



МЧС РОССИИ

Управление информационных технологий и связи

РЕФЕРАТ

по самостоятельной подготовке

Тема: «DHCP-сервер. Пространство внешних и внутренних имен».

Выполнил:

Старший мастер связи (обеспечения эксплуатации инфраструктуры на территории г. Арзамас Нижегородской области) отделения ФПС ГПС обеспечения эксплуатации инфраструктуры управления информационных технологий и связи Главного управления МЧС России по Нижегородской области
сержант внутренней службы

Д.В. Кучин

Проверил:

Заместитель начальника управления информационных технологий и связи
майор внутренней службы

Д.С. Соколов

Нижегород 2022 год

О Г Л А В Л Е Н И Е

| Рассматриваемый вопрос | Страница |
|---|-----------------|
| ОГЛАВЛЕНИЕ | 2 |
| ВВЕДЕНИЕ | 3 |
| СЕРВИСЫ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ | 4 |
| КОНТРОЛЛЕРЫ ДОМЕНА И РЯДОВЫЕ СЕРВЕРЫ | 6 |
| ФУНКЦИИ КОМАНДНОЙ СТРОКИ | 7 |
| ИСПОЛЬЗОВАНИЕ КОМАНДЫ NET | 7 |
| СОЗДАНИЕ СОЕДИНЕНИЯ УДАЛЕННОГО РАБОЧЕГО СТОЛА | 8 |
| СЛУЖБА DNS | 9 |
| ВОЗМОЖНОСТИ DNS-КЛИЕНТОВ | 11 |
| СТРУКТУРА DNS | 11 |
| ПРОСТРАНСТВО ИМЕН DNS | 12 |
| ЗОНЫ | 14 |
| РЕСУРСНЫЕ ЗАПИСИ | 15 |
| УПРОЩЕННЫЕ ЗОНЫ | 16 |
| ДИНАМИЧЕСКАЯ РЕГИСТРАЦИЯ ИМЕН | 17 |
| РАЗВЕРТЫВАНИЕ DNS | 19 |
| ФАЙЛ HOSTS | 20 |
| ЗАКЛЮЧЕНИЕ | 21 |
| ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА | 22 |

ВВЕДЕНИЕ

DHCP-сервер (DHCP Server). Предоставляет службы автоматического выделения IP-адресов клиентам, настроенным на динамическое получение IP-адресов. Если выбрать этот вариант, устанавливаются службы DHCP и запускается Мастер создания области (New Scope Wizard), позволяющий определить один или несколько диапазонов IP-адресов в сети.

Стандартный механизм сопровождения зоны предполагает создание администратором вручную статических ресурсных записей. Любое произведенное изменение доменного имени хоста или его IP-адреса администратор должен синхронизировать с базой данных службы DNS, вручную изменяя соответствующие записи. Подобная схема изменения содержимого зоны делает практически невозможным использование в корпоративной сети службы динамического выделения адресов (DHCP).

В спецификации службы DNS определена возможность использования механизма динамической регистрации хостами своих доменных имен. В процессе динамической регистрации клиенты могут создавать и изменять ресурсные записи типа A и PTR. Контроллеры домена могут также динамически регистрировать ресурсные записи типа SRV.

СЕРВИСЫ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ

После установки и активации Windows необходимо настроить сервер, используя Управление данным сервером (Manage Your Server), которая автоматически открывается при входе в систему. Эта страница упрощает установку некоторых служб, инструментов и конфигураций в зависимости от роли сервера.

В режиме Особая конфигурация (Custom Configuration), мастер может настроить следующие роли.

- **Файловый сервер (File Server).** Обеспечивает централизованный доступ к файлам и каталогам для пользователей, отделов и организации в целом. Выбор этого варианта позволяет управлять пользовательским дисковым пространством путем включения и настройки средств управления дисковыми квотами и ускорить поиск в файловой системе за счет активизации Службы индексирования (Indexing Service).

- **Сервер печати (Print Server).** Обеспечивает централизованное управление печатающими устройствами, предоставляя клиентским компьютерам доступ к общим принтерам и их драйверам. Если выбрать этот вариант, запустится Мастер установки принтеров (Add Printer), позволяющий установить принтеры и соответствующие драйверы. Кроме того, мастер устанавливает службы IIS 6.0 (Internet Information Services), настраивает протокол печати IPP (Internet Printing Protocol) и Web-средства управления принтерами.

- **Application Server IIS, ASP.NET (Сервер приложений IIS, ASP.NET).** Предоставляет компоненты инфраструктуры, которые требуются для поддержки размещения Web-приложений. Эта роль устанавливает и настраивает IIS 6.0, ASP.NET и COM+.

- **Mail Server POP3, SMTP (Почтовый сервер POP3, SMTP).** Устанавливает POP3 и SMTP, чтобы сервер мог выступать в роли почтового сервера для клиентов POP3.

- **Сервер терминалов (Terminal Server).** Позволяет множеству пользователей с помощью клиентского ПО Службы терминалов (Terminal Services) или Дистанционное управление рабочим столом (Remote Desktop) подключаться к приложениям и ресурсам сервера, например принтерам или дисковому пространству, как если бы эти ресурсы были установлены на их компьютерах. В отличие от Windows 2000, Windows Server 2003 предоставляет Дистанционное управление рабочим столом автоматически. Роли сервера

терминалов требуются, только когда нужно размещать приложения для пользователей на сервере терминалов.

- Сервер удаленного доступа или VPN-сервер (Remote Access/VPN Server). Обеспечивает маршрутизацию по нескольким протоколам и службы удаленного доступа для коммутируемых, локальных (LAN) и глобальных (WAN) вычислительных сетей. Виртуальная частная сеть (virtual private network, VPN) обеспечивает безопасное соединение пользователя с удаленными узлами через стандартные Интернет-соединения.

- Контроллер домена Active Directory (Domain Controller Active Directory). Предоставляет службы каталогов клиентам сети. Этот вариант позволяет создать контроллер нового или существующего домена и установить DNS. Если выбрать эту роль, запускается Мастер установки Active Directory (Active Directory Installation Wizard).

- DNS Server (DNS-сервер). Обеспечивает разрешение имен узлов: DNS-имена преобразуются в IP-адреса (прямой поиск) и обратно (обратный поиск). Если выбрать этот вариант, устанавливается служба DNS и запускается Мастер настройки DNS- сервера (Configure A DNS Server Wizard).

- DHCP-сервер (DHCP Server). Предоставляет службы автоматического выделения IP-адресов клиентам, настроенным на динамическое получение IP-адресов. Если выбрать этот вариант, устанавливаются службы DHCP и запускается Мастер создания области (New Scope Wizard), позволяющий определить один или несколько диапазонов IP-адресов в сети.

- Сервер потоков мультимедиа (Streaming Media Server). Предоставляет службы WMS (Windows Media Services), которые позволяют серверу передавать потоки мультимедийных данных через Интернет. Содержимое может храниться и предоставляться по запросу или в реальном времени. Если выбрать этот вариант, устанавливается сервер WMS.

- WINS-сервер (WINS Server). Обеспечивает разрешение имен компьютеров путем преобразования имен NetBIOS в IP-адреса. Устанавливать службу WINS (Windows Internet Name Service) не требуется, если вы не поддерживаете старые ОС, например Windows 95 или NT. Такие ОС, как Windows 2000 и XP не требуют WINS, хотя старым приложениям, работающим на этих

платформах, может понадобиться разрешать имена NetBIOS. Если выбрать этот вариант, устанавливается сервер WINS.

КОНТРОЛЛЕРЫ ДОМЕНА И РЯДОВЫЕ СЕРВЕРЫ

При установке Windows Server 2003 систему можно конфигурировать как рядовой сервер, контроллер домена или изолированный сервер. Различия между этими типами серверов чрезвычайно важны. Рядовые серверы являются частью домена, но не хранят информацию каталога. Контроллеры домена хранят данные каталога и выполняют службы аутентификации и каталога в рамках домена. Изолированные серверы не являются частью домена и имеют собственную БД пользователей, поэтому изолированный сервер также аутентифицирует запросы на вход.

Windows Server 2003 не различает основные и резервные контроллеры домена, так как поддерживает модель репликации с несколькими хозяевами. В этой модели любой контроллер домена может обрабатывать изменения каталога и затем автоматически реплицирует их на другие контроллеры домена. В модели репликации с одним хозяином в Windows NT все происходит не так: основной контроллер домена хранит главную копию каталога, а резервные — ее копии. Кроме того, Windows NT распространяет только БД диспетчера учетных записей безопасности (security access manager, SAM), а Windows Server 2003 — весь каталог информации, называемый хранилищем данных (datastore). В нем есть наборы объектов, представляющие учетные записи пользователей, групп и компьютеров, а также общие ресурсы, например серверы, файлы и принтеры.

Домены, в которых применяются службы Active Directory, называют доменами Active Directory, чтобы отличать их от доменов Windows NT. Хотя Active Directory работает только с одним контроллером домена, в домене можно и нужно создать дополнительные контроллеры. Если ОДИН контроллер выходит из строя, для выполнения аутентификации и других важных задач можно задействовать другие.

В домене Active Directory любой рядовой сервер разрешается повысить до уровня контроллера домена без переустановки ОС, как того требовала Windows NT. Для превращения рядового сервера в контроллер следует лишь установить на него компонент Active Directory. Возможно и обратное действие: понижение контроллера

домена до рядового сервера, если он не является последним контроллером домена в сети. Вот как повысить или понизить уровень сервера посредством мастера установки Active Directory.

ФУНКЦИИ КОМАНДНОЙ СТРОКИ

В Windows Server 2003 масса утилит командной строки. Многие из них используют протокол TCP/IP, поэтому его следует предварительно установить.

Как администратору, вам следует знать следующие утилиты командной строки.

- ARP отображает и управляет программно-аппаратной привязкой адресов, используемой Windows Server 2003 для отправки данных по сети TCP/IP.
- FTP запускает встроенный FTP-клиент.
- HOSTNAME отображает имя локального компьютера.
- IPCONFIG отображает свойства TCP/IP для сетевых адаптеров, установленных в системе. Также используется для обновления и освобождения выданных службой DHCP адресов.
- NBTSTAT отображает статистику и текущее соединение для протокола NetBIOS по-верх TCP/IP.
- NET отображает список подкоманд команды NET.
- NETSH отображает и управляет сетевой конфигурацией локального и удаленных компьютеров.
- NETSTAT отображает текущие TCP/Ip соединения и статистику протокола.
- NSLOOKUP проверяет статус узла или IP-адреса при использовании с DNS.
- PATHPING проверяет сетевые пути и отображает информацию о потерянных пакетах.
- PING тестирует соединение с удаленным узлом.
- ROUTE управляет таблицами маршрутизации в системе.
- TRACERT вовремя цитирован и я определяет сетевой путь к удаленному узлу.

ИСПОЛЬЗОВАНИЕ КОМАНДЫ NET

Большинство задач, соответствующих подкомандам команды NET, проще решить с помощью графических средств администрирования и инструментов панели управления, тем не менее, эти подкоманды удобны для быстрого выполнения

некоторых действий или для оперативного получения информации, особенно во время сеансов Telnet с удаленными системами.

NET SEND отправляет сообщения пользователям, зарегистрированным в указанной системе.

NET START запускает службу в системе.

NET STOP останавливает службу в системе.

NET TIME отображает текущее системное время или синхронизирует системное время с другим компьютером.

NET USE подключает и отключает от общего ресурса.

NET VIEW выводит список доступных сетевых ресурсов.

СОЗДАНИЕ СОЕДИНЕНИЯ УДАЛЕННОГО РАБОЧЕГО СТОЛА

Как администратор вы можете создавать соединения удаленного рабочего стола с серверами и рабочими станциями Windows. В Windows 2003 Server для этого необходимо установить службы терминалов (Terminal Services) и настроить их на использование в режиме удаленного доступа. В Windows XP соединения удаленного рабочего стола разрешены по умолчанию, и все администраторы автоматически имеют право доступа. В Windows Server 2003 удаленный рабочий стол устанавливается автоматически, но по умолчанию отключен, и вам вручную следует разрешить эту функцию.

Один из способов создать соединение удаленного рабочего стола с сервером или с рабочей станцией.

1. Щелкните Пуск, затем Программы или Все программы (All Programs), затем Стандартные (Accessories), затем Связь (Communications), затем Подключение к удаленному рабочему столу (Remote Desktop Connection). Откроется одноименное диалоговое окно.

2. В поле Компьютер (Computer) введите имя компьютера, с которым хотите установить соединение. Если вы не знаете имени, воспользуйтесь предлагаемым раскрывающимся списком или укажите в списке вариант Поиск других (Browse For More), чтобы открыть список доменов и компьютеров в этих доменах.

3. По умолчанию Windows Server 2003 берет для регистрации на удаленном компьютере текущее имя пользователя, домен и пароль. Если нужна информация другой учетной записи, щелкните

Параметры (Options) и зашагайте поля. Имя пользователя (User Name), Пароль (Password) и Домен (Domain).

4. Щелкните подключиться (Connect). При необходимости «введите пароль и щелкните О К. Если соединение создано успешно, вы увидите окно удаленного рабочего стола выбранного компьютера и получите возможность работать с ресурсами этого компьютера. Если соединение создать не удалось, проверьте введенную вами информацию и повторите попытку. С командой Подключение к удаленному рабочему столу (Remote Desktop Connection) работать просто, но она неудобна, если вам приходится создавать удаленные соединения с компьютерами достаточно часто. Вместо нее рекомендуется обращаться к консоли Удаленные рабочие столы (Remote Desktops). В ней можно настраивать соединения с несколькими системами и затем легко переключаться с одного соединения на другое.

СЛУЖБА DNS

Служба доменных имен, Domain Name System, DNS, является одним из важнейших компонентов сетевой инфраструктуры Windows Server 2003. Служба доменных имен осуществляет разрешение, или преобразование, символьных имен в IP-адреса. Клиенты доменов на базе Active Directory используют службу DNS для обнаружения контроллеров домена.

Доменная структура каталога отображается на пространство имен DNS. Поэтому процесс проектирования доменной структуры каталога должен происходить одновременно с формированием пространства имен DNS. Ошибки, допущенные при проектировании пространства имен DNS, могут стать причиной недостаточной производительности сети и, возможно, даже привести к ее отказу.

Служба dns в windows 2000 server и windows server 2003 обладает общими функциональными возможностями, перечисленными ниже.

- DNS-сервер, полностью соответствующий стандартам RFC. Служба DNS базируется на открытых протоколах и полностью соответствует промышленным стандартам (RFC).

- Способность взаимодействия с другими реализациями DNS-серверов. Поскольку служба DNS построена на основе существующих стандартов, она успешно взаимодействует

совместно с большинством других реализаций DNS, например, использующих программное обеспечение Berkeley Internet Name Domain (BIND).

- Поддержка Active Directory. Как уже упоминалось ранее, служба DNS является обязательным условием развертывания Active Directory. Служба DNS используется как основной механизм обнаружения ресурсов в Active Directory-доменах. В свою очередь, DNS-серверы могут использовать каталог Active Directory для размещения баз данных зон. При этом процесс репликации зон осуществляется непосредственно средствами Active Directory.

- Интеграция с другими сетевыми службами Microsoft. Служба DNS обеспечивает интеграцию с другими службами Windows и содержит функции, не описанные в RFC. Это касается интеграции со службами WINS и DHCP.

- Улучшенные административные инструменты. Для управления DNS-серверами администратор может использовать специальную оснастку с улучшенным графическим интерфейсом. Кроме того, в составе операционной системы имеется целый ряд мастеров конфигурации, позволяющих выполнять повседневные задачи по администрированию сервера. Также имеется ряд дополнительных утилит, помогающих управлять и поддерживать серверы DNS и клиентов в сети.

- Поддержка протокола динамического обновления в соответствии с RFC. Служба DNS позволяет клиентам динамически обновлять ресурсные записи при помощи динамического протокола обновления DNS (стандарт RFC 2136). Это облегчает администрирование DNS, избавляя от необходимости вносить эти записи вручную. Компьютеры под управлением Windows 2000, Windows XP и Windows Server 2003 могут динамически регистрировать свои доменные имена.

- Поддержка инкрементных передач зоны между серверами. Передача зоны осуществляется между DNS-серверами в качестве средства синхронизации отдельных экземпляров базы данных зоны. Стандартная процедура передачи зоны предполагает копирование всей базы данных зоны с одного сервера на другой. Инкрементная передача зоны позволяет копировать только сведения об изменениях.

- Поддержка новых типов ресурсных записей. Служба DNS обеспечивает поддержку нескольких новых типов ресурсных

записей (RR): записи SRV (расположение службы) и АТМА (адрес АТМ), что значительно расширяет возможности использования DNS в глобальных сетях.

ВОЗМОЖНОСТИ DNS-КЛИЕНТОВ

В составе Windows Server 2003 имеется служба DNS-клиента. DNS-клиент осуществляет взаимодействие с DNS-сервером с целью разрешения доменных имен в IP-адреса. При этом реализация DNS-клиента в Windows Server 2003 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 не отвечающих 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. Не отвечающие серверы временно удаляются из списка.

СТРУКТУРА DNS

Для правильного формирования пространства имен DNS администратор должен ясно понимать структуру службы DNS, ее основные компоненты и механизмы.

Используемая терминология.

Службой DNS называется служба, выполняющая преобразование символических доменных имен в IP-адреса в ответ на запросы клиентов. Компьютер, на котором функционирует экземпляр службы DNS, называется DNS-сервером. Компьютер,

обращающийся к DNS-серверу с запросом на разрешение имени, называется DNS-клиентом. Клиент DNS функционирует на уровне прикладного программного интерфейса (API), осуществляя разрешение доменных имен прозрачно для пользователей и приложений. Основная задача DNS-клиента заключается в передаче запроса на разрешение доменного имени DNS-серверу. В ответ на свой запрос клиент должен получить либо IP-адрес, либо сообщение о невозможности разрешить предоставленное серверу доменное имя. Клиент DNS передает полученный IP-адрес приложению, инициировавшему процесс разрешения имени.

Рассмотрим более подробно структуру службы DNS. Четкое понимание назначения всех ее компонентов и возможностей позволит администратору выполнить грамотное развертывание этой службы в корпоративной сети.

ПРОСТРАНСТВО ИМЕН DNS

Основным компонентом пространства имен DNS являются домены (domain). Домен рассматривается как группа сетевых хостов, объединенных по некоторому логическому признаку. Домены соединяются друг с другом при помощи отношений "родитель-потомок", образуя тем самым некоторую иерархию. Положение домена в этой иерархии определяет уровень домена.

В основании иерархического пространства имен DNS лежит домен, который называется корневым доменом (root domain) (рис. 1). Корневой домен является формальным элементом, символизирующим иерархичность пространства доменных имен, выступая в качестве родительского контейнера для всех доменов первого уровня.

Если домены выступают в роли контейнеров или узлов рассматриваемой иерархической структуры, то в качестве листьев выступают сведения о ресурсах этих доменов. Служба DNS определена в рамках стека протоколов TCP/IP, в котором для обозначения любого объекта сети используется понятие хост (host).

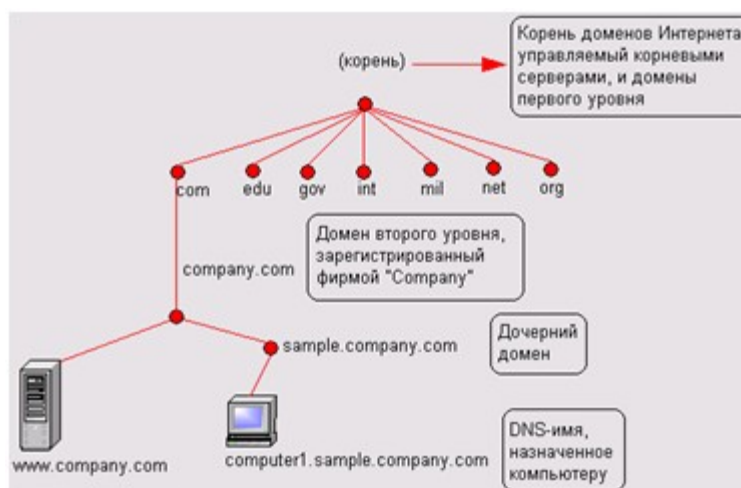


Рис. 1. Пространство имен DNS

Любой объект пространства имен DNS, будь это домен или хост, имеет имя, уникальное в пределах родительского контейнера. Это имя может быть образовано из символов латинского алфавита, цифр и знака тире ("—"). Некоторые версии DNS (включая реализацию DNS в Windows Server 2003) допускают использование в именах объектов символа подчеркивания ("_"), а также символов в формате UTF-8.

Единственным объектом пространства имен DNS, не имеющим имени, является корневой домен. Для ссылки на него используют точку ("."). В записи полного доменного имени завершающая точка, обозначающая корневой домен, обычно опускается.

| Элемент пространства имен | Описание | Пример |
|---|---|--|
| Корневой домен | Корень — самый высокий уровень доменной иерархии; домен без имени. При использовании в полном доменном имени указывается точкой в конце | Точка (.) или точка, стоящая в конце имени, например, "sample.mydomain.org." |
| Домен первого уровня (Top-Level Domain, TLD) | Имя, состоящее из двух или трех символов, обычно указывающее страну (Россия — ru, Нидерланды — nl, Украина — ua и т. п.) или тип организации, использующей имя (com — коммерческая, mil — военная и т. д.) | Суффикс ".com" означает, что имя зарегистрировано фирмой или другой организацией для коммерческого использования в Интернете |
| Домен второго уровня (Second-Level Domain, SLD) | Имя произвольной (ограниченной) длины, зарегистрированное частным лицом или организацией для использования в Интернете. Такие имена всегда основаны на домене верхнего уровня, в зависимости от типа организации или географического местоположения | "mydomain.org." или просто "mydomain.org" — имя домена второго уровня (вымышленное) |
| Дочерние домены | Дополнительные домены, которые организация может создавать в пределах домена второго уровня. Применяются для отражения структурной иерархии различных подразделений больших организаций | "sample.mydomain.org." — дочерний домен домена второго уровня "mydomain.org." |
| Имя хоста или ресурса | Листья дерева имен DNS, задают определенный ресурс или хост | "host.sample.mydomain.org.", где host — имя хоста или какого-либо ресурса в сети |

Таблица 1. Элементы пространства имен DNS

ЗОНЫ

Деление доменного пространства имен между DNS-серверами осуществляется посредством механизма зон (zone). Зона представляет собой базу данных, в которой содержатся записи о соответствии некоторого множества доменных имен IP-адресам. Каждая зона представляет собой фрагмент доменного пространства имен. Следует рассматривать зоны как основной административный элемент, на уровне которого происходит как управление пространством имен в целом, так и управление процессом разрешения имен. Зоны, используемые для размещения содержимого обратных доменов, называются зонами обратного просмотра (reverse lookup zone).

Границы зоны не определяются доменной структурой. Одна зона может включать в себя несколько доменов, в то время как объекты, принадлежащие к одному домену, могут быть размещены в

нескольких зонах. Осуществляя разделение доменного пространства имен на зоны, необходимо исходить, в первую очередь, из удобства администрирования.

Зону можно разместить на нескольких серверах. На каждом из вовлеченных DNS-серверов размещается отдельная копия зоны. Для поддержания этих копий в согласованном состоянии используется модель репликации с одним основным участником (single-master replication). Один из DNS-серверов выступает в качестве основного носителя зоны (primary zone). Только основной носитель зоны обладает возможностью вносить изменения в ее содержимое (другими словами, имеет право на запись).

Остальные DNS-серверы располагают копией зоны, доступной только для чтения. Эти серверы называются дополнительными носителями зоны (secondary zone). Изменения, произведенные в копии зоны основным носителем, реплицируются на дополнительные носители. Использование нескольких носителей зоны позволяет, с одной стороны, распределить нагрузку между несколькими серверами, а с другой стороны, реализовать некоторый уровень отказоустойчивости. В случае выхода из строя одного из носителей зоны разрешение имен будет осуществляться остальными носителями зоны.

На каждом DNS-сервере может быть размещено несколько зон. В этом случае каждая зона конфигурируется отдельно. Один и тот же сервер может выступать как основным, так и дополнительным носителем для различных зон.

РЕСУРСНЫЕ ЗАПИСИ

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

owner TTL class type RDATA

Характеристика полей ресурсной записи приводится в табл. 2.

| Имя поля | Описание |
|----------|---|
| 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, до тех пор пока не будет удалена. Данное поле является необязательным. Если поле не определено, используется значение, определенное на уровне зоны (в записи SOA) |
| class | Определяет класс ресурсной записи. В настоящее время в данном поле всегда указывается IN |
| type | Указывает тип ресурсной записи. Существующие типы будут перечислены далее |
| RDATA | Данные ресурсной записи. Конкретное значение данного поля определяется типом ресурсной записи |

Таблица 2. Поля ресурсной записи

УПРОЩЕННЫЕ ЗОНЫ

Упрощенная зона (stub zone) представляет собой копию зоны, содержащую только те ресурсные записи, которые необходимы для локализации DNS-серверов, являющихся носителями полной версии зоны. Основное назначение упрощенной зоны — идентификация DNS-серверов, которые способны выполнить разрешение доменных имен, принадлежащих к этой зоне.

Любая упрощенная зона состоит из следующих элементов:

- записи типа SOA, определяющей параметры зоны;
- записей типа NS, указывающих доменные имена DNS-серверов, выступающих носителями полной версии зоны;
- записей типа A, определяющих адреса DNS-серверов.

Упрощенные зоны позволяют облегчить и сократить процесс разрешения доменного имени. Рассмотрим пример. Допустим, на DNS-сервере, обслуживающем домен ayan.ru, содержится упрощенная зона для домена khsu.ru. В этом случае при поступлении запроса на разрешение имени www.usoz.ru DNS-сервер не будет использовать рекурсивный запрос на разрешение этого имени.

Вместо этого запрос будет напрямую отправлен некоторому серверу имен домена usoz.ru, адрес которого будет извлечен из упрощенной зоны. Разрешение имени посредством рекурсивных запросов потребовало бы больше шагов, чем в случае использования упрощенной зоны. Следует обратить внимание на то, что в процесс разрешения доменного имени не вовлекаются корневые серверы DNS. Это имеет одно очень важное и полезное следствие.

Упрощенные зоны можно использовать для организации взаимодействия двух лесов доменов, реализующих собственные пространства имен DNS. В этом сценарии в каждом из лесов имеются собственные корневые серверы. Посредством упрощенных зон администратор может создавать ссылки на домены, расположенные в другом пространстве имен DNS.

С упрощенными зонами связано одно ограничение. Упрощенная зона не может располагаться на DNS-сервере, который одновременно выступает в качестве носителя полной версии зоны.

Поддержание упрощенной зоны в актуальном состоянии осуществляется тем же методом что и для обычной зоны. Периодически один из носителей зоны выполняет обновление упрощенной зоны, передавая DNS-серверу, на котором она размещается, требуемое подмножество ресурсных записей. Конфигурация процесса передачи упрощенной зоны определяется параметрами записи SOA этой зоны.

ДИНАМИЧЕСКАЯ РЕГИСТРАЦИЯ ИМЕН

Стандартный механизм сопровождения зоны предполагает создание администратором вручную статических ресурсных записей. Любое произведенное изменение доменного имени хоста или его IP-адреса администратор должен синхронизировать с базой данных службы DNS, вручную изменяя соответствующие записи. Подобная схема изменения содержимого зоны делает практически невозможным использование в корпоративной сети службы динамического выделения адресов (DHCP).

В спецификации службы DNS определена возможность использования механизма динамической регистрации хостами своих доменных имен. В процессе динамической регистрации клиенты могут создавать и изменять ресурсные записи типа A и PTR. Контроллеры домена могут также динамически регистрировать ресурсные записи типа SRV.

Механизм динамической регистрации доменных имен предполагает тесную интеграцию служб DNS и DHCP. Динамическая регистрация доменных имен может быть осуществлена либо DHCP-клиентом, либо службой сервера DHCP. Такое решение легко объяснимо, учитывая, что в большинстве случаев изменение IP-адреса клиента связано со службой DHCP.

Если клиент находится под управлением операционных систем Windows 2000/XP или Windows Server 2003, он может самостоятельно зарегистрировать свое имя в базе данных DNS-сервера. В этом случае регистрация осуществляется службой клиента DHCP компьютера. Остальные версии Windows (Windows 9.X/NT/ME) не способны динамически зарегистрировать свое доменное имя. В этой ситуации задача регистрации имени может быть возложена на службу сервера DHCP. Служба сервера DHCP, реализованная в Windows Server 2003, может зарегистрировать доменное имя одновременно с выделением в аренду IP-адреса. В этом случае, регистрация доменного имени происходит без участия клиента и незаметно для них.

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

- происходит изменение IP-адреса. Операция динамической регистрации инициируется при любом изменении списка адресов хоста (добавление нового адреса, удаление или модификация существующего);

- выполнение утилиты командной строки Ipconfig с ключом /renew. В этом случае инициируется процесс выделения хосту в аренду нового IP-адреса (или набора адресов, если компьютер имеет несколько сетевых адаптеров);

- в процессе загрузки системы. Каждый раз при включении компьютера и загрузки системы происходит регистрация доменного имени в базе данных соответствующей зоны;

- выполнение утилиты командной строки Ipconfig с ключом /registerdns. В результате происходит принудительное обновление доменного имени клиента в базе данных DNS-сервера.

Механизм динамической регистрации подразумевает не только регистрацию доменных имен, но и их освобождение. При завершении работы системы ассоциированные с ней ресурсные записи автоматически удаляются из зоны. Если работа системы была завершена некорректно, например, в результате сбоя или зависания компьютера, ресурсные записи могут оставаться в базе данных. Подобные записи называются фантомами. Наличие фантомов в базе данных зоны нежелательно, поскольку клиенты получают в ответ на свои запросы неактуальную информацию.

Параллельно с механизмом динамической регистрацией имен DNS-сервер активизирует механизм очистки (scavenging) базы данных от устаревших ресурсных записей.

РАЗВЕРТЫВАНИЕ DNS

В данном разделе мы кратко рассмотрим процесс установки и настройки DNS-серверов в корпоративной сети. Этот процесс включает в себя следующие стадии:

- планирование;
- установка программного обеспечения DNS-сервера;
- настройка DNS;
- мониторинг и оптимизация.

Планирование

Перед использованием DNS в сети необходимо тщательно спланировать пространство имен DNS. При этом нужно определить, как будет применяться служба DNS и какие цели должны быть достигнуты в ходе ее развертывания. Вот вопросы, которые необходимо решить до установки службы.

- Выбор и предварительная регистрация имени домена, используемого в Интернете.
- В какой сети будут установлены серверы DNS — в частной сети или в Интернете.
- Нужно ли использовать DNS для поддержки работы Active Directory?
- Требования к выбору доменных имен для компьютеров.

Управление клиентами

Для клиентов Windows конфигурация DNS при настройке свойств TCP/IP для каждого компьютера включает следующие задачи:

- установка имени хоста DNS для каждого компьютера или сетевого подключения;
- установка имени родительского домена, которое помещается после имени хоста, чтобы формировать полное (fully qualified) имя домена для каждого клиента;
- установка основного DNS-сервера и списка дополнительных DNS-серверов, которые будут использоваться клиентом в ситуации, когда основной сервер недоступен;

- установка очередности списка поиска доменов, используемого в запросах для дополнения не полностью заданного имени компьютера.

Мониторинг и оптимизация

В Windows Server 2003 администратор может осуществлять мониторинг DNS-сервера и по его результатам оптимизировать соответствующие параметры настройки. Для этой задачи администратор может использовать следующие инструменты и возможности:

- системный монитор (Performance Monitor);
- опции протоколирования;
- статистика по DNS-серверу;
- настройка дополнительных параметров.

ФАЙЛ HOSTS

Файл HOSTS используется в Windows для преобразования символьных имен доменов (google.com) в соответствующие им IP-адреса (64.233.167.99) и наоборот (точно такие же задачи в сетях TCP/IP выполняет и DNS - Domain Name System - система доменных имен). То есть каждый раз, когда вы вводите в адресную строку браузера название сайта, ваш компьютер, прежде чем с ним соединится, должен преобразовать это "буквенное" название в соответствующие ему числа.

Файл HOSTS не имеет видимого расширения, но, по сути, его можно редактировать в любом текстовом редакторе (например, Notepad ([Ссылки могут видеть только зарегистрированные и активированные пользователи]) или Блокнот), как обычный файл текстового формата.

LMHOSTS (LAN Manager hosts) отвечает за отображение (преобразование) имен NetBIOS в IP адреса.

ЗАКЛЮЧЕНИЕ

Компания Microsoft впервые включила сервер DHCP в поставку серверной версии Windows NT 3.5, выпущенной в 1994 году. Начиная с Windows 2000 Server реализация DHCP-сервера от Microsoft позволяет динамически обновлять записи DNS, что используется в Active Directory.

Internet Systems Consortium выпустил первую версию ISC DHCP Server (для Unix-подобных систем) 6 декабря 1997 года. 22 июня 1999 года вышла версия 2.0, более точно соответствующая стандарту.

Компания Cisco включила сервер DHCP в Cisco IOS 12.0 в феврале 1999 года. Sun добавила DHCP-сервер в Solaris 8 в июле 2001 года.

В настоящее время существуют реализации сервера DHCP для ОС Windows в виде отдельных программ, в том числе открытых, позволяющих выполнять роль сервера DHCP компьютерам под управлением не серверных версий данной ОС.

ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА

1. <https://ru.wikipedia.org>
2. <https://teacherbox.ru>
3. <https://seti.ucoz.ru/>