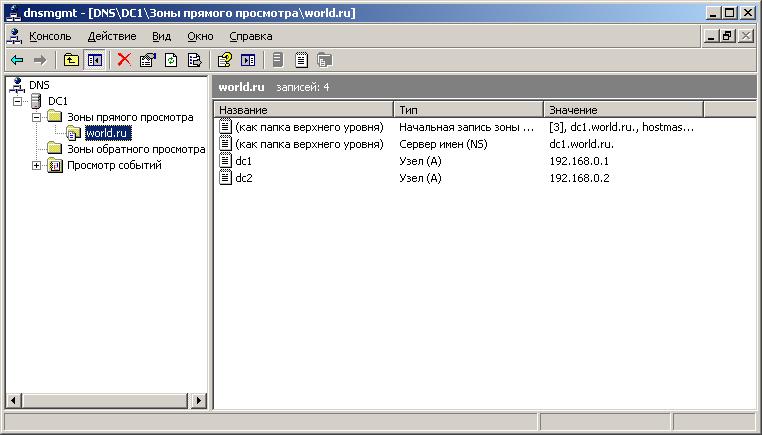


Рис. 6.20. Консоль DNS-сервера с зоной прямого просмотра

* в поле *«Код сети (ID)»* введите параметры идентификатора сети – «192.168.0», а затем выполните команду принудительной регистрации клиента на сервере DNS – *«ipconfig /registerdns»*.

В итоге серверы зарегистрируются в обратной зоне DNS (рис. 65.21).

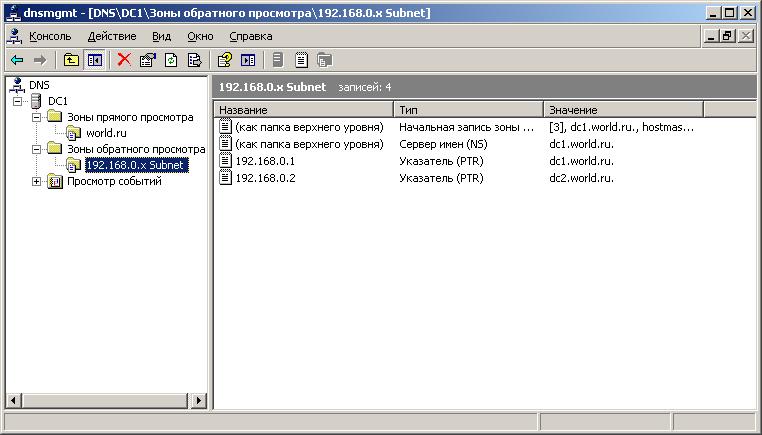


Рис. 6.21. Консоль DNS-сервера с зоной обратного просмотра

***5.3.2. Имена NetBIOS***

Протокол *NetBIOS* (Network Basic Input/Output System – сетевая базовая система ввода/вывода) был разработан в 1984 г. для корпорации IBM как сетевое дополнение стандартной BIOS на компьютерах IBM PC. Начиная с Windows 2000, операционные системы Microsoft ориентируются на глобальную сеть Интернет, в этой связи фундаментом сетевых решений стали протоколы TCP/IP и доменные имена. Однако поддержка имен NetBIOS осталась и в операционной системе Windows Server 2008.

**Система имен NetBIOS** представляет собой простое неиерархическое пространство, т. е. в имени NetBIOS отсутствует структура, деление на уровни, как в DNS-именах. Длина имени не более 15 символов (плюс один служебный).

Для преобразования NetBIOS-имен в IP-адреса в операционной системе Windows Server используется служба *WINS* – Windows Internet Naming Service (служба имен в Интернете для Windows).

Служба WINS работает, как и служба DNS, по модели «клиент-сервер». WINS-клиенты используют WINS-сервер для регистрации своего NetBIOS-имени и преобразования неизвестного NetBIOS-имени в IP-адрес. Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

**5.4. Утилиты диагностики TCP/IP и DNS**

Любая операционная система имеет набор диагностических утилит для тестирования сетевых настроек и функционирования коммуникаций. Большой набор диагностических средств есть и в системах семейства Windows (как графических, так и в режиме командной строки).

Утилиты командной строки, являющиеся инструментами первой необходимости для проверки настроек протокола TCP/IP и работы сетей и коммуникаций представлены в табл. 6.2. Подробное описание данных утилит содержится в системе интерактивной помощи Windows (вызывается нажатием кнопки *F1*). В табл. 6.2 указаны основные и наиболее часто используемые параметры этих команд, а также дано их краткое описание.

Таблица 6.2

**Утилиты диагностики TCP/IP и DNS**

|  |  |  |
| --- | --- | --- |
| Название  утилиты | Параметры | Комментарии |
| 1 | 2 | 3 |
| **ipconfig** | **/?** ­– Отобразить справку по команде  **/all** – Отобразить полную информацию о настройке параметров всех адаптеров  **/release** – Освободить динамическую IP-конфигурацию  **/renew** – Обновить динамическую IP-конфигурацию с DHCP-сервера  **/flushdns** – Очистить кэш разрешений DNS  **/registerdns** – Обновить регистрацию на DNS-сервере  **/displaydns** – Отобразить содержимое кэша разрешений DNS | Служит для отображения всех текущих параметров сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды ipconfig без параметров выводятся IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера |
| **arp** | **-a** — Отображает текущие ARP-записи | Отображение и изменение ARP-таблиц |
| **ping** | Формат команды:  **«ping <*сетевой узел*> параметры»**  Параметры:  **-t** – Бесконечная (до нажатия клавиш <Ctrl>+<Break>) отправка пакетов на указанный узел  **-a** – Определение имени узла по IP-адресу  **-n <число>** – Число отправляемых запросов  **-l <размер>** – Размер буфера отправки  **-w <таймаут>** – Таймаут ожидания каждого ответа в миллисекундах | Мощный инструмент диагностики (с помощью протокола ICMP). Команда ping позволяет проверить: работоспособность IP-соединения; правильность настройки протокола TCP/IP на узле; работоспособность маршрутизаторов; работоспособность системы разрешения имен FQDN или NetBIOS; доступность и работоспособность какого-либо сетевого ресурса |
| **tracert** | **-d** – Без разрешения IP-адресов в имена узлов  **-h <максЧисло>** – Максимальное число прыжков при поиске узла  **-w <таймаут>** – Таймаут каждого ответа в миллисекундах | Служебная программа для трассировки маршрутов, используемая для определения пути, по которому IP-дейтаграмма доставляется по месту назначения |
| **pathping** | **-n** – Без разрешения IP-адресов в имена узлов  **-h максЧисло** – Максимальное число прыжков при поиске узла  **-q <число\_запросов>** – Число запросов при каждом прыжке  **-w <таймаут>** – Таймаут каждого ответа в миллисекундах | Средство трассировки маршрута, сочетающее функции программ *ping* и *tracert* и обладающее дополнительными возможностями. Эта команда показывает степень потери пакетов на любом маршрутизаторе или канале, с ее помощью легко определить, какие маршрутизаторы или каналы вызывают неполадки в работе сети |
| **netstat** | **-a** – Отображение *всех* подключений и ожидающих (слушающих) портов  **-n** – Отображение адресов и номеров портов в числовом формате  **-o** – Отображение кода (ID) процесса каждого подключения  **-r** – Отображение содержимого локальной таблицы маршрутов | Используется для отображения статистики протокола и текущих TCP/IP-соединений |
| **nbtstat** | **–n** – Выводит имена пространства имен NetBIOS, зарегистрированные локальными процессами  **–c** – Отображает кэш имен NetBIOS (разрешение NetBIOS-имен в IP-адреса)  **–R** – Очищает кэш имен и перезагружает его из файла Lmhosts  **–RR** – Освобождает имена NetBIOS, зарегистрированные на WINS-сервере, а затем обновляет их регистрацию | Средство диагностики разрешения имен NetBIOS |
| **hostname** | Никаких ключей для данной утилиты не предусмотрено. | Это самая простая утилита – она выводит на экран имя компьютера |

Рассмотрим примеры использования утилит командной строки для диагностики протокола TCP/IP и символьной адресации (DNS).