Министерство образования Республики Беларусь
Учреждение образования «Полоцкий государственный университет»

Факультет информационных технологий
Кафедра технологий программирования

Методические указания
к выполнению лабораторной работы №1

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

на тему «**Настройка служб DHCP, DNS и WINS в Windows**»

Новополоцк, 2018 г.

Название: «Настройка служб DHCP, DNS и WINS в Windows».

Цель работы: Изучение протокола IP, понятий адреса подсети, маски подсети, назначений протоколов TCP/IP и UDP. Получение теоретических сведений о протоколе NetBIOS поверх TCP/IP. Получение практических навыков в настройке служб DHCP, DNS, WINS в ОС Windows 2003.

Теоретическая часть

Протокол IP

IP (англ. Internet Protocol – межсетевой протокол) – маршрутизируемый сетевой протокол, основа стека протоколов TCP/IP.

Протокол IP используется для негарантированной доставки данных от одного узла сети к другому. Это означает, что на уровне этого протокола (третий уровень сетевой модели OSI) не даётся гарантий надёжной доставки пакета до адресата. В частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться, оказаться повреждёнными или не прибыть вовсе. Гарантии безошибочной доставки пакетов дают протоколы более высокого (транспортного) уровня сетевой модели OSI – например, TCP – которые IP используют в качестве транспорта.

В современной сети Интернет используется IP четвёртой версии, также известный как IPv4. В протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета. При этом компьютеры в подсетях объединяются общими начальными битами адреса. Количество этих бит, общее для данной подсети, называется маской подсети.

В настоящее время вводится в эксплуатацию шестая версия протокола – IPv6, которая позволяет адресовать значительно большее количество узлов, чем IPv4. Эта версия отличается повышенной разрядностью адреса, встроенной возможностью шифрования и некоторыми другими особенностями. Переход с IPv4 на IPv6 связан с трудоёмкой работой операторов связи и производителей программного обеспечения и не может быть выполнен одномоментно.

Протокол UDP

Протокол UDP (User Datagram Protocol) является одним из основных протоколов, расположенных непосредственно над IP. Он предоставляет прикладным процессам транспортные услуги, немногим отличающиеся от услуг протокола IP. Протокол UDP обеспечивает доставку дейтограмм, но не требует подтверждения их получения. Протокол UDP не требует соединения с удаленным модулем UDP («бессвязный» протокол). К заголовку IP-пакета UDP добавляет поля порт отправителя и порт получателя, которые обеспечивают мультиплексирование информации между различными прикладными процессами, а также поля длина UDP-дейтограммы и контрольная сумма, позволяющие поддерживать целостность данных. Таким образом, если на уровне IP для определения места доставки пакета используется адрес, на уровне UDP - номер порта.

Протокол TCP/IP

The Transmission Control Protocol (TCP) (протокол управления передачей) – один из основных сетевых протоколов Internet, предназначенный для управления передачей данных в сетях и подсетях TCP/IP.

Выполняет функции протокола транспортного уровня упрощённой модели OSI.

TCP – это транспортный механизм, предоставляющий поток данных, с предварительной установкой соединения, за счёт этого дающий уверенность в достоверности получаемых данных, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета. В отличие от UDP, гарантирует, что приложение получит данные точно в такой же последовательности, в какой они были отправлены, и без потерь.

Реализация TCP как правило, встроена в ядро системы, хотя есть и реализации TCP в контексте приложения.

TCP часто обозначают «TCP/IP». Когда осуществляется передача от компьютера к компьютеру через Internet, TCP работает на верхнем уровне между двумя конечными системами, например, интернет-браузер и интернет-сервер. Также TCP осуществляет надежную передачу потока байт от одной программы на некотором компьютере в другую программу на другом компьютере. Программы для электронной почты и обмена файлами используют TCP. TCP контролирует длину сообщения, скорость обмена сообщениям, сетевой трафик.

IP-адрес

IP-адрес (Internet Protocol Address) – уникальный идентификатор устройства, подключённого к локальной сети или интернету. IP-адрес представляет собой 32-битовое (по версии IPv4) или 128-битовое (по версии IPv6) двоичное число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками, например, 192.168.0.1. (или 128.10.2.30 – традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса).

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень протокола IP передаёт пакеты между сетями. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: номера сети и номера узла. В случае изолированной сети её адрес может быть выбран администратором из специально зарезервированных для таких сетей блоков адресов (192.168.0.0/16, 172.16.0.0/12 или 10.0.0.0/8).

Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае

компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Маска подсети

В терминологии сетей TCP/IP маской подсети или маской сети называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.0.0 находится в сети 12.34.0.0.

Другой вариант определения – это определение подсети IP-адресов. Например, с помощью маски подсети можно сказать, что один диапазон IP-адресов будет в одной подсети, а другой район соответственно в другой подсети.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И). Например, в случае более сложной маски:

IP-адрес: 11000000 10101000 00000001 00000010 (192.168.1.2)

Маска подсети: 11111111 11111111 11111111 00000000 (255.255.255.0)

Адрес сети: 11000000 10101000 00000001 00000000 (192.168.1.0)

Разбиение одной большой сети на несколько маленьких подсетей позволяет упростить маршрутизацию. Например, пусть таблица маршрутизации некоторого маршрутизатора содержит следующую запись:

Сеть назначения	Маска	Адрес шлюза
192.168.1.0	255.255.255.0	192.168.15.1

Пусть теперь маршрутизатор получает пакет данных с адресом назначения 192.168.1.2. Обрабатывая построчно таблицу маршрутизации, он обнаруживает, что при наложении маски 255.255.255.0 на адрес 192.168.1.2 получается адрес сети 192.168.1.0. В таблице маршрутизации этой сети соответствует шлюз 192.168.15.1, которому и отправляется пакет.

Шлюз по умолчанию

Для того чтобы установить соединение с узлом из другой сети, необходимо сконфигурировать IP-адрес шлюза по умолчанию. TCP/IP посылает пакеты, предназначенные для удаленных сетей, на шлюз по умолчанию, но только в том случае, если на локальном узле не сконфигурирован другой маршрут к сети получателя. Если не сконфигурирован шлюз по умолчанию, то связь может быть ограничена локальной сетью.

Сетевые команды

ping

Утилита ping является, скорее, не инструментом DNS, а инструментом TCP/IP, позволяющим установить, подключен ли узел к сети. Она также предусматривает некоторые возможности ответа на сетевые запросы. ping

практически использует *протокол контроля сообщений в Internet* (Internet Control Message Protocol, ICMP) для отправки на удаленный узел запроса отклика и затем ожидает ответа. Если ответ приходит до истечения периода тайм-аута (который может быть задан пользователем), на экране отображаются время прохождения сообщения и сам ответ. Утилита ping по умолчанию посылает на удаленный узел серию из четырех запросов. ping выводит для пользователя отклик на запрос и краткую общую статистику, например, подобную показанной ниже. Учтите, если задать узел назначения его именем, ping возвратит соответствующий IP-адрес. Обратное действие можно выполнить с помощью опции -a.

Статистика Ping для 10.10.10.100:

Пакетов: отправлено = 4, получено = 4, потеряно =0 (0% потерь). Приблизительное время передачи и приема:

наименьшее = 10мс, наибольшее = 50мс, среднее = 30мс

С ping можно использовать множество опций командной строки, придерживаясь следующего синтаксиса.

ping [-taf] [-n число] [-l размер] [-1 ttl] [-v tos] [-r число][-s число] [[-j список_узлов]|[-k список_узлов]][-w тайм-аут]

В этом синтаксисе применены следующие обозначения.

-t заставляет ping работать непрерывно, пока пользователь не остановит его.

-a используется для разрешения имен узлов по адресам.

-f запрещает фрагментацию пакетов. (Если в -l установлено значение, требующее фрагментации, запрос не отправляется и выводится сообщение о состоянии флага запрета фрагментации DF.)

-n задает количество отправляемых запросов.

-l задает длину запроса отклика.

-I задает срок жизни (TTL). (Допускаются значения от 0 до 255.)

-v позволяет пользователю изменять поле типа службы (Type of Service, TOS).

-r записывает маршрут запросов и ответов. Можно записывать от одного до девяти узлов.

-s создает штампы времени для указанного числа переходов.

-j указывает узлы свободного исходного маршрута. Можно задать до девяти узлов исходного маршрута. (Свободные исходные маршруты предусматривают промежуточные маршрутизаторы между узлами.) Учтите, что опции -j и -k взаимоисключающие.

-k указывает узлы жесткого исходного маршрута. Можно задать до девяти узлов исходного маршрута. (Жесткие исходные маршруты не предусматривают промежуточных маршрутизаторов между узлами.) Учтите, что опции -j и -k взаимоисключающие.

-w позволяет задать интервал тайм-аута для откликов в миллисекундах.

Назначение может быть именем узла или IP-адресом.

pathping

Эта программа показывает использованный маршрут и более полную информацию о качестве линии. В сравнении с tracert эта программа быстрее выдает информацию о маршруте, но в сравнении с ping она требует больше времени для выполнения из-за подсчета статистики.

Синтаксис этой программы следующий.

C:\>pathping /?

Использование: pathping [-n] [-h Число_прыжков] [-g Список] [-p Пауза] [-q Число_запросов] [-w Тайм-аут] [-t] [-R] [-r] узел

Параметры:

-n Не разрешать имена узлов по адресам

-h Число прыжков Максимальное число прыжков при поиске конечного
узла

-g Список Свободный исходный маршрут по списку узлов

-p Пауза Пауза между отправками, мс

-q Число запросов Число запросов при каждом прыжке

-w тайм-аут Время ожидания каждого ответа, мс

-T Тестировать возможность взаимодействия для каждого прыжка с метками приоритета протокола уровня 2

-R Тестировать, если каждый прыжок резервируется с помощью RSVP

Проверим работу pathping в трассировке узла www.example.net.

C:\pathping www.example.net

Трассировка маршрута к VENERA.ISI.EDU [128.9.176.32] с максимальным числом прыжков 30:

0 ns.win2000dns.com [10.10.10.1]
1 prxy.win2000dns.com [10.10.10.253]
2 209.217.25.11
3 USC-abilene.ATM.calren2.net [198.32.248.85]
4 ISI-USC.POC.calren2.net [198.32.248.26]
5 128.9.16.17
6 128.9.32.7
7 venera.isi.edu [128.9.176.32]

tracert (traceroute)

Утилита traceroute или tracert (эта команда более известна как traceroute в UNIX) задает относительный путь, по которому должны проходить пакеты к своему месту назначения. Отправляется серия пакетов ICMP (вспомните, что в большинстве вариантов traceroute в UNIX фактически передаются пакеты UDP), но TTL устанавливается на 1 для первых трех пакетов и увеличивается на 1 для каждой последующей тройки пакетов. Поскольку маршрутизаторы уменьшают TTL на 1, первый пакет исчерпывает TTL только на первом маршрутизаторе. Затем маршрутизатор посылает отправителю ответ ICMP о том, что TTL истек. Следовательно, второй пакет с TTL 2 исчерпает его на втором

маршрутизаторе. Тогда отправителю будет послан второй ответ ICMP. Этот процесс увеличения TTL продолжается, пока не ответит узел назначения или пока не будет достигнуто максимальное значение TTL – 255.Синтаксис командной строки и параметры tracert следующие.

*tracert [-d] [-h макс*Число*] [-j списокУзлов][-w интервал] назначение*

Здесь

-d указывает, что не надо разрешать имена узлов по IP-адресам.

-h задает максимальное число прыжков при поиске узла (фактически максимальное значение TTL).

-j позволяет задать узлы свободного исходного маршрута (как и для ping, их может быть не более девяти).

-w задает интервал тайм-аута в миллисекундах.

Назначение может быть именем узла или IP-адресом.

В очередном примере с www.example.net можно увидеть, что tracert не имеет никаких преимуществ в информативности по сравнению с pathping, но в целом работает быстрее (если не считать замедления начала вывода) за счет уменьшенной точности измерения времени.

C:\>tracert www.example.net

Трассировка маршрута к VENERA.ISI.EDU [128.9.176.32]

с максимальным числом прыжков 30:

1 <10мс <10мс <10мс prxy.win2000dns.com [10.10.10.253]

1 <10мс <10мс <10мс 209.217.25.11

3 10мс 10мс 10мс USC-abilene.ATM.calren2.net[198.32.248.85]

4 10мс 10мс 20мс ISI-USC.POC.calren2.net [198.32.248.26]

5 10мс 10мс 20мс 128.9.16.17

6 10мс 10мс 20мс 128.9.32.7

7 10мс 10мс 20мс venera.isi.edu [128.9.176.32]

Трассировка завершена.

ipconfig

Утилита ipconfig – это диагностическая программа для работы в командной строке в Windows. Раньше, в Windows NT, можно было узнать настройку стека IP компьютера и заставить клиент DHCP освободить или обновить свою аренду IP. В Windows NT программа ipconfig имеет следующий синтаксис:

ipconfig

ipconfig /all

ipconfig /release [адаптер]

ipconfig /renew [адаптер]

Если использовать ipconfig без аргументов, она показывает базовую конфигурацию сети, как в этом примере.

C:\>ipconfig

Настройка протокола IP для Windows NT Адаптер Ethernet E190xl:

IP-адрес : 192.168.1.2
Маска подсети : 255.255.255.0
Основной шлюз : 192.168.1.1

Если включена служба DHCP, можно использовать ipconfig с переключателем /release, чтобы освободить аренду IP. Подобным образом, переключатель /renew перестраивает стек IP непосредственно с сервера DHCP в процессе аренды. Переключатели /release и /renew можно также использовать с именами адаптеров. Это важно для группового компьютера. В Windows 2000 базовые выводимые данные в основном такие же; в каждой версии можно предусмотреть выводимый листинг для каждого настраиваемого интерфейса. Но в Windows 2000 возможности этой программы расширены за счет управления кэшем распознавание клиента и классом клиента DHCP. Дополнительные параметры для Windows 2000 следующие.

ipconfig /flushdns

В соответствии со своим названием параметр /flushdns очищает кэш распознавателя DNS у клиента.

ipconfig /registerdns

Параметр /register заставляет клиент DNS перерегистрироваться путем динамического обновления DNS после обновления своей аренды DHCP, если это допустимо.

ipconfig /displaydns

Параметр /displaydns можно использовать для просмотра содержимого кэша распознавателя клиента DNS.

ipconfig /showclassid адаптер

Параметр /showclassid отображает все допустимые для данного адаптера коды классов. Указывать адаптер обязательно.

ipconfig /setclassid адаптер[устанавливаемый код класса]

Параметр /setclassid можно использовать для задания кодов классов; если никакой код не указан, код класса удаляется из адаптера. Указывать адаптер обязательно. Последние два параметра описаны в документации несколько неясно. На момент написания книги код уже был зафиксирован; однако документы RFC, определяющие параметр 81 DHCP, все еще пересматривались. Скорее всего, причина в этом.

Дополнительно в Windows 2000 можно задавать шаблоны имен адаптеров, используя звездочку (*) вместо любого количества символов и вопросительный знак (?) вместо одного символа.

Если задать переключатель /all, ipconfig покажет несколько больше, чем базовую информацию о настройке. Будут показаны доменное имя узла, серверы DNS и WINS, тип узла NetBIOS, код области NetBIOS (если есть) и другие параметры. Программа также покажет информацию о каждом сетевом адаптере, если их установлено несколько. Ниже приведен пример типичного использования ipconfig с параметром /all.

C:\>ipconfig
Настройка протокола IP для Windows 2000
Имя компьютера : machine.example.net

Основной DNS суффикс : .example.net
Тип узла .. ' : Гибридный
Код области NetBIOS :
Включена IP-маршрутизация .... : Нет
Доверенный WINS-сервер : Нет
Адаптер Ethernet Подключение к локальной сети
DNS суффикс этого подключения .. :
Описание ..... :
3Com Etherlink XL 10/100 PCI TX NIC (3C905B)
Физический адрес ..... : 00-AO-B9-68-B1-60
DHCP разрешен ..... : Нет
IP-адрес ..... : 192.168.1.2
Маска подсети ..... : 255.255.255.0
Основной шлюз ..... : 192.168.1.1
DNS-серверы ..... : 192.168.1.1
Основной WINS-сервер ..... : 192.168.1.1
Дополнительный WINS-сервер .....: 192.198.1.254

netstat

Программа netstat отображает статистику протокола и состояние текущих подключений TCP/IP. Обратите внимание на различие: netstat работает с подключениями TCP/IP, а nbstat – с подключениями NetBIOS.

Синтаксис утилиты netstat следующий:

C:\>netstat /?

Отображение статистики протокола и текущих сетевых подключений TCP/IP.

NETSTAT [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]

-a Отображение всех подключений и ожидающих портов. (Подключения со стороны сервера обычно не отображаются).

-e Отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s.

-n Отображение адресов и номеров портов в числовом формате.

-p имя Отображение подключений для протокола "имя":tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.

-r Отображение содержимого таблицы маршрутов.

-s Отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -p позволяет указать подмножество выводящихся данных, интервал. Повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

nbtstat

Программа nbtstat проверяет состояние подключений NetBIOS через TCP/IP (NetBT), а также выдает статистику сеанса NetBIOS и разрешения

имен. Кроме того, эту программу можно использовать для запуска обновления локального кэша имен NetBIOS. От версии NT она почти не отличается, но надо указать, что, начиная с Service Pack 4 добавлен очень полезный переключатель -rr, позволяющий не делать перезагрузку для перерегистрации в WINS. Синтаксис программы nbtstat следующий.

C:\>nbtstat /?

Отображение статистики протокола текущих подключений TCP/IP с помощью NBT (NetBIOS через TCP/IP).

NBTSTAT [-a Узел] [-A IP-адрес] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [интервал]]

-a (adapter status) Вывод таблицы имен узла, указанного по имени.

-A (Adapter status) Вывод таблицы имен узла, указанного по IP-адресу,

-c (cache) Вывод буфера имен удаленных узлов, включая адреса IP.

-n (names) Вывод локальных имен NetBIOS.

-r (resolved) Вывод имен, определенных с помощью рассылки и WINS.

-R (Reload) Очистка и перезагрузка таблицы удаленного буфера имен.

-S (Sessions) Вывод таблицы сеансов с IP-адресами,

-s (sessions) Вывод таблицы сеансов с преобразованием IP-адресов в имена NETBIOS.

-RR (ReleaseRefresh) Отсылка пакетов освобождения имени (Name Release) на WINS-сервер, а затем запуск обновления

route

Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации. Запущенная без параметров, команда route выводит справку.

ROUTE [-f] [-p] [команда [узел][MASK маска] [шлюз] [METRIC метрика] [IF-интерфейс]

-f Очистка таблиц маршрутов от записей для всех шлюзов. При указании одной из команд, таблицы очищаются до выполнения команды.

-p При использовании с командой ADD задает сохранение маршрута при перезагрузке системы. По умолчанию маршруты не сохраняются при перезагрузке. Игнорируется для остальных команд, изменяющих соответствующие постоянные маршруты.

[команда] Одна из четырех команд

PRINT Печать маршрута

ADD Добавление маршрута

DELETE Удаление маршрута

CHANGE Изменение существующего маршрута

[узел] Адресуемый узел.

[MASK] Если вводится ключевое слово MASK, то следующий параметр интерпретируется как параметр «маска».

маска Значение маски подсети, связываемое с записью для данного маршрута. Если этот параметр не задан, по умолчанию подразумевается 255.255.255.255.

шлюз Шлюз.

[METRIC] Определение параметра метрика/цена для адресуемого узла.

Поиск всех символических имен узлов проводится в файле сетевой базы данных NETWORKS. Поиск символических имен шлюзов проводится в файле базы данных имен узлов HOSTS.

Для команд PRINT и DELETE можно указать узел и шлюз с помощью подстановочных знаков или опустить параметр «шлюз».

*Если адресуемый узел содержит подстановочные знаки * или ?, он используется в качестве шаблона, и печатаются только соответствующие ему маршруты.*

Знак '' соответствует любой строке, а '?' - ровно одному знаку.*

Примеры: 157..1, 157.*, 127.*, *224*.*

Диагностические сообщения:

Недопустимое значение MASK вызывает ошибку, если (УЗЕЛ & МАСКА) != УЗЕЛ.

Например> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1

Добавление маршрута завершится ошибкой, поскольку указан недопустимый параметр сетевой маски: не выполняется условие

(УЗЕЛ & МАСКА) == УЗЕЛ.

Примеры:

> route PRINT

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2

*узел^ ^маска ^шлюз метрика^ ^ интерфейс^*

Если IF не задан, то производится попытка найти лучший интерфейс для указанного шлюза.

> route PRINT

> route PRINT 157 .... Печать только узлов, начинающихся со 157*

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

CHANGE используется для изменения только для изменения адреса основного шлюза и/или метрики.

> route PRINT

> route DELETE 157.0.0.0

> route PRINT

Службы Windows 2003

Службы DNS и DHCP являются ключевыми сетевыми службами в любой корпоративной сети, построенной на базе стека протоколов TCP/IP. Более того, в среде Windows Server 2003 наличие службы DNS является одним из обязательных условий развертывания службы каталога Active Directory. Служба DNS осуществляет разрешение символических доменных

имен в соответствующие им IP-адреса. Удобным дополнением к службе DNS в среде Windows Server 2003 является служба DHCP, упрощающая процесс конфигурации сетевых хостов (в том числе выделение хосту IP-адреса). Кроме того, в среде Windows многими администраторами традиционно используется служба WINS, осуществляющая разрешение символических NetBIOS-имен в соответствующие IP-адреса. Хотя роль этой службы в Windows Server 2003 была значительно уменьшена за счет реализации механизма динамической регистрации доменных имен, служба WINS может по-прежнему использоваться для организации процесса разрешения имен (например, в процессе перехода с Windows NT на Windows Server 2003).

Служба WINS

Основное назначение *службы имен Интернета Windows* (Windows Internet Name Service, WINS), заключается в организации процесса разрешения NetBIOS-имен в соответствующие IP-адреса. В предыдущих версиях Windows эта служба занимала центральное положение и на её основе строилось функционирование всей сети. Однако NetBIOS-имена используются исключительно системами семейства Windows. Второе существенное ограничение заключалось в возможности интеграции корпоративных сетей, использующих плоское пространство NetBIOS-имен, в глобальную сеть Internet, где реализуется иерархическое пространство имен DNS. В последних ОС Windows сделан упор на поддержку службы доменных имен DNS, однако для осуществления совместимости с предыдущими версиями Windows оставлена служба WINS.

При всех своих достоинствах, IP-адреса имеют существенный недостаток – они неинформативны. Для адресации желательно использовать дружественные пользователю имена. Для Windows традиционно использовалась система NetBIOS-имен.

Имя NetBIOS – это уникальный 16-байтный адрес, используемый для идентификации в сети ресурса NetBIOS. Имена бывают эксклюзивные (exclusive) или групповые – не эксклюзивные (non-exclusive). Первые, как правило, используют для взаимодействия с некоторым процессом на компьютере, вторые – для передачи информации нескольким компьютерам одновременно. Вы можете применить команду **nbtstat -n** для просмотра имен NetBIOS вашего компьютера. Например, имя NetBIOS используется службой сервера на компьютере, работающем под управлением Windows NT. При загрузке системы служба сервера регистрирует уникальное имя NetBIOS, основанное на имени компьютера. Точнее, имя, используемое сервером, – это 15-символьное имя компьютера плюс 16-й символ – шестнадцатеричное число 20. Остальные сетевые службы также используют имя компьютера для построения своих имен NetBIOS, поэтому 16-й символ применяется для однозначного определения таких служб, как редиректор (Redirector), сервер (Server) или почтовая служба (Messenger services). Все сетевые службы Windows NT регистрируют свои имена NetBIOS. Все сетевые команды Windows NT (Windows NT Explorer, File Manager и команды net) используют имена NetBIOS для доступа к этим службам. Имена NetBIOS также

применяются в других системах, основанных на NetBIOS, например, Windows for Workgroups, LAN Manager и LAN Manager для UNIX.

Интерфейс NetBIOS определяет интерфейс сеансового уровня и протокол передачи данных и управления сеансом. Интерфейс NetBIOS – доступный пользовательским приложениям стандартный прикладной интерфейс (API) для выполнения сетевого ввода/вывода и отправки команд управления к ПО нижележащего протокола. Прикладная программа, использующая интерфейс NetBIOS для сетевого взаимодействия, может работать с любым протоколом, поддерживающим интерфейс NetBIOS.

Стандартом NetBIOS определяется также протокол, действующий на сеансовом/транспортном уровне. Он реализуется в ПО нижележащего протокола, например, NBFP (NetBEUI) или NetBT, где представлен весь набор команд сетевого ввода/вывода интерфейса NetBIOS. NetBIOS поверх TCP/IP, или просто NetBT, это сетевая служба сеансового уровня.

Имя NetBIOS назначается Вашему компьютеру. NetBIOS поддерживает следующие команды и функции:

1 Регистрацию и проверку сетевых имен.

2 Запуск и завершение сеанса.

3 Надежную передачу данных сеанса, ориентированного на соединение.

4 Ненадежную передачу датаграмм (datagram) без установки соединения.

5 Возможность мониторинга и управления протоколом (драйвером) и адаптером.

Пространство имен NetBIOS представляет собой плоское пространство имен и не позволяет отобразить сложные иерархические отношения. Пространство имен NetBIOS состоит из равноправных элементов, которые представляют собой NetBIOS-имена. Эти имена присваиваются всем участникам сетевого взаимодействия: пользователям, группам пользователей, компьютерам и даже доменам. При этом существуют два различных типа NetBIOS-имени:

1 Уникальное Net-BIOS-имя. Этот тип имени используется для идентификации в сети конкретного пользователя или компьютера. Это имя обязательно должно быть уникальным. С каждым именем должен быть связан только один IP-адрес.

2 Групповое NetBIOS-имя. Групповое имя идентифицирует некоторую группу пользователей или компьютеров (например, домен). С именем этого типа может быть связанно несколько IP-адресов.

Поскольку сами по себе NetBIOS-имена не дают возможности адресации, а TCP/IP работает только с IP-адресами, необходим механизм для разрешения имен в адреса. Существует два стандарта RFC1001 и RFC1002, согласно которым используются два метода разрешения NetBIOS-имен:

1 Рассылка широковещательных запросов. У данного способа есть два основных недостатка – возможность создания значительного трафика в сети и широковещательные запросы не ретранслируются маршрутизаторами в

другие подсети, т.е. данный метод эффективен только в пределах одной подсети.

2 Использование службы разрешения NetBIOS-имен. В данном случае клиент устанавливает прямое соединение с сервером, на котором стоит служба разрешения NetBIOS-имен, и отправляет запрос на разрешение имени. Сервер предоставляет клиенту IP-адрес, соответствующий имени, указанному в запросе.

Функционирование клиента возможно в одном из четырёх режимов:

1 Режим b-узла (B-node). Для разрешения имен клиент использует исключительно широковещательные запросы.

2 Режим p-узла (P-node). В этом режиме, чтобы разрешить имя в IP-адрес, клиент обращается к серверу имен.

3 Режим m-узла (M-node). При необходимости разрешить NetBIOS-имя в IP-адрес, клиент сначала использует широковещательный запрос. Если это не привело к требуемому результату, то клиент отправляет запрос серверу имен.

4 Режим h-узла (H-node). В данном режиме клиент первоначально пытается разрешить имя, отправив запрос серверу имен. Если сервер имен не способен разрешить имя, то клиент осуществляет рассылку широковещательных сообщений.

Microsoft предложила использовать в процессе разрешения имен файл LMHOSTS. Это текстовый файл, в котором последовательно перечисляются имена NetBIOS и соответствующие им IP-адреса.

Если имя по-прежнему не разрешено, система использует службу DNS для разрешения имени. Предполагается, что имя хоста, входящее в состав доменного имени, аналогично NetBIOS-имени. Поэтому к запрашиваемому имени добавляется DNS-суффикс и предпринимается попытка разрешить доменное имя.

Общая схема разрешения имени представлена на рисунке 1.

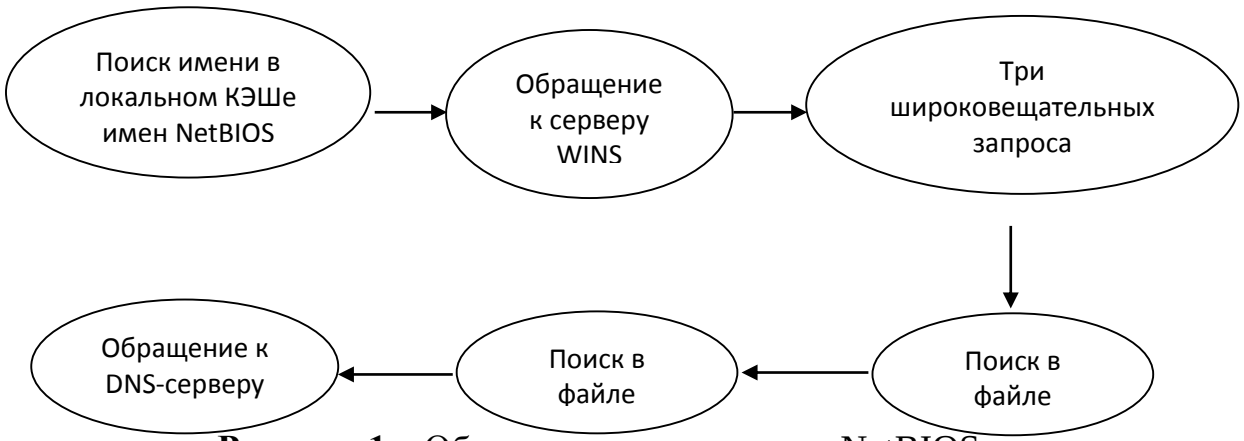

Рисунок 1 – Общая схема разрешения NetBIOS-имени

Пример функционирования службы DNS представлен на рисунке 2.

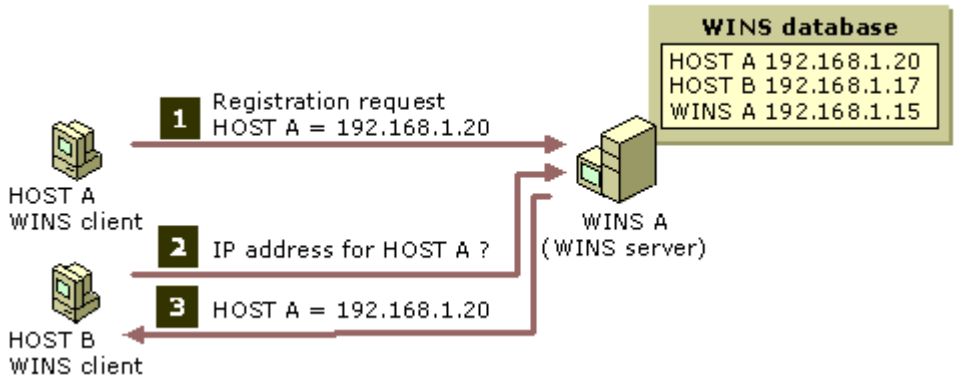

Рисунок 2 – Пример функционирования службы DNS

Регистрация имени – это запрос WINS-клиентом использования NetBIOS-имени в сети. Запрос может быть на уникальное (единственное) или групповое (общее) имя. Приложения NetBIOS также могут регистрировать одно или несколько имен.

Как показано на приведенном ниже рисунке 3, WINS-клиент (HOST-C) передает запрос регистрации имени непосредственно своему WINS-серверу, WINS-A.

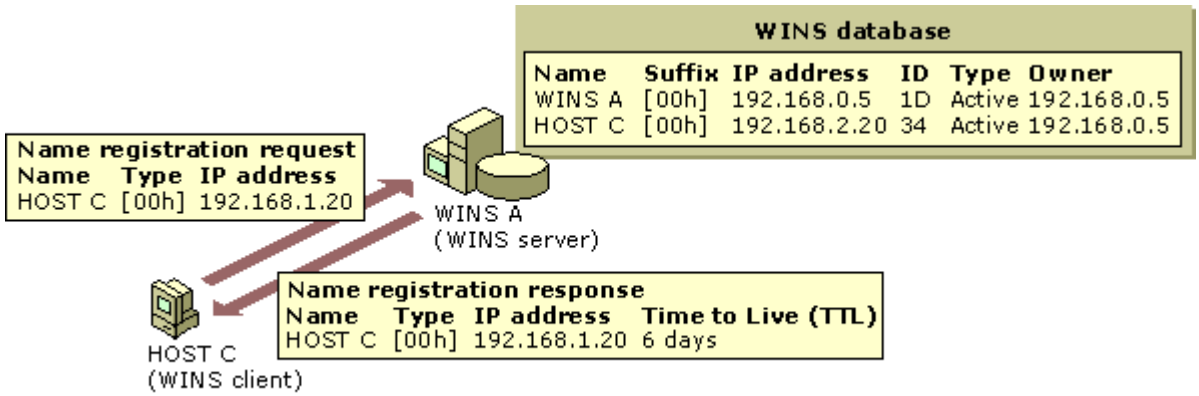

Рисунок 3 – Пример запроса на разрешение имени NetBIOS

Сервер WINS-A может принять или отклонить запрос регистрации имени и дать положительный или отрицательный ответ клиенту HOST-C. Предпринимаемые сервером WINS-A действия зависят от ряда факторов:

1 Существует или нет это имя в базе данных сервера WINS-A.

2 Если запись имени существует – каково состояние этой записи в базе данных на сервере WINS-A, а также совпадает ли записанный IP-адрес с IP-адресом запрашивающего клиента (HOST-C).

3 Запрашивается уникальное или групповое имя.

Если имя отсутствует в базе данных, оно признается новой регистрацией и выполняются перечисленные ниже действия:

1 Имя HOST-C вводится с новым номером версии, с указанным штампом времени и помечается идентификатором владельца, присвоенным WINS-серверу. Штамп времени вычисляется сложением значения параметра Интервал обновления (равного по умолчанию 6 дням), установленного на WINS-сервере, с текущей датой и временем на сервере.

2 Положительный ответ на регистрацию направляется HOST-C со сроком жизни (TTL), равным штампу времени, записанному для имени на сервере WINS-A.

Если имя HOST-C уже введено в базу данных с тем же IP-адресом, что и в запросе, предпринимаемые действия зависят от состояния и владельца существующего имени:

1 Если запись помечена как активная и принадлежит серверу (WINS-A), сервер обновляет штамп времени для записи и возвращает положительный ответ клиенту.

2 Если запись помечена как освобожденная или захороненная, или принадлежит другому WINS-серверу, регистрация рассматривается как новая. Штамп времени, номер версии и владелец обновляются, и возвращается положительный ответ.

Если имя существует в базе данных, но IP-адрес не совпадает с указанным в запросе, ожидается, что WINS-сервер избежит дублирования имен. Если запись данных освобождена или захоронена, WINS-сервер может назначать это имя.

Если же запись находится в активном состоянии, вызывается узел, содержащий имя, для выяснения его наличия в сети. В этом случае WINS-сервер (WINS-A) может вызвать имя и выполнить следующие действия:

1 WINS-A отправляет ответ ожидания подтверждения (WACK) запрашивающему клиенту (HOST-C), указывая в поле TTL время, в течение которого клиент может получить ответ.

2 Затем WINS-A формирует запрос к узлу, зарегистрированному в настоящее время для данного имени в базе данных сервера.

3 Если узел существует, серверу WINS-A отправляется положительный ответ.

4 WINS-A, в свою очередь, отправляет отрицательный ответ на запрос регистрации имени запрашивающему клиенту (HOST-C), отвергая регистрацию имени.

5 Если на первый запрос вызова, сделанный WINS-A, не получен положительный ответ, делаются еще два запроса имени. Если на все три попытки не получен ответ, процесс вызова завершается и запрашивающему клиенту (HOST-C) возвращается положительный ответ на регистрацию. В базе данных сервера обновляется имя для новой регистрации клиента.

В отличие от клиентов, поддерживающих WINS, которые могут непосредственно обращаться к WINS-серверу, клиенты, не использующие службу WINS (например, клиенты b-узлов NetBT), должны регистрировать и непрерывно защищать свои имена, направляя широковещательные запросы имени в локальной сети и отвечая на широковещательные рассылки.

NetBIOS-имена регистрируются службой WINS (Windows Internet Name Service) и обычно освобождаются при правильном завершении работы компьютера. Если работа компьютера не была завершена должным образом или компьютер не смог обратиться к WINS-серверу во время прекращения работы, команда **nbtstat** может быть использована для обновления локальных имен компьютера в службе WINS. Это полезно при работе с

портативными компьютерами, которые могут переноситься в различные участки сети.

Служба DNS

Согласно концепции TCP/IP, каждый хост в сети должен иметь как минимум один IP-адрес. Этот адрес используется для однозначной идентификации этого хоста в сети. Однако, существует недостаток данного метода, заключающийся в субъективности человеческого восприятия. В сети с большим количеством хостов, невозможно запомнить все нужные IP-адреса. Для решения этой проблемы была предложена схема именования, получившая название **системы доменных имен** (DNS – Domain Name System). Имена, используемые DNS для именования хостов, получили название **полных имен домена** (FQDN – Full Qualified Domain Name).

В основе системы доменных имен лежит иерархическое пространство имен.

При этом всё пространство имен DNS представлено в виде отдельных фрагментов, называемых **доменами** (domains). Домены, связываясь между собой при помощи отношений родитель – потомок, образуют определенную иерархию. В зависимости от того, какое положение занимает домен в этой иерархии, принято говорить об уровне домена.

Домен, лежащий в основании иерархического пространства имен DNS, получил название **корневого домена** (root domain). Корневой домен выполняет функцию родоначальника всех доменов первого уровня. Фактически он является чисто формальным элементом, символизирующим иерархичность пространства доменных имен. Для записи доменного имени корневой домен обозначается как пустое место точки, которой заканчивается любое доменное имя.

Домены первого уровня используются для группировки других доменов по организационному признаку либо географическому положению. В случае группировки по организационному уровню имена доменов первого уровня образуются тремя символами(.edu – образовательные учреждения, .com – коммерческие организации, .org – некоммерческие организации). Для определения принадлежности к стране используют имена из двух символов(.ru,.by).

Кроме этого существует еще один домен первого уровня, который используется для группировки **обратных адресов** (reverse domains). Обратные домены применяются для осуществления поиска доменного имени хоста по его IP-адресу. Этот специальный домен получил название **.arpa**, и он является единственным доменом первого уровня, имеющим имя из четырех символов. Домен содержит только один домен второго уровня: **.in-addr.arpa**.

Домены первого уровня используются исключительно для группировки доменов следующих уровней по некоторому признаку. Пример иерархии DNS в виде дерева предоставлен на рисунке 4.

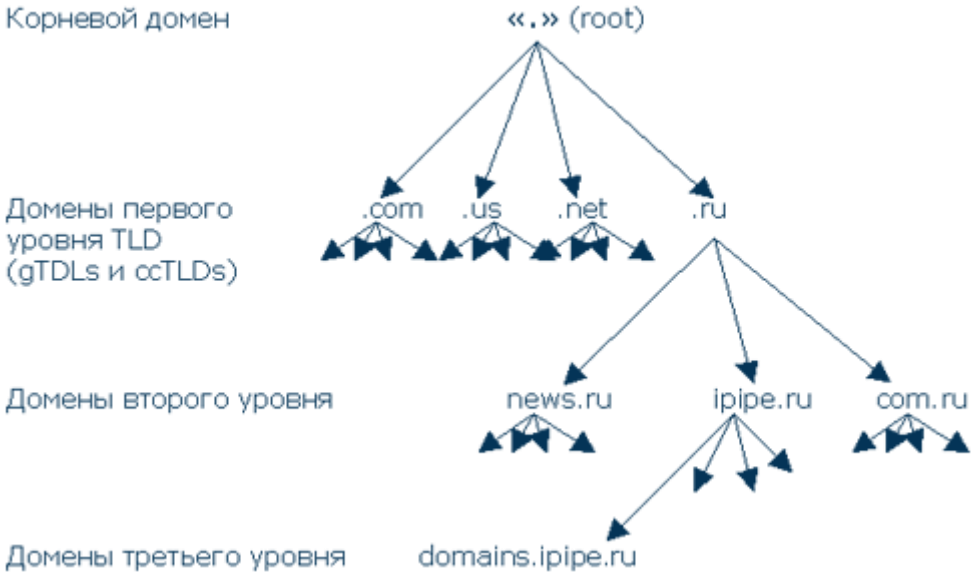

Рисунок 4 – Иерархия DNS в древовидном виде

Каждый из узлов соответствует либо домену, либо хосту. Под хостом в этом дереве понимают лист, т.е. такой узел ниже которого нет других узлов. Именовать хост можно либо частичным именем, либо полным именем. Полное имя хоста – это имя, в котором перечисляются слева направо имена всех промежуточных узлов между листом и корнем дерева доменного именования, при этом начинают с имени листа, а кончают корнем, например:

polyn.net.kiae.su.

Частичное имя – это имя, в котором перечислены не все, а только часть имен узлов, например:

polyn

apollo.polyn

quest.polyn.kiae

Обратите внимание на то, что в частичных (неполных именах) символ точки в конце имени не ставится. В реальной жизни программное обеспечение системы доменных имен расширяет неполные имена до полных прежде, чем обратиться к серверам доменных мен за IP-адресом.

Слово «Хост» не является в полном смысле синонимом имени компьютера, как это часто упрощенно представляется. Во-первых, у компьютера может быть множество IP-адресов, каждому из которых можно поставить в соответствие одно или несколько доменных имен. Во-вторых, одному доменному имени можно поставить в соответствие несколько разных IP-адресов, которые, в свою очередь могут быть закреплены за разными компьютерами.

Еще раз обратим внимание на то, что именование идет слева направо, от минимального имени хоста (от листа) к имени корневого домена. Разберем, например, полное доменное имя demin.polyn.kiae.su. Имя хоста – demin, имя домена, в который данный хост входит, – polyn, имя домена, который охватывает домен polyn, т.е. является более широким по отношению к polyn, – kiae, в свою очередь последний (kiae) входит в состав домена su.

Имя polyn.kiae.su – это уже имя домена. Под ним понимают имя множества хостов, у которых в их имени присутствует polyn.kiae.su. Вообще говоря, за именем polyn.kiae.su может быть закреплен и конкретный IP-адрес. В этом случае кроме имени домена данное имя будет обозначать и имя хоста. Такой прием довольно часто используется для обеспечения коротких и выразительных адресов системе электронной почты.

Следует также упомянуть о канонических доменных именах. Это понятие встречается в контексте описания конфигураций поддоменов и зон ответственности отдельных серверов доменных имен. С точки зрения дерева доменные имена не разделяют на канонические и неканонические, но с точки зрения администраторов, серверов и систем электронной почты такое разделение является существенным. Каноническое имя – это имя, которому в соответствие явно поставлен IP-адрес, и которое само явно поставлено в соответствие IP-адресу. Неканоническое имя – это синоним канонического имени.

Как работает DNS?

DNS работает в режиме вопрос/ответ. Допустим, вы ввели в строке своего браузера ipipe.ru. Рассмотрим работу DNS пошагово:

Шаг 1. Ваш браузер об IP адресе ipipe.ru ничего не знает и с запросом IP адреса ipipe.ru, через специальную программу resolver обращается к локальному серверу имен.

Локальный DNS сервер – это сервер имен вашей локальной сети или DNS сервер вашего Интернет провайдера. При настройках сетевого подключения вы прописываете IP адреса DNS серверов (или же этот параметр получен через DHCP) один из которых будет отвечать на запросы, посылаемые вашим браузером через resolver – это и есть локальный или местный сервер вашей сети. Если вы используете модемное подключение (через телефонную линию), то для Вас местным сервером имен будет DNS сервер вашего провайдера. IP адрес этого сервера также будет прописан в настройках сетевого подключения, не зависимо от того как осуществлялась настройка (вручную или автоматически). Вы всегда сможете посмотреть IP-адрес вашего локального DNS сервера.

Шаг 2. Запрос на IP адрес ipipe.ru доходит до местного сервера имен. Этот сервер об этом IP адресе ничего не знает, и посылает запрос одному из корневых серверов «.» (root).

Шаг 3. Корневой сервер отдает локальному серверу IP адрес сервера, который поддерживает зону .ru.

Шаг 4. Далее по полученному адресу локальный сервер имен обращается к DNS серверу, который поддерживает .ru.

Шаг 5. Этот DNS сервер по полученному запросу отдает IP адрес сервера, который поддерживает зону ipipe.ru.

Шаг 6. Местный DNS сервер с запросом IP адреса ipipe.ru обращается к DNS серверу зоны ipipe.ru.

Шаг 7. Локальный сервер имен получает IP адрес ipipe.ru. от DNS сервера зоны ipipe.ru.

Шаг 8. Получив адрес ipipe.ru локальный DNS сервер сообщает его Вашему браузеру.

Теперь браузер знает IP адрес ipipe.ru и напрямую обращается к серверу, на котором расположен сайт ipipe.ru.

Простейший алгоритм работы представлен на рисунке 5.

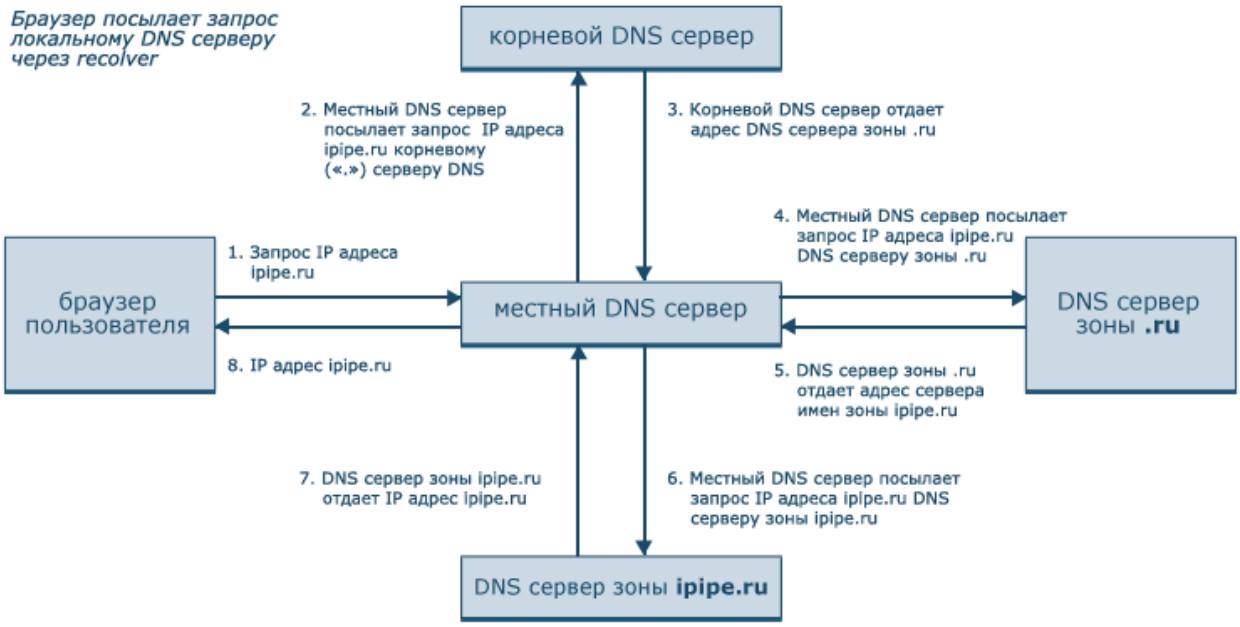

Рисунок 5 – Алгоритм работы получения IP-адреса по имени

Пространство доменных имен (информация о соответствии имен узлов IP-адресам) организовано иерархически в так называемые зоны. Понятие зоны должно быть уже знакомо вам по работе в Интернете. Иногда вместо слова «зона» говорят «домен», но это не совсем точно: зона может включать пространство нескольких доменов.

Локальная сеть образует одну зону. Нужно выбрать для нее название. Если в ваши намерения не входит «публикация» имен узлов вашей сети в Интернете, то название зоны можете выбирать произвольно.

Служба DHCP

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – протокол динамического конфигурирования хостов был выделен из стандартного протокола Интернета начальной загрузки (BOOTP Bootstrap Protocol) определенного в RFC 951 и 1084, который позволял динамически назначать IP-адреса (а также удаленную загрузку бездисковых рабочих станций). В дополнение к поддержке динамического назначения IP-адресов, DHCP снабжает клиентов всеми необходимыми конфигурационными данными TCP/IP, а также данными, необходимыми конкретным серверам.

Для обеспечения рационального использования адресов, сервер DHCP выдает адреса в аренду – на время, определяемое администратором и ограничивающее срок действия адреса. По истечении половины периода

аренды, клиент DHCP отправляет запрос на обновление аренды, и сервер DHCP продлевает текущую аренду. Это означает, что по завершении использования IP-адреса, выданного машине (например, при переносе ее в другой сетевой сегмент), срок аренды закончится, и адрес возвратится в пул для повторного выделения.

Протокол DHCP, реализованный Microsoft, состоит из трех основных компонентов:

- серверов DHCP;
- клиентов DHCP;
- агентов ретрансляции DHCP/BOOTP.

Конфигурационные параметры TCP/IP, которые могут назначаться сервером DHCP, включают:

- IP-адреса для каждого сетевого адаптера на клиентском компьютере;
- маски подсетей, используемые для идентификации участка IP-сети, в которую входят хосты;
- шлюзы по умолчанию (маршрутизаторы), которые используются при подключении одного сегмента сети к другим сегментам;
- дополнительные параметры, которые могут опционально назначаться клиентам DHCP (такие как IP-адреса DNS-серверов или WINS-серверов, используемые клиентами).

Протоколы BOOTP и DHCP основываются на широковещании при выполнении своей работы. Маршрутизаторы в обычных условиях работы не могут участвовать в передаче широковещательных пакетов между интерфейсами, поэтому для выполнения этой передачи должен быть использован агент ретрансляции. В качестве агента ретрансляции DHCP может выступать маршрутизатор или компьютер, сконфигурированный на прослушивание широковещательных сообщений DHCP/BOOTP и пересылку их на конкретный сервер DHCP (или на несколько серверов). Использование агентов ретрансляции исключает необходимость иметь в каждом физическом сегменте сети локальный сервер DHCP. Агенты ретрансляции могут не только направлять запросы локальных клиентов DHCP на удаленные серверы DHCP, но также и возвращать ответы сервера DHCP для клиентов DHCP.

Параметры DHCP

Область DHCP – это административное группирование, которое определяет последовательный диапазон допустимых IP-адресов, предназначенных для клиентов DHCP, принадлежащих конкретной физической подсети. Область определяет логическую подсеть, для которой предназначена служба DHCP, а также позволяет серверу использовать конфигурационные параметры, предназначенные клиентам DHCP. Область должна быть определена до того, как клиентам будет позволено использовать сервер DHCP для динамического конфигурирования TCP/IP.

Пул адресов (Address Pools)

Адреса, оставшиеся после определения области DHCP и исключаемых диапазонов, образуют доступный пул адресов данной области. Адреса из пула динамически назначаются клиентам DHCP в сети.

Исключаемые диапазоны (Exclusion Ranges)

Исключаемый диапазон – это ограниченная последовательность IP-адресов в области, которая исключается из числа адресов, предлагаемых службой DHCP. Использование исключаемых диапазонов гарантирует, что адреса из исключаемых диапазонов не будут предложены сервером DHCP клиентам в сети.

Резервирование (Reservations)

Резервирование используется при выдаче DHCP-сервером адресов в аренду на неограниченный срок. Резервирование позволяет предоставить постоянный IP-адрес определенным устройствам в сети.

Суперобласть (Superscopes)

Суперобласть – это административная группа областей, которая используется для поддержки нескольких логических IP-подсетей в одной физической подсети. Суперобласть содержит только список отдельных областей, которые могут быть активированы вместе. Для настройки большинства свойств областей, входящих в суперобласть, необходимо индивидуально настроить свойства отдельных областей. Суперобласти полезны при решении некоторых задач, касающихся службы DHCP.

Аренда (Leases)

Как уже говорилось, аренда – это интервал времени, задаваемый сервером DHCP, в течение которого клиент может использовать назначенный IP-адрес. После назначения клиенту IP-адреса аренда является активной. По истечении половины срока аренды клиент пытается обновить аренду на сервере. Срок аренды определяет длительность действия аренды и частоту, с которой ее назначение должно обновляться клиентом через сервер.

Типы параметров DHCP (DHCP Options)

Типы параметров DHCP – это различные параметры настройки клиентов, которые DHCP-сервер может назначать при выполнении запросов аренды DHCP-клиентам, к таким параметрам относятся IP-адреса основных шлюзов (маршрутизаторов), серверов WINS и серверов DNS. Обычно эти типы параметров устанавливаются для каждой области. Консоль DHCP позволяет также настроить типы параметров по умолчанию, которые используются всеми областями на сервере.

Установка служб Windows 2003

Для добавления службы Windows 2003 требуется запустить окно «Управление данным сервером» (Пуск → Панель управления → Администрирование → Управление данным сервером). Выбрать вкладку «Добавить, удалить роли». Затем выбрать особую настройку сервера и в списке ролей выбрать требуемую роль.

Настройка сети

Для настройки сетевого интерфейса необходимо зайти в Пуск → Настройка → Сетевые подключения и выбрать свойства необходимого интерфейса.

Для настройки протокола TCP/IP в списке Компонент необходимо выбрать Свойства «Протокол Интернета TCP/IP». В открывшемся окне по необходимости можно установить ip адрес, маску подсети, основной шлюз, основной DNS-сервер или альтернативный сервер.

Кнопка «Дополнительно» открывает окошко с дополнительными настройками, где можно задать списки WINS-серверов, DNS-сервером, ip-адреса для данного подключения.

В закладке DNS можно принудительно задать DNS-суффикс, установить требование регистрации данного адреса в DNS и определить какие DNS-суффиксы и в каком порядке будут использоваться при подключении.

В закладке WINS возможно управление протоколом NETBIOS.

Для задания имени компьютера необходимо Пуск → Настройка → Панель управления → Система (либо свойства «Мой компьютер») → «Имя компьютера» и нажать кнопку «Изменить». В появившемся окне можно задать имя компьютера, рабочую группу либо домен. По нажатии кнопки «Дополнительно» открывается окно в котором можно задать основной DNS-суффикс компьютера и определить будет ли он меняться при смене членства в домене.

Практическая часть

Содержание задания

В рамках задания требуется настроить на сервере с ОС Windows службы DHCP, DNS, WINS. Проверить правильность функционирования с помощью сетевых команд, приведенных в теоретической части. По результатам работы составить отчет.

Рекомендуемое ПО: VMware Workstation или VirtualBox.

Порядок выполнения работы

1 Ознакомиться с теоретической частью.

2 Установить необходимое ПО.

3 Установить Windows Server на виртуальную машину.

4 Установить ОС Windows в качестве клиентской машины.

5 Настроить на сервере службу DHCP (*IP-адрес сервера должен быть записан следующим образом 192.168.1.Номер студента в списке группы*).

6 Настроить на сервере службу DNS с прямой и обратной зоной (*в состав доменного имени должна входить фамилия студента, выполняющего задание. Формат суффикса: Фамилия.local*).

7 Настроить на сервере службу WINS.

8 С помощью сетевых команд проверить функционирование настроенных служб.

9 Составить отчёт о проделанной работе.

10 Показать отчёт и выполненную работу преподавателю.

Содержание отчёта

1 Титульный лист.

2 Цель работы.

3 Краткие теоретические сведения.

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

5 Описание проверок функционирования служб со скриншотами результатов.

6 Выводы о проделанной работе (*нельзя списывать из цели*).

Защита работ проводится индивидуально.

Контрольные вопросы

1 Перечислите недостатки протокола IP.

2 Назовите основные отличия протокола UDP от TCP.

3 Из каких частей состоит IP-адрес?

4 Какого назначение команды ipconfig? Назовите параметры данной команды.

5 Определите адрес сети по IP-адресу (192.168.1.2) и маске подсети (255.255.255.0).

6 Перечислите основные службы Windows 2003 и их назначение.

7 Какие функции выполняет NetBIOS?

8 Дайте определение понятию домен.
9 Дайте определение понятию каноническое имя.