2 Службы поддержки инфраструктуры сети

2.1 Система символьных имен NetBIOS

2.1.1 Использование символьных имен NetBIOS

Система NetBIOS (Network Basic Input/Output System) является совместной разработкой IBM и Microsoft и представляет собой интерфейс прикладного программирования (API). Уровень NetBIOS располагается между прикладным и транспортным уровнями стека протоколов TCP/IP. Главная функция NetBIOS – это обеспечение независимости между прикладным и транспортными уровнями. Наряду с NetBIOS в продуктах Microsoft поддерживается интерфейс Windows Sockets. NetBIOS и WinSock - это два разных пути реализации коммуникаций между узлами сети.

Для идентификации узла в сети в системе NetBIOS используется символьное имя. Имена NetBIOS должны быть уникальны в пределах сети и имеют длину до 15 символов. Символьное имя NetBIOS требуется ввести в процессе установки ОС Microsoft. Позднее это имя может быть легко изменено администратором компьютера. В ОС Windows 9x/NT4.0 наряду с NetBIOS именем компьютера имелась возможность указать DNS имя хоста (это делалось в настройках TCP/IP и в принципе они могли и не совпадать друг с другом). В последующих ОС DNS-имя хоста и NetBIOS имя компьютера были объединены.

2.1.1.1 Способы разрешения имен NetBIOS

Для взаимодействия между хостами имена NetBIOS должны быть преобразованы в IP-адреса. Для разрешения имен NetBIOS используются следующие механизмы:

1. Кеш имен – клиенты Microsoft поддерживают кэш имен NetBIOS с именами компьютеров и IP-адресами, которые ранее были разрешены данным клиентом. (Для просмотра кэша имен можно использовать утилиту nbtstat –c).
2. Просмотр локального файла LMHOSTS (расположен в папке %SystemRoot%\system32\drivers\etc) – может быть опубликован централизованно или на уровне отдельной системы. Файл содержит список имен NetBIOS и соответствующих им IP-адресов
3. Просмотр локального файла HOSTS (расположен в папке %SystemRoot%\system32\drivers\etc) – Файл содержит список хостов в формате полностью определенных доменных имен (FQDN) и соответствующих им IP-адресов
4. Широковещательная рассылка – клиент может разослать запрос в локальном сегменте сети, чтобы узнать принадлежит ли разрешаемое имя этому сегменту.
5. Запрос к WINS-серверу – сервер WINS (Windows Internet Naming Service) поддерживает базу данных с информацией о связях NetBIOS имен с IP-адресами.

2.1.1.2 Типы узлов NetBIOS

Порядок обращения к различным способам разрешения имен определяется режимом работы, или типом узла NetBIOS.

1. B-узел (Broadcast Широковещательный) – Широковещательные запросы используются для регистрации имени и для разрешения имен. При работе в данном режиме система посылает широковещательный запрос в локальный сегмент сети. Если этот запрос не позволяет разрешить имя, то просматривается содержимое самого файла LMHOSTS.
2. P-узел (Peer-Peer Равноправный) – широковещательные запросы не

используются. При своем запуске хост регистрирует свое имя на указанном WINS-сервере. Для разрешения имени используется обращение к WINS-серверу. Для нормальной работы необходимо, чтобы WINS-сервер был работоспособен и доступен. В случае отказа этого сервера разрешение имен выполняться не может.

3. M-узел (Mixed Смешанный) – сначала узел работает в B-режиме. Если имя не удалось разрешить, то используется P-режим.
4. H-узел (Hybrid Гибридный) – сначала используется P-режим, а в случае неудачи – B-режим. При таком подходе широковещательные пакеты используются только тогда, когда не дает результата обращение к WINS-серверу.

В системах Windows 2000 и более ранних версиях по умолчанию задается режим B-узла. В системах Windows XP и Windows Server 2003 устанавливается режим H-узла.

2.1.1.3 Типы имен NetBIOS

Существует несколько типов имен NetBIOS, образуемых присоединением к имени компьютера шестнадцатеричного идентификатора. Каждое уникальное имя описывает уровень сервиса, поддерживаемого компьютером. Например, имя рабочей станции – этот уровень сервиса позволяет компьютерам взаимодействовать по сети.

pc12[00h] – имя рабочей станции
pc12[20h] – сервис файл-сервера
serv[1Ch] – сервис контроллера домена
serv[1Bh] – сервис domain master browser
domain[1Eh] – имя домена

Таким образом, каждый компьютер регистрирует в сети несколько имен NetBIOS. Существует два способа регистрации имен: если система является клиентом WINS, она регистрирует все свои имена NetBIOS на сервере WINS; системы не являющиеся клиентами WINS рассылают имена в локальном сегменте сети: если другая система не отвечает на разосланные запросы, информируя о том, что запрашиваемые имена уже заняты, имена считаются зарегистрированными. Если имена NetBIOS уже используются другим компьютером, то система, пытающаяся их зарегистрировать, автоматически отключается от сети.

2.1.2 Служба Internet имен WINS

2.1.2.1 Спецификация WINS

Служба WINS (Windows Internet Naming Service) обеспечивает поддержку распределенной базы данных для динамической регистрации и разрешения NetBIOS-имен. Служба WINS отображает пространство имен NetBIOS и адресное пространство IP-адресов друг на друга и предназначена для разрешения NetBIOS-имен в маршрутизируемых сетях, использующих NetBIOS поверх TCP/IP.

Процесс разрешения строится на основе базы данных WINS-сервера. Входя в сеть, клиент регистрирует свое имя в базе данных WINS-сервера. При завершении работы клиент отправляет сообщение WINS-серверу, извещая его об освобождении им зарегистрированного имени.

Преимущества WINS:

1. WINS сокращает объем широковещательного трафика при разрешении имен.

2. Клиенты WINS могут связываться с серверами WINS в удаленных сегментах, тогда как широковещательные запросы блокируются маршрутизаторами.

3. WINS работает в динамическом режиме. Клиенты автоматически регистрируются и администратору не надо вести списки NetBIOS-имя-IP-адрес вручную.

4. WINS упрощает ведение списков просмотра (browse lists). Системы Microsoft

поддерживают большие списки ресурсов, доступных через сеть – «списки просмотра». Сервер WINS облегчает задачу документирования доступных ресурсов за счет получения информации об именах NetBIOS на каждом компьютере. Если сеть полагается только на широковещательный трафик, то для многосегментной сети такие списки являются неполными.

В спецификации службы WINS описываются три участника: WINS-сервер, WINS-клиент и посредник WINS (WINS proxy). WINS сервер обрабатывает запросы на регистрацию имен от WINS-клиентов, регистрирует их имена и соответствующие им IP-адреса, а также отвечает на запросы разрешения имен от клиентов. В сети может быть установлено несколько WINS-серверов. Базы данных всех существующих WINS-серверов синхронизируются в результате процесса репликации.

Под посредником WINS понимается специальный WINS-клиент, который может обращаться к WINS-серверу от имени других хостов, не способных обратиться к WINS-серверу самостоятельно. WINS-посредники используются для поддержки хостов, осуществляющих разрешение NetBIOS-имен методом широковещательных рассылок (хостов функционирующих в режиме b-узла). Поскольку широковещательные сообщения не ретранслируются маршрутизаторами, для нормальной работы сети возникает необходимость устанавливать WINS-серверы в каждой подсети или отказаться от таких клиентов. В качестве альтернативы администратор может сконфигурировать один из WINS-клиентов в качестве WINS-посредника. Хост, функционирующий в режиме b-узла, не подозревает о существовании WINS-посредника. Этот хост рассылает широковещательные запросы, которые принимаются всеми узлами подсети, в том числе и WINS-посредником. WINS-посредник переадресует эти сообщения WINS-серверу, информируя его о регистрации или освобождении соответствующего имени. При поступлении широковещательного запроса о разрешении NetBIOS-имени WINS-посредник проверяет собственный локальный Кеш имен, и если в нем не обнаружено запрашиваемое имя, переадресует запрос WINS-серверу.

2.1.2.2 Регистрация имен NetBIOS

При запуске клиент WINS должен зарегистрировать свое NetBIOS имя на сервере WINS. Запросы отправляются непосредственно на сервер WINS. Если имя не используется другой системой, сервер WINS регистрирует имя и посылает пакет подтверждения клиентской системе. Пакет содержит зарегистрированное имя и его срок жизни (TTL) – интервал времени, зарезервированный для клиента, в течение которого имя должно быть перерегистрировано. Если клиент не перерегистрирует имя в указный срок, оно удаляется из базы WINS.

Если клиент пытается зарегистрировать имя уже имеющееся в базе данных WINS, сервер посылает клиенту пакет с приказом на ожидание и убеждается в том, что имя действительно используется. Для этого зарегистрированному владельцу имени посылается пакет с запросом на подтверждение. Если сервер WINS получает ответ от системы-владельца имени, то запрос второй системы на регистрацию имени отвергается. Если ответа нет, то сервер еще дважды посылает запросы, а после освобождает имя и предоставляет его той системе, которая его запросила.

2.1.2.3 Обновление имен NetBIOS

По полученному TTL клиент WINS определяет, в течение какого срока имя NetBIOS должно быть обновлено на сервере WINS (по умолчанию 6 дней). Клиенты WINS пытаются обновить свои имена по истечении 1/8 части срока. Если обновить имя не удается, то клиент ожидает половину срока и вновь повторяет попытку и т.д. Если все попытки окажутся безуспешными, имя NetBIOS высвобождается.

2.1.2.4 Освобождение имен NetBIOS

Перед отключением клиент WINS обязательно должен выдать запрос на

освобождение имени. Для каждого имени зарегистрированного клиентом передается отдельный запрос. Пакет содержит освобождаемое имя и соответствующий ему IP-адрес.

Администрирование сервера WINS

1. Добавление статических записей
2. Настройка репликации
3. Чистка базы данных
4. Архивация базы данных WINS
5. Сжатие базы данных WINS
6. Восстановление базы данных WINS

2.1.2.5 Интеграция WINS и DNS

Служба WINS входит в комплект ОС Windows NT Server и Windows 2000/2003 Server. Поскольку в службе каталога Active Directory вместо NetBIOS-имен применяются имена DNS, сервер WINS включен в эту систему только для обслуживания клиентов, работающих под управлением предыдущих версий Windows. Служба DNS поддерживает интеграцию с WINS. DNS может использовать базу данных WINS и разрешать запросы клиентов WINS в стиле DNS. Если, например, DNS-серверу отправлен запрос на преобразование имени client1.companyabc.com, то DNS-сервер может использовать базу данных WINS для преобразования запросов, адресованных любым зонам, в которых сконфигурирован прямой поиск WINS. Если client1 не существует в базе данных DNS, но существует в базе данных WINS, DNS-сервер возвратит IP-адрес, полученный из WINS, и присоединит к записи суффикс companyabc.com.

2.1.3 Служба обозревателя компьютеров (Browser)

2.1.3.1 Назначение службы обозревателя компьютеров

Основное назначение службы обозревателя заключается в составлении списка компьютеров, совместно использующих ресурсы данного домена, а также списка имен других доменов и рабочих групп в составе глобальной сети (WAN). Этот список передается клиентским компьютерам, которые просматривают сетевые ресурсы с помощью сетевого окружения или команды NET VIEW.

Служба обозревателя определяет имя домена или рабочей группы, в состав которых входит компьютер. В каждом сегменте сети из группы компьютеров, на которых запущена служба обозревателя, выбирается основной обозреватель.

Основной обозреватель собирает объявления серверов (узлов), которые каждые 12 минут отправляются в виде датаграммы каждым сервером в сетевом сегменте основного обозревателя. Кроме того, он отправляет потенциальным обозревателям в каждом сетевом сегменте указание назначать себя в качестве резервных обозревателей. Резервный обозреватель предоставляет список просмотра клиентским компьютерам, которые входят в состав того же сегмента сети.

В структуре домена Windows NT основной контроллер домена (PDC) всегда выбирается в качестве основного обозревателя домена (только PDC может исполнять эту роль). В случае отсутствия основного контроллера домена основной обозреватель домена недоступен, т. е. получить список просмотра от других рабочих групп невозможно.

В каждом сегменте сети может быть только один основной обозреватель. Все контроллеры домена, кроме основного, назначаются резервными обозревателями. Кроме того, один резервный обозреватель назначается для каждых 32 компьютеров в составе сетевого сегмента.

В рабочей группе, которая содержит компьютеры под управлением Windows NT Workstation, всегда имеется один основной обозреватель. Кроме того, если в рабочей группе есть хотя бы два компьютера под управлением Windows NT Workstation, в ней назначается резервный обозреватель (один резервный обозреватель для каждых 32 компьютеров под управлением

Windows NT Workstation в составе рабочей группы).
Если в сетевом сегменте нет контроллеров домена, из состава компьютеров, которые входят в сегмент, проводятся выборы основного и резервного обозревателей. При этом соблюдается следующий порядок очередности:

- Windows 2000 Server
- Windows 2000 Professional
- Windows NT 4.0 Server Enterprise Edition
- Windows NT 4.0 Server
- Windows NT 4.0 Workstation
- Windows 98
- Windows 95
- Windows for Workgroups 3.11

2.1.3.2 Роль основного обозревателя домена

Поскольку служба обозревателя функционирует на основе сегментов широковещания, т. е. каждый основной обозреватель составляет собственный список просмотра, требуется их объединение в единый общедоменный список. Эта задача возложена на основного обозревателя домена, роль которого исполняет основной контроллер домена (реализация этой функции требуется только для протокола TCP/IP).
Кроме того, основной контроллер домена каждые 12 минут подключается к основному серверу WINS для получения списка всех записей NetBIOS-имен типа <1b> (DomainName), зарегистрированных основными контроллерами домена в пределах всей организации. Эти имена, а также собранные основными обозревателями глобальной сети датаграммы объявлений рабочих групп образуют полный список имен доменов и рабочих групп. Имена, определенные с помощью объявлений рабочих групп, имеют более высокий приоритет по сравнению с полученными от службы WINS. Имена доменов и рабочих групп также содержат имя сервера, регистрирующего каждый компьютер в списке просмотра. Если сервер WINS не доступен или не зарегистрирован, обозреватель запрашивает список серверов у компьютера, который зарегистрировал имя. Такая операция производится от имени клиентского компьютера его обозревателем и называется двойным переходом или двойным скачком (double-hop).

Основной контроллер домена объединяет списки, составленные основными обозревателями для каждого сегмента глобальной сети. Каждые 12 минут основной обозреватель подключается к основному контроллеру домена и запрашивает общедоменный список.

Чтобы основной контроллер домена забрал составленный список, основной обозреватель через UDP-порт 138 отправляет ему направленный пакет объявления. Получив этот пакет, основной контроллер домена немедленно подключается к основному обозревателю для получения списка. Каждый резервный обозреватель сегмента с 12-минутным интервалом так же отправляет запросы для получения полного списка серверов, доменов и имен рабочих групп.

2.2 Система доменных имен (DNS)

2.2.1 Общие сведения о DNS

2.2.1.1 Использование плоских символьных имен

В операционных системах, которые первоначально разрабатывались для локальных сетей, таких как Novell NetWare, Microsoft Windows или IBM OS/2, пользователи всегда работали с символьными именами компьютеров. Так как локальные сети состояли из небольшого числа компьютеров, применялись так называемые плоские имена, состоящие из последовательности символов, не разделенных на части. Примерами таких имен являются: NW1_1, mail2, MOSCOW, SALES_2. Для установления соответствия между символьными именами и MAC-адресами в этих операционных системах применялся механизм широковещательных запросов, подобный механизму запросов протокола ARP. Так, широковещательный способ разрешения имен реализован в протоколе NetBIOS, на котором были построены многие локальные ОС. Так называемые NetBIOS-имена стали на долгие годы одним из основных типов плоских имен в локальных сетях.

Для стека TCP/IP, рассчитанного в общем случае на работу в больших территориально распределенных сетях, подобный подход оказывается неэффективным.

2.2.1.2 Иерархические символьные имена

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую наличие в имени произвольного количества составных частей (Рис. 2.1).

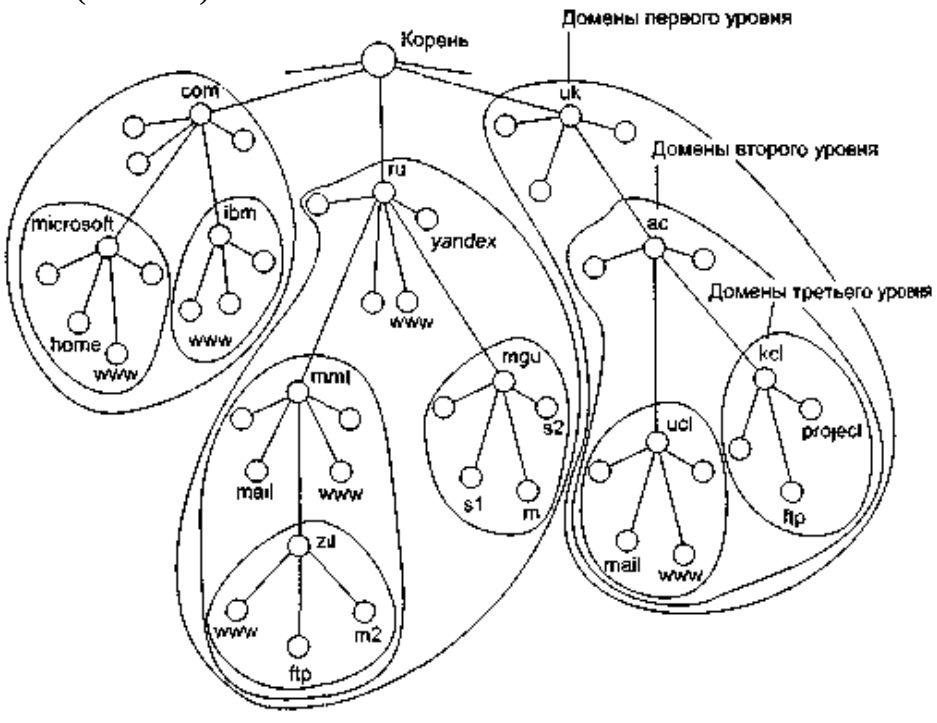

Рис. 17.7. Пространство доменных имён

Рис. 2.1. Пространство иерархических доменных имен

Дерево имен начинается с корня, обозначаемого точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети. Запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей. Составные части доменного имени отделяются друг от друга точкой. Например, в имени partnering.microsoft.com составляющая partnering является именем одного из компьютеров в домене microsoft.com.

Различают краткие имена, относительные имена и полные доменные имена. Краткое имя — это имя конечного узла сети: хоста или порта маршрутизатора. *Краткое имя* — это лист дерева имен. *Относительное имя* — это составное имя, начинающееся с некоторого уровня иерархии, но не самого верхнего. Например, wwwl.zil — это относительное имя. *Полное доменное имя* (Fully Qualified Domain Name, FQDN) включает составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой; www1.zil.mmt.ru.

2.2.1.3 Пространство имен DNS

Ограниченную область, определенную именем DNS, называют пространством имен DNS (microsoft.com, marketing.companyabc.com). Пространства имен могут быть общедоступными или внутренними. Общедоступные пространства публикуются в Internet и определяются набором стандартов. Внутренние пространства не публикуются в Internet и не ограничиваются никакими правилами. Внутренние пространства имен используются в Active Directory. К ним нельзя получить доступ непосредственно из Internet.

2.2.1.4 Преимущества иерархической системы имен

Разделение имени на части позволяет *разделить административную ответственность* за назначение уникальных имен между различными людьми или организациями в пределах своего уровня иерархии. Так, для примера, приведенного на Рис. 2.1, один человек может нести ответственность за то, чтобы все имена, которые имеют окончание «ru», имели уникальную следующую вниз по иерархии часть. Если этот человек справляется со своими обязанностями, то все имена типа www.ru, mail.mmt.ru или we.zil.mmt.ru будут отличаться второй по старшинству частью.

Разделение административной обязанности позволяет решить проблему образования уникальных имен без взаимных консультаций между организациями, отвечающими за имена одного уровня иерархии. Очевидно, что должна существовать одна организация, отвечающая за назначение имен верхнего уровня иерархии.

Корневой домен управляется центральными органами Интернета IANA и InterNIC. Домены верхнего уровня назначаются для каждой страны, а также для различных типов организаций. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, например ru (Россия), uk (Великобритания), fi (Финляндия), us (Соединенные Штаты), а для различных типов организаций — например, следующие обозначения:

- com — коммерческие организации (например, microsoft.com);
- edu — образовательные организации (например, mit.edu);
- gov — правительственные организации (например, nsf.gov);
- org — некоммерческие организации (например, fidonet.org);
- net — сетевые организации (например, nsf.net).

Каждый домен администрирует отдельная организация, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой орган InterNIC делегировал свои полномочия по распределению имен доменов.

Компьютеры входят в домен в соответствии со своими составными именами, при этом они могут иметь абсолютно независимые друг от друга IP-адреса, принадлежащие различным сетям и подсетям. Например, в домен nigu.ru могут входить хосты с адресами 132.13.34.15, 201.22.100.33 и 14.00.6.

2.2.2 Принципы организации DNS

2.2.2.1 Использование файлов hosts.txt

В сетях TCP/IP соответствие между доменными именами и IP-адресами может

устанавливаться средствами, как локального хоста, так и централизованной службы.

Изначально для разрешения доменных имен использовался специальный текстовый файл с известным именем hosts.txt. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «доменное имя — IP-адрес», например:

rhino.acrne.com – 102.54.94.97.

Этот файл помещался на сервере. Каждый клиент копировал этот файл и использовал его для разрешения имен.

По мере роста Интернета файлы hosts.txt также увеличивались в объеме, и создание *масштабируемого* решения для разрешения имен стало необходимостью.

2.2.2.2 Централизованная служба DNS

Таким решением стала *централизованная служба* **DNS** (Domain Name System — система доменных имен), основанная на распределенной базе отображений «доменное имя — IP-адрес». Служба DNS использует в своей работе DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена, как это происходит при использовании файлов hosts. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер.

Имеется два способа распределения имен на серверах:

1. Сервер может хранить отображения «доменное имя - IP-адрес» для всего домена, включая все его поддомены. Такое решение оказывается плохо масштабируемым, так как при добавлении новых поддоменов нагрузка на этот сервер может превысить его возможности.
2. Сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети. В этом случае в зоне DNS обычно присутствуют адреса серверов имен всех его поддоменов. Наличие подобной цепочки позволяет DNS-клиентам опускаться вниз по дереву доменов в поисках нужного узла. Если в родительском домене не упоминаются серверы имен определенных поддоменов, они становятся внутренними и недоступными для внешнего мира.

Например, в первом случае DNS-сервер домена mmt.ru будет хранить отображения для всех имен, заканчивающихся на mmt.ru (www1.zil.mmt.ru, ftp.zil.mmt.ru, mail.mmt.ru и т. Д.). Во втором случае этот сервер хранит отображения только имен типа mail.mmt.ru, www.mmt.ru, а все остальные отображения должны храниться на DNS-сервере поддомена zil.

Каждый DNS-сервер помимо таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

2.2.2.3 Схемы разрешения DNS -имен

Существует две основные схемы разрешения DNS-имен. В первом варианте работу по поиску IP-адреса координирует DNS-клиент.

1. DNS-клиент обращается к своему DNS-серверу с указанием полного доменного имени.

2. DNS-сервер отвечает клиенту, указывая адрес одного из корневых DNS-серверов или DNS-сервера, обслуживающего домен верхнего уровня, заданный в следующей старшей части запрошенного имени.
3. DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена и т.д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Такая процедура разрешения имени называется итерационной, когда клиент сам итеративно выполняет последовательность запросов к разным серверам имен.

Во втором варианте реализуется рекурсивная процедура.

1. DNS-клиент запрашивает свой DNS-сервер
2. Далее возможны два варианта действий:
   a. если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту (это может произойти, когда запрошенное имя входит в тот же поддомен, что и имя клиента, или когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше);
   b. если локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в предыдущем варианте, а получив ответ, передает его клиенту, который все это время просто ждет его от своего локального DNS-сервера.

Для ускорения поиска IP-адресов DNS-серверы широко применяют *кэширование* проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на относительно короткое время — обычно от нескольких часов до нескольких дней.

Используемая схема разрешения DNS-имен определяется настройками конкретного DNS-сервера: является ли он рекурсивным или нет. Если у нерекурсивного DNS-сервера есть искомый ответ, оставшийся в кэше от предыдущих запросов, или он хранит информацию о запрашиваемом узле, то он даст соответствующий ответ. В противном случае он вернет отсылку на DNS-серверы другого домена, которые с большей вероятностью ответят на запрос. Клиенты нерекурсивного DNS-сервера должны быть готовы принимать отсылки и обрабатывать их. Рекурсивный DNS-сервер возвращает только реальные ответы или сообщения об ошибках. Он сам отслеживает отсылки, освобождая от этой обязанности клиента. Все корневые DNS-серверы и серверы доменов верхнего уровня являются нерекурсивными.

2.2.3 Зоны DNS

2.2.3.1 Назначение зоны DNS

Зона в DNS это часть пространства имен DNS, управляемая конкретным сервером или группой серверов DNS. В DNS зона представляет собой основной механизм делегирования полномочий и используется для установки границ, в пределах которых может выполнять запросы конкретный сервер. Границы зоны не определяются доменной структурой. Одна зона может включать в себя несколько доменов, и в то же время объекты домена могут быть размещены в нескольких зонах.

Любой раздел или подраздел DNS может существовать внутри единой зоны. Организация может поместить в единую зону все пространство имен домена, поддоменов и под-поддоменов или может определенные разделы этого пространства имен разделить на отдельные зоны.

Любой сервер, на котором размещена какая-либо зона называют ответственным за эту зону (первичным DNS-сервером для данной зоны). Зона может быть размещена на нескольких серверах. В этом случае на каждом DNS-сервере размещается отдельная копия зоны. Для поддержания этих копий в согласованном состоянии используется модель

репликации с одним основным участником. Один из DNS-серверов выступает в качестве основного носителя зоны. Только основной носитель зоны обладает возможностью вносить изменения в ее содержимое. Остальные DNS-серверы располагают копией зоны доступной только для чтения. Эти серверы называются дополнительными носителями зоны. Изменения, произведенные в копии зоны основным носителем, реплицируются на дополнительные носители.

Использование нескольких серверов позволяет распределить нагрузку между ними, а предоставляет некоторый уровень отказоустойчивости.

На каждом DNS-сервере может быть размещено несколько зон.

2.2.3.2 Виды зон

1. Зоны прямого просмотра (forward lookup zone) создаются для выполнения прямого просмотра в базе данных DNS. Этот тип зон выполняет преобразование имен в IP-адреса и информацию о ресурсах.
2. Зоны обратного просмотра (reverse lookup zone) выполняют преобразование IP-адреса в имя DNS. Для организации распределенной службы и использования для поиска имен того же программного обеспечения, что и для поиска адресов, применяется подход, связанный с представлением IP-адреса в виде DNS-имени.

Первый этап преобразования заключается в том, что составляющие IP-адреса интерпретируются как составляющие DNS-имени. Например, адрес 192.31.106.0 рассматривается как состоящий из старшей части, соответствующей домену 192, затем идет домен 31, в который входит домен 106.

Далее, учитывая, что при записи IP-адреса старшая часть является самой *левой* частью адреса, а при записи DNS-имени — самой *правой,* то составляющие в преобразованном адресе указываются в обратном порядке, то есть для данного примера - 106.31.192.

Для хранения соответствия всех адресов, начинающихся, например, с числа 192, заводится зона 192 со своими серверами имен. Для записей о серверах, поддерживающих старшие в иерархии обратные зоны, создана специальная зона in-addr.arpa, поэтому полная запись для использованного в примере адреса выглядит так: 106.31.192.in-addr.arpa

2.2.3.3 Типы зон

1. Первичные зоны – зоны доступные для редактирования на первичном DNS-сервере
2. Вторичные зоны – копии первичных зон доступные только для чтения и расположенные на вторичных DNS-серверах
3. Зоны-заглушки (упрощенные зоны) – зона заглушка представляет собой копию зоны, содержащую только те ресурсные записи, которые необходимы для локализации DNS-серверов, являющихся носителями полной версии зоны. Основное назначение – идентификация DNS-серверов, которые способны выполнить разрешение доменных имен, принадлежащих этой зоне. Эта зона служит только для переадресации запросов к списку назначенных серверов имен для различных доменов. Зона-заглушка содержит только записи NS, SOA и связанные записи. Связанные записи – это записи типа A, которые используются в сочетании с конкретной записью NS для преобразования IP-адреса конкретного сервера имен. Сервер, содержащий зону-заглушку какого-либо пространства имен, не управляет этой зоной.

2.2.3.4 Методы хранения зон

1. Хранение зоны в файле – этот метод является традиционным и единственным в спецификации службы DNS. Вся информация о

содержимом зоны храниться в текстовом файле. Имя файла образуется из названия зоны добавлением расширения dns (%SystemRoot%\system32\dns).

2. Хранение зоны в доменном разделе каталога - в результате интеграции службы DNS со службой каталога стало возможным размещение содержимого зоны в Active Directory. В этом случае зона представляется в виде объекта каталога контейнерного типа, внутри которого размещаются объекты, ассоциированные с ресурсными записями. Для размещения зоны используется доменный раздел каталога. Такая зона называется зоной, интегрированной в Active Directory. Подобная схема хранения зоны может быть использована только если служба DNS устанавливается на контроллере домена. Размещение зоны в каталоге позволяет задействовать подсистему репликации изменений Active Directory. Это означает, что изменение зоны может производиться в контексте любого контроллера домена. DNS-сервер, установленный на контроллера домена может выступать в качестве основного носителя для зоны, размещенной в каталоге. Недостаток размещения зоны в доменном разделе каталога состоит в том, что она может реплицироваться только в пределах домена.
3. Хранение зоны в разделах приложения – впервые реализован в Windows Server 2003. Может быть использован только на контроллерах домена, работающих под управлением только этой ОС. В этом случае зона храниться в разделе приложений Active Directory. Администратор может размещать раздел приложений только на тех контроллерах домена, которые являются DNS-серверами. Кроме того репликация данных из раздела приложений настраивается и может производиться в пределах всего леса доменов.

2.2.4 Записи ресурсов

2.2.4.1 Структура ресурсной записи

Зона рассматривается как база данных, содержащая сведения об элементах пространства имен DNS. База данных состоит из записей, которые в терминологии DNS называются записями ресурсов или ресурсными записями (resource records). Каждая ресурсная запись имеет следующий состав:

Owner – имя хоста или домена, к которому принадлежит ресурсная запись

TTL – 32-разрядное число, определяющее интервал времени, в течение которого данная запись будет храниться в кэше DNS-сервера или DNS-клиента. Данное поле является не обязательным.

Class – определяет класс ресурсной записи. В настоящее время в данном поле всегда указывается IN.

Type – указывает тип ресурсной записи.

RDATA – данные ресурсной записи. Конкретное значение данного поля определяется типом ресурсной записи.

2.2.4.2 Виды ресурсных записей

1. Запись начала полномочий (SOA – Start of Authority) – указывает, какой сервер ответственен за указанную зону. Указанный в записи SOA сервер считается лучшим источником информации об этой зоне и ответственным за обработку обновлений зоны. Запись SOA информацию о контактном лице, отвечающем за работу DNS и значение TTL по-умолчанию для ресурсных записей данной зоны DNS. Кроме того, в записи SOA указывается ряд параметров, определяющих поведение вторичных серверов DNS для данной зоны:

- порядковый номер (serial number) – целое число, определяющее текущую версию зоны DNS. При изменении содержимого зоны DNS администратор обязан увеличить значение этого параметра. Вторичные DNS-сервера при проведении процедуры синхронизации сравнивают значение порядкового номера в записи SOA своей копии зоны со значением в записи SOA на первичном DNS сервере. Если значение на первичном DNS-сервере больше, то происходит обновление содержимого зоны DNS на вторичном сервере
- период обновления зоны (refresh) – промежуток между синхронизациями зоны DNS на вторичных серверах в секундах
- период повтора обновления (retry) – промежуток времени в секундах, по истечении которого на вторичном сервере повторно инициируется процедура синхронизации, если предыдущая синхронизация закончилась неудачно
- период актуальности (expire) – промежуток времени в секундах, в течение которого вторичный DNS-сервер будет разрешать запросы в данную зону в случае недоступности первичного DNS-сервера. По истечении этого времени содержимое зоны DNS на вторичном сервере считается устаревшим и вторичный DNS-сервер прекращает разрешать запросы об этой зоне DNS вплоть до очередной удачной синхронизации с первичным DNS-сервером

Пример записи SOA:

```
@               IN  SOA serv01.companyA.local.  hostmaster.companyA.local. (
                        26            ; serial number
                        900          ; refresh
                        600          ; retry
                        86400        ; expire
                        3600       ) ; default TTL
```

2. Записи хостов (A) – основной тип ресурсной записи зон прямого просмотра. Содержит имя хоста и соответствующий ему IP-адрес.

```
pc01                    A     192.168.99.2
```

3. Записи сервера имен (NS) – указывают, какие компьютеры в БД DNS являются серверами имен, т.е. DNS-серверами для данной зоны. Для каждой зоны может существовать только одна запись SOA, но несколько NS-записей, которые указывают клиентам, к каким хостам можно адресовать DNS-запросы. Записи NS не содержат IP-адреса конкретного ресурса, а указывают на записи типа A DNS-сервера:

```
@                       NS    serv01.companyA.local.
```

4. Записи служб (SRV) – это записи ресурсов, которые указывают на ресурсы, выполняющие конкретные услуги. Каждая запись SRV содержит информацию о конкретных функциях, выполняемых данным ресурсом. Например, LDAP-сервер может добавить запись SRV, указывающую, что он может обрабатывать LDAP-запросы для конкретной зоны. Обращение к контроллерам в Active Directory осуществляется посредством записей SRV, определяющих следующие службы: глобальный каталог, LDAP и Kerberos. Позволяет администраторам использовать несколько серверов для предоставления каких-либо услуг (http, smtp, ldap и т.д.) для одного имени DNS, просто перенося службу TCP/IP с одного узла администрирования на другой, и назначать некоторые узлы-поставщики служб в качестве основных серверов служб, а другие узлы - в качестве вспомогательных или архивных. Например, когда WEB-броузер, поддерживающий srv-записи, получает запрос вида http://www.lipetsk.ru он пробует разрешить следующий запрос DNS: http.tcp.www.lipetsk.ru. В DNS могут быть созданы несколько таких SRV-записей для различных хостов, которые и будут возвращены

клиенту. Клиент выберет для обращения один из серверов с учетом приоритетов и весов, которые указываются в SRV-записи (RFC 2052). Клиент должен всегда сначала выбирать хосты с меньшим значением приоритета. Хосты с одинаковым приоритетом выбираются в случайном порядке, при этом учитывается вес каждого хоста. Вероятность выбора какого-либо хоста из группы с одинаковым приоритетом пропорциональна указанному в SRV-записи весу хоста. Кроме этого запись SRV содержит номер порта службы.

```
ftp.tcp     SRV   10 5 21     serv02.companya.local.
ftp.tcp     SRV   10 8 21     serv03.companya.local.
```

5. Записи обмена почтой (MX) – указывают, какие ресурсы позволяют принимать почту по протоколу SMTP. Запись MX содержит имя хоста или домена, обслуживаемого обработчиком почты, FQDN имя обработчика почты и его приоритет. Записи MX могут быть определены на уровне домена, чтобы адресованная конкретному домену почта направлялась серверу или серверам, указанным в этой записи. Например, если запись MX определена для домена companyabc.com, то вся почта по адресу user@companyabc.com, будет автоматически направляться серверу, указанному в MX записи.

```
company.com                    MX   10    serv02.companyA.local.
```

6. Записи указателей (PTR) – содержат ссылки на записи типа A. Используются для разрешения по IP-адресу имени хоста. Обычно находятся в зонах обратного просмотра.

```
2                       PTR   pc01.companyA.local.
```

7. Записи канонических имен (CNAME) – представляет псевдоним хоста, что делает возможной в DNS ссылку на любой хост по нескольким именам. Позволяет назначать узлу дополнительные мнемонические имена. Псевдонимы широко применяются для закрепления за компьютером какой-либо функции либо просто для сокращения его имени. Эта запись перенаправляет адресованные ей запросы на записи A данного хоста.

```
www                     CNAME pc01.companyA.local.
```

8. Записи AAA – отображает стандартный IP-адрес на 128-битный адрес IPv6
9. Запись MB – указывает хост, содержащий конкретный почтовый ящик (RFC 1035).

```
@                       MB    serv02.companya.local.
```

10. Запись хорошо известной службы (WKS - Well Known Service) - используется для описания хорошо известных служб TCP/IP, поддерживаемых на конкретном порту на конкретном хосте. В записи указывается IP-адрес хоста, код протокола (например, TCP (6) или UDP (17)) и битовая маска определяющая порты, работающие на сервере (0-й бит – порт№0, 1-й бит – порт№1 и т.д.) Например, если на хосте работают службы FTP (21) и HTTP (80), то – биты 22 и 81 будут установлены в битовой маске. Записи WKS обеспечивают доступность информации об открытых TCP и UDP портах. Если сервер поддерживает и TCP, и UDP для хорошо известной службы или если сервер имеет несколько IP-адресов, по которым работает служба, то используются несколько записей WKS. (Подробнее см. RFC 1035)

```
serv01                  WKS   192.168.3.10      tcp (
                                ftp
                                http )
```

2.2.5 Особенности функционирования DNS

2.2.5.1 Возможности DNS-клиентов Windows

В составе Windows Server 2003 имеется служба DNS-клиента. DNS-клиент осуществляет взаимодействие с DNS-сервером с целью разрешения доменных имен в IP-адреса. Реализация DNS-клиента характеризуется следующими возможностями:

- клиентское кэширование. Ресурсные записи (RR), полученные как ответы на запросы, добавляются в клиентский кэш. Эта информация хранится в течение заданного времени и может использоваться для ответа на последующие запросы;

- кэширование отрицательных ответов. В дополнение к кэшированию положительных ответов на запросы от серверов DNS, служба DNS также кэширует отрицательные ответы на запросы. Отрицательный ответ приходит, если ресурсная запись с запрошенным именем не существует. Кэширование отрицательных ответов предотвращает повторные запросы для несуществующих имен, снижающие производительность клиентской службы;

- блокировка неотвечающих серверов DNS. Клиентская служба DNS использует список поиска серверов, упорядоченных по предпочтению. Этот список включает все серверы DNS, настроенные для каждого из активных сетевых подключений в системе. Система способна перестраивать этот список, основываясь на следующих критериях: предпочтительные серверы DNS имеют высший приоритет, а остальные серверы DNS чередуются. Неотвечающие серверы временно удаляются из списка.

2.2.5.2 Режимы работы DNS-серверов

Выделяют следующие работы DNS-серверов: режим работы в качестве основного (авторитетного), вторичного (подчиненного) и кэширующего сервера. Эти режимы отличаются двумя характеристиками: откуда поступают данные и авторитетен ли сервер для домена.

1. Основной (авторитетный, primary) – это сервер, который поддерживает обновляемую, авторитетную зону для некоторого домена. На нем хранится официальная копия данных зоны DNS. Гарантируется, что ответ авторитетного сервера является абсолютно точным.
2. Вторичный (подчиненный, secondary) – это сервер, хранящий доступную для чтения копию зоны, копируемой с некоторого основного сервера. Ответ вторичного сервера является неавторитетным и может быть устаревшим. Если основной и вторичный серверы DNS поддерживают зоны, интегрированные в Active Directory, то такие серверы рассматриваются как равноправные, и обновления могут выполняться на любом сервере.
3. Кэширующий (cashing) - это автономный сервер DNS, который не хранит авторитетных зон, содержит адреса серверов корневого домена и может только хранить ответы на запросы клиентов, полученные от других DNS-серверов. Кэширующий сервер не является авторитетным. Он позволяет сократить объем DNS-трафика во внутренней сети и уменьшить время на выполнение DNS-запросов.

2.2.5.3 Расщепление DNS

Во многих организациях требуется, чтобы внутреннее представление сети отличалось от представления этой сети с точки зрения пользователей Internet. Например, в сети организации имеется почтовый сервер mail-serv (192.168.1.10), который доступен внешним пользователям по внешнему адресу 195.34.239.56. Данный почтовый сервер обслуживает почтовый домен OrganizationA.dom.ru. Сотрудники организации пользуются ноутбуками и им требуется получать почту как находясь в организации, так и вне ее. Таким образом, одно и то же DNS-имя, например, mail-serv.organizationA.dom.ru должно разрешаться в два разных

IP-адреса: 192.168.1.10 - для пользователей локальной сети организации и 195.34.239.56 – для пользователей сети Internet.

Подобная конфигурация называется расщеплением DNS и реализуется путем запуска различных DNS-серверов для внутренней и внешней версий зоны DNS. Локальные клиенты обращаются к DNS-серверам, рассылающим внутреннюю версию зоны, а записи NS родительской зоны DNS сети Internet ссылаются на серверы, хранящие ее внешнюю версию.

2.2.5.4 Динамическая DNS

Пользуясь динамической DNS, клиенты могут автоматически обновлять свои записи в DNS в соответствии с настройками безопасности данной зоны. По умолчанию динамические обновления отключены для стандартных зон. Для зон, интегрированных в AD, существует механизм, который позволяет клиентам выполнять безопасные динамические обновления. При безопасных обновлениях используется аутентификация пользователей с помощью Kerberos, обеспечивающая, что запись могут обновлять только создавшие ее клиенты.

Клиент предпринимает попытку зарегистрировать доменное имя в базе данных DNS-сервера в следующих ситуациях:

1. Происходит изменение IP-адреса.
2. В процессе загрузки системы.
3. Выполняется команда ipconfig /registerdns, вызывающая принудительное обновление доменного имени клиента в базе данных DNS-сервера

Динамические обновления поддерживают только клиенты Windows 2000/XP. Для обновления в DNS информации клиентов предыдущих систем (NT/9x) они должны иметь сконфигурированный соответствующим образом протокол DHCP.

Параллельно с механизмом динамической регистрации имен DNS-сервер активизирует механизм очистки базы данных от устаревших ресурсных записей. С каждой ресурсной записью ассоциируется временная метка, определяющая время ее создания. Ресурсная запись считается актуальной в течение определенного периода времени, называемого периодом стабильности. Обновление сведений о ресурсной записи в течение этого периода приводит к обновлению значения временной метки. Система ожидает обновления ресурсной записи в течение периода, который называется периодом обновления. Если для ресурсной записи истек период обновления, то запись помечается как устаревшая. Все устаревшие записи удаляются автоматически в процессе очистки базы DNS-сервера. Этот процесс инициируется системой автоматически через определенные промежутки времени.

2.3 Протокол DHCP

2.3.1 Назначение и спецификация DHCP

Для нормальной работы сети каждому сетевому интерфейсу компьютера и маршрутизатора должен быть назначен IP-адрес.

Процедура присвоения адресов происходит в ходе конфигурирования компьютеров и маршрутизаторов. Назначение IP-адресов может происходить вручную в результате выполнения процедуры конфигурирования интерфейса, для компьютера сводящейся, например, к заполнению системы экранных форм. При этом администратор должен помнить, какие адреса из имеющегося множества он уже использовал для других интерфейсов, а какие еще свободны. При конфигурировании помимо IP-адресов сетевых интерфейсов (и соответствующих масок) устройству сообщается ряд других конфигурационных параметров. При конфигурировании администратор должен назначить клиенту не только IP-адрес, но и другие параметры стека TCP/IP, необходимые для его эффективной работы, например маску и IP-адрес маршрутизатора по умолчанию, IP-адрес сервера DNS, доменное имя компьютера и т. д.

Протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCP) автоматизирует процесс конфигурирования сетевых интерфейсов, гарантируя от дублирования адресов за счет централизованного управления их распределением. Работа DHCP описана в RFC 2131 и 2132.

2.3.1.1 Спецификация протокола DHCP

В спецификации протокола определяются два участника: DHCP-сервер и DHCP-клиенты. Служба клиента DHCP запрашивает у DHCP-сервера параметры для настройки стека протоколов TCP/IP. Служба сервера DHCP обрабатывает клиентские запросы, осуществляя выдачу в аренду IP-адреса из некоторого диапазона. Каждый адрес выделяется на определенный срок. По окончании срока хост должен либо продлить срок аренды, либо освободить адрес. Все удовлетворенные запросы пользователей фиксируются службой сервера DHCP в собственной базе данных. Это позволяет предотвратить выделение одного и того же IP-адреса двум хостам. Одновременно с выдачей IP-адреса DHCP-сервер может предоставить клиенту дополнительную информацию о настройках стека протоколов TCP/IP (маска подсети, адрес шлюза, серверов DNS, WINS и т.д.)

В спецификации DHCP определен так же агент ретрансляции DHCP (DHCP-relay), который может осуществлять трансляцию широковещательных сообщений DHCP между подсетями. Агент ретранслятор прослушивает подсети на наличие широковещательных сообщений DHCP и переадресовывает их на некоторый заданный DHCP-сервер. Использование агентов ретрансляции избавляет от необходимости устанавливать DHCP сервер в каждом физическом сегменте сети.

2.3.1.2 Основные понятия DHCP

1. Область DHCP (scope). Под областью понимается административная группа, идентифицирующая полные последовательные диапазоны возможных IP-адресов для всех DHCP-клиентов в физической подсети. Области определяют логическую подсеть, для которой должны предоставляться услуги DHCP. Область должна быть определена прежде, чем DHCP-клиенты смогут использовать DHCP-сервер для динамической конфигурации TCP/IP. Область должна быть создана для каждой физической подсети.
2. Супербласть (superscope). Множество областей, сгруппированных в отдельный административный объект, представляет собой супербласть. Использование суперобластей оправдано в ситуации, когда для одной подсети имеется несколько несмежных диапазонов IP-адресов. В этом случае каждый диапазон реализуется в

виде отдельной области действия. Суперобласть действия выступает в качестве средства объединения получившихся областей. Суперобласти используются для реализации в пределах одной физической сети нескольких логических подсетей – мультисетей.

3. Диапазоны исключения (exclusion range). Диапазон исключения – ограниченная последовательность IP-адресов в пределах области, которые должны быть исключены из предоставления службой DHCP.
4. Пул адресов (address pool). Если определена область и заданы диапазоны исключения, то оставшаяся часть адресов называется пулом доступных адресов. Эти адреса могут быть динамически назначены клиентам DHCP в сети.
5. Резервирование (reservation). Резервирование позволяет на основе MAC-адреса назначить клиенту постоянный адрес и гарантировать, что указанное устройство в подсети может всегда использовать один и тот же IP-адрес.
6. Период аренды (lease). Под периодом аренды понимается отрезок времени, в течение которого клиентский компьютер может использовать выделенный IP-адрес.
7. Опции DHCP (option DHCP). Опции DHCP представляют собой дополнительные параметры настройки клиентов, которые DHCP_сервер может назначать одновременно с выделением IP-адреса. В RFC 2132 определено более 30 опций. Каждая опция идентифицируется посредством 8-разрядного кода, определяющего назначение опции. Опции могут быть определены на уровне всего сервера, отдельной области действия, класса и отдельного клиента.
8. Класс DHCP. Класс DHCP рассматривается как некая логическая группа компьютеров, объединенных по некоторому признаку. Например, компьютеры, имеющие доступ в Internet, или клиенты удаленного доступа. Чтобы отнести хост к некоторому классу, администратор должен использовать утилиту ipconfig с ключом /setclassid. С помощью классов можно переопределить параметры DHCP для некоторых компьютеров.

2.3.2 Режимы работы DHCP

Сервер DHCP может работать в разных режимах:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

2.3.2.1 Ручное назначение статических адресов

В ручном режиме администратор, помимо пула доступных адресов, снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, *всегда* выдает определенному DHCP-клиенту *один и тот же* назначенный ему администратором IP-адрес (а также набор других конфигурационных параметров).

2.3.2.2 Автоматическое назначение статических адресов

В режиме автоматического назначения статических адресов DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает клиенту IP-адрес из пула наличных IP-адресов. Адрес дается клиенту из пула в постоянное пользование, то есть между идентифицирующей информацией клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первого назначения DHCP-сервером IP-адреса клиенту. При всех последующих запросах сервер возвращает клиенту тот же самый IP-адрес.

2.3.2.3 Динамическое распределение адресов

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, являющийся DHCP-клиентом, удаляется из подсети, 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 дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру. Динамическое разделение адресов позволяет строить IP-есть, количество узлов в которой превышает количество имеющихся в распоряжении администратора IP-адресов.

Пример

Рассмотрим преимущества, которые дает динамическое разделение пула адресов на примере организации, в которой сотрудники значительную часть рабочего времени проводят вне офиса — дома или в командировках. Каждый из них имеет портативный компьютер, который во время пребывания в офисе подключается к корпоративной сети. Возникает вопрос, сколько IP-адресов необходимо этой организации? Первый ответ — столько *скольким сотрудникам необходим доступ в сеть.* Если их 500 человек, то каждому из них должен быть назначен IP-адрес и выделено рабочее место. То есть администрация должна получить у поставщика услуг адреса двух сетей класса С и оборудовать соответствующим образом помещение. Однако, сотрудники в этой организации редко появляются в офисе, значит, большая часть ресурсов при таком решении будет простаивать.

Второй ответ — столько, *сколько сотрудников обычно присутствует в офисе* (с некоторым запасом). Если обычно в офисе работает не более 50 сотрудников, то достаточно получить у поставщика услуг пул из 64 адресов и установить в рабочем помещении сеть с 64 коннекторами для подключения компьютеров. Но возникает другая проблема — кто и как будет конфигурировать компьютеры, состав которых постоянно меняется? Существует два пути. Во-первых, администратор (или сам мобильный пользователь) может конфигурировать компьютер вручную каждый раз, когда возникает необходимость подключения к офисной сети. Такой подход требует от администратора (или пользователей) выполнения большого объема рутинной работы, следовательно — это плохое решение. Гораздо привлекательнее выглядят возможности автоматического динамического назначения адресов DHCP. Действительно, администратору достаточно один раз при настройке DHCP-сервера указать диапазон из 64 адресов, а каждый вновь прибывающий мобильный пользователь будет просто физически подключать в сеть свой компьютер, на котором запускается DHCP-клиент. Он запросит конфигурационные параметры и автоматически получит их от DHCP-сервера. Таким образом, для работы 500 мобильных сотрудников достаточно иметь в офисной сети 64 IP-адреса и 64 рабочих места.

2.3.2.4 Алгоритм динамического назначения адресов

Ниже дана упрощенная схема обмена сообщениями между клиентскими и серверными частями DHCP.

1. DHCP-клиент посылает ограниченное широковещательное сообщение DHCP-поиска (DCHP Discover) - IP-пакет с адресом назначении, состоящим из одних единиц, который должен быть доставлен всем узлам данной IP-сети.
2. Все DHCP-серверы, получившие сообщение DHCP-поиска, посылают DHCP-клиенту, обратившемуся с запросом, свои DHCP-предложения. Каждое предложение содержит IP-адрес и другую конфигурационную информацию (DCHP offer).
3. DHCP-клиент собирает конфигурационные DHCP-предложения ото всех DHCP-серверов. Как правило, он выбирает первое из поступивших предло-

жений и отправляет в сеть широковещательный DHCP-запрос. В этом запросе содержатся идентификационная информация о DHCP-сервере, предложение которого принято, а также значения принятых конфигурационных параметров (DHCP Request).

4. Все DHCP-серверы получают DHCP-запрос, и только один выбранный DHCP-сервер посылает положительную DHCP-квитанцию (DHCP Acknowledgement) (подтверждение IP-адреса и параметров аренды), а остальные серверы аннулируют свои предложения, в частности возвращают в свои пулы предложенные адреса.
5. DHCP-клиент получает положительную DHCP-квитанцию и переходит в рабочее состояние.

Адрес клиенту предоставляется на определенный срок, называемый периодом аренды. По истечении половины этого срока клиент должен возобновить аренду. Если ответа нет или ответ отрицательный, он через некоторое время снова посылает запрос. Если аренда не продлена до окончания срока аренды, то выделенный клиенту адрес возвращается в пул для повторного использования. В этой ситуации клиент должен инициализировать процедуру получения IP-адреса с самого начала.

2.3.2.5 Проблемы, обусловленные использованием динамического назначения адресов

В сети, где адреса назначаются динамически, нельзя быть уверенным в адресе, который в данный момент имеет тот или иной узел. И такое непостоянство IP-адресов влечет за собой некоторые проблемы.

Во-первых, *возникают сложности при преобразовании символьного доменного имени в IP-адрес*. Действительно, представьте себе функционирование системы DNS, которая должна поддерживать таблицы соответствия символьных имен IP-адресам в условиях, когда последние меняются каждые два часа! Учитывая это обстоятельство, для серверов, к которым пользователи часто обращаются по символьному имени, назначают статические IP-адреса, оставляя динамические только для клиентских компьютеров. Однако в некоторых сетях количество серверов настолько велико, что их ручное конфигурирование становится слишком обременительным. Это привело к разработке усовершенствованной версии DNS (так называемой динамической системы DNS), в основе которой лежит согласование информационной адресной базы в службах DHCP и DNS.

Во-вторых, *трудно осуществлять удаленное управление и автоматический мониторинг интерфейса* (например, сбор статистики), если в качестве его идентификатора выступает динамически изменяемый IP-адрес.

Наконец, для обеспечения безопасности сети многие сетевые устройства могут блокировать (фильтровать) пакеты, определенные поля которых имеют некоторые заранее заданные значения. Другими словами, при динамическом назначении адресов *усложняется фильтрация пакетов по IP-адресам.*

Последние две проблемы проще всего решаются отказом от динамического назначения адресов для интерфейсов, фигурирующих в системах мониторинга и безопасности.

2.3.3 Обеспечение отказоустойчивости DHCP

Для обеспечения отказоустойчивости рекомендуется использовать в сети по крайней мере два DHCP-сервера. Хотя в службе DHCP отсутствует какой-либо метод динамической работы нескольких серверов, можно сконфигурировать среду DHCP с возможностью подхвата функций при отказе сервера. Для обеспечения избыточности существуют три возможности.

2.3.3.1 Метод подхвата функций 50/50.

В этом случае используются два DHCP-сервера. Каждый DHCP-сервер конфигурируется с одной и той же областью действия, но с различными диапазонами исключения IP-адресов. Диапазон исключаемых адресов одного сервера должен соответствовать диапазону адресов, предоставляемых другим сервером, чтобы при попытке продления аренды клиентом другого сервера он не получил отказ. В диалоге клиента и сервера могут возникнуть проблемы, если клиент использовал IP-адрес вне присутствовавшего в области диапазона. Однако если диапазон существует, но заданы исключения из него, сервер просто назначит клиенту новый адрес из пула доступных адресов.

Преимуществом подхода является то, что в среду DHCP внедряется значительная избыточность без резервирования для клиентов дополнительных диапазонов IP-адресов.

Недостатком является то, что клиенты могут все время обращаться только к одному из серверов, что приведет к исчерпанию DHCP-сервером арендуемых адресов. Таким образом, избыточность DHCP-среды пропадет.

2.3.3.2 Метод подхвата функций 80/20.

Эффективный диапазон адресов распределяется между двумя серверами в соотношении 80/20. В большинстве случаев сервер, содержащий 20% процентов располагается в другой подсети и начинает обслуживать клиентов, только в случае отказа основного DHCP-сервера.

Недостаток подхода состоит в том, что при длительном простое основного сервера все арендуемые адреса второго сервера будут исчерпаны, и возобновление аренды адресов клиентами DHCP станет невозможно.

2.3.3.3 Метод подхвата функций 100/100

Это метод предполагает использование двух DHCP-серверов, обслуживающих одни и те же подсети организации. Каждый сервер содержит различные равные по размеру пулы доступных IP-адресов. Количество адресов в каждом пуле достаточно для обслуживания всех клиентов конкретной подсети.

Преимущество такой архитектуры состоит в том, что в случае отказа одного сервера, второй немедленно выдаст новые IP-адреса клиентам, которые ранее обслуживались отказавшим сервером. Отказавший сервер может оставаться отключенным в течение всего срока аренды, т.к. второй сервер способен взять на себя всех его клиентов. Поскольку оба сервера работают постоянно, подхват функций происходит немедленно.

Недостатком этого подхода является необходимость наличия большого количества доступных клиентам IP-адресов.