Разрешение имен с помощью DNS

Лаштанов И.Г.

Введение в DNS

DNS — это распределенная база данных в сетях TCP/IP для преобразования имен компьютеров (имен узлов) в IP-адреса.

Систему доменных имен DNS (Domain Name System) разработал Пол Мокапетрис (Paul Mokapetris), который на заре интернета (в начале 1980-х) задался вопросом, как работать в системе (она стала со временем называться DNS), которая преобразует Web-адрес в состоящий из четырех октетов IP-адрес, который используется сетевыми машинами для связи через TCP/IP. Мокапетрис разработал иерархическое пространство имен, которое позволяло присваивать машинам понятные (дружественные) пользователям имена и связывать эти имена с IP-адресами. Эти группы машин разбивались на домены, и в каждом домене предусматривалось свое собственное управление.

Введение в DNS

DNS можно также использовать для поиска элементов, хранящихся в базе данных LDAP. DNS - это клиент/серверный процесс, который читает текстовый (плоский) файл, аналогичный файлам HOSTS, которые вы можете иногда видеть и в настоящее время. В Windows DNS начали применять еще в версии NT4, и служба

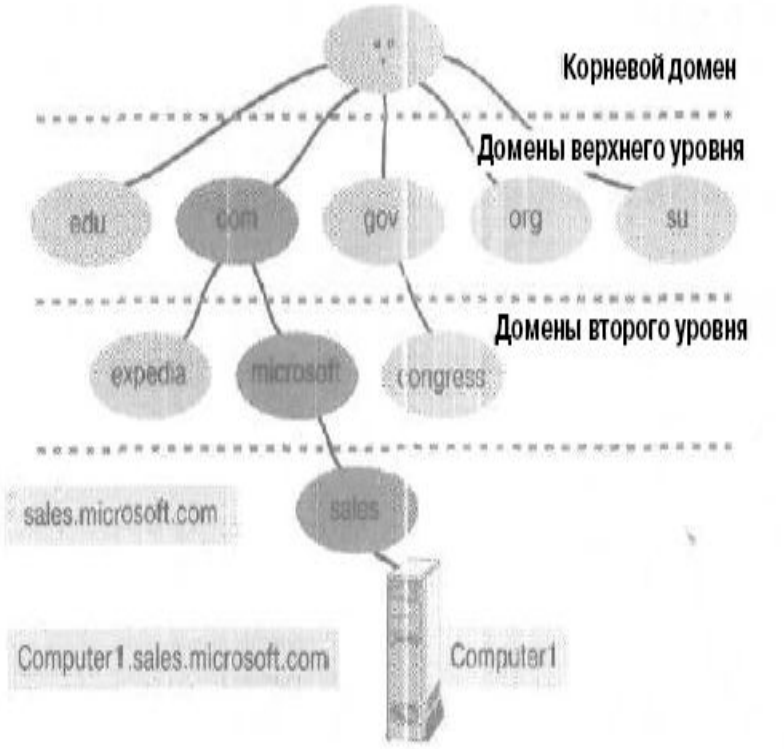
DNS стала составной частью операционной системы в Windows 2000. Это в основном произошло потому, что Microsoft перешла в используемом по умолчанию методе разрешения имен от имен NetBIOS и службы WINS (Windows Internet Naming Service) к полностью уточненным доменным именам FQDN (Fully Qualified Domain Names) и службе DNS. С появлением Active Directory (AD) и DNS, согласующейся с документом RFC 2136 (динамическое обновление записей) все изменилось еще больше. Еще больше вещей изменилось (и еще больше изменится) с появлением предложений по таблице для расширений DNSSEC (RFC 2541). DNS по-прежнему является службой с серверной и клиентской (resolver) частями. Взаимодействие между DNS и Active Directory является взаимозависимым, то есть предлагается одна система вместо двух.

Пространство имен домена

Пространство имен домена - это схема именования, обеспечивающая иерархичную структуру БД DNS. Каждый узел представляет раздел БД DNS и называется доменом.

БД DNS индексируется по имени, т. е. у каждого домена должно быть имя. При добавлении доменов в иерархичную структуру имя родительского домена добавляется к именам его дочерних доменов (поддоменов). Следовательно, имя домена определяет его положение в иерархии. Например, имя sales.microsoft.com указывает, что домен sales состоит в домене microsoft, а домен microsoft является поддоменом домена com.

Структура пространства имен домена включает корневой домен, домены верхнего и второго уровней и имена узлов.



Правила именования доменов

При создании пространства имен домена помните следующее:
• Ограничивайте число уровней домена. Обычно записи узлов должны стоять на 3 или 4, но не более, чем на 5 уровней ниже по иерархии DNS. При увеличении числа уровней увеличивается объем задач администрирования.
• Используйте уникальные имена. Чтобы в пространстве имен DNS были лишь уникальные имена, в домене не должно быть поддоменов с идентичными именами.
• Используйте простые уникальные имена. Простые и точные имена доменов легче запоминаются и делают возможным интуитивный поиск \\еЬ-узлов и других компьютеров в Интернете и интрасети.
• Избегайте длинных имен. Доменное имя может включать до 63 символов с учетом точек. Общая длина полного доменного имени не может превышать 255 символов.
В именах не учитывается регистр.
• Используйте стандартные символы DNS и Unicode:
• Windows 2000 поддерживает стандартные символы DNS, определенные в RFC 1035: **A-Z,** a-z, 0-9 и дефис (-);
• служба **DNS** поддерживает набор символов Unicode, включающий дополнительные символы, не заложенные в набор символов ASCII, но нужные таким языкам, как французский, немецкий и испанский.

Зоны

Зона — это отдельная часть пространства имен домена. Зоны позволяют делить пространство имен домена на управляемые секции.

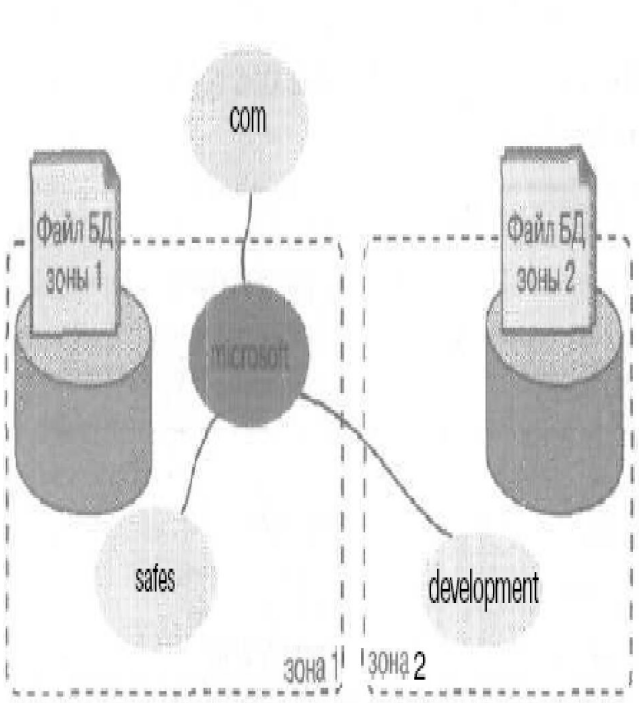
Для распространения административных задач по группам пространство имен домена делится на несколько зон. Например, пространство имен домена microsofi.com разделено на две зоны. Благодаря этому один администратор может управлять доменами microsoft и sales, а другой — доменом development.

Зона должна охватывать непрерывное пространство имен домена. Например, можно создать зону, охватывающую sales.microsoft.com и родительский домен microsoft.com, поскольку эти зоны связаны (рис. 9-11). Однако создать зону, содержащую только домены sales.microsoft.com и development.microsoft.com, нельзя, поскольку эти домены не связаны.

Используемые в зоне привязки «IP-адрес/имя> хранятся в файле БД зоны. Каждая зона

прикреплена к определенному домену — корневому домену зоны. Файл БД зоны может

содержать сведения не обо всех поддоменах корневого домена зоны.



Серверы имен DNS

Хранят файлы БД зон. На сервере могут размещаться БД нескольких зон. Сервер имен обладает полномочиями в пространстве имен, охватываемом зоной.

В зоне должен иметься хотя бы один сервер имен, но их может быть и несколько. Один из них содержит мастер-файл БД этой зоны, или первичный файл БД зоны. Изменения в конфигурации зоны, например добавление доменов или хостов, обрабатываются на сервере, содержащем первичный файл БД зоны. Все остальные серверы имен, связанные с данной зоной, являются резервными и содержат вторичные файлы БД.

Преимущества нескольких серверов DNS

Передача зоны — дополнительные серверы имен получают от сервера, содержащего первичный файл БД зоны, копию этого файла. Это называется передачей зоны. Резервные серверы периодически обращаются к серверу, содержащему первичный файл БД, за обновленными сведениями о конфигурации зоны.

Избыточность — при сбое сервера, содержащего первичный файл БД зоны, в работу включаются резервные серверы.

Повышение скорости доступа удаленных клиентов — при наличии удаленных клиентов дополнительные серверы имен позволят снизить трафик запросов в низкоскоростных каналах связи с ГВС.

Снижение нагрузки — дополнительные серверы имен уменьшают нагрузку на сервер, содержащий первичный файл БД зоны, Кроме того, благодаря Б'Д Active Directory Windows 2000 поддерживает хранилище зоны, интегрированное с каталогом. Зоны, хранимые подобным образом, содержатся в дереве Active Directory в объекте-контейнере Domain. Каждая зона, интегрированная с каталогом, хранится в объекте-контейнере зоны DNS, которому присваивается имя зоны.

Установка службы DNS

Для внедрения DNS надо настроить сервер и установить службу DNS. Сервер DNS должен обладать статичным IP-адресом. Параметры TCP/IP следует сконфигурировать так, чтобы настройки DNS указывали обратно на сервер. Установить службу DNS можно в любое время после или в процессе установки Windows 2000 Server.

Процесс установки DNS:

- устанавливает оснастку DNS и добавляет в меню Administrative Tools (Администрирование) соответствующий ярлык; оснастка DNS служит для управления локальными и удаленными серверами имен DNS;
- добавляет в реестр раздел, используемый службой DNS, — HKEY_ LQCAL_ MACHTNE\System\CurrentControlSet\Services\DNS;
- создает папку %systemroot%\System32\DNS, содержащую файлы БД DNS.

Обычно редактировать файлы БД DNS не надо, хотя их можно использовать при устранении неполадок DNS. Служба DNS представляет Вам набор файлов-примеров; при установке службы DNS они копируются в папку %systemroot%\System32\DNS\Samples.

Конфигурирование службы DNS

Оснастка DNS

Оснастка DNS служит для настройки зон прямого и обратного поиска, добавления в файл БД зоны записей о ресурсах, конфигурирования службы DNS для использования *динамической системы доменных имен* (Dynamic DNS, DDNS), позволяющей другим серверам и службам автоматически обновлять файлы Вашей зоны.

Оснастку DNS можно запустить из консоли управления (MMC) или из узла Services And Applications (Службы и приложения) дерева оснастки Computer Management (Управление компьютером), Для установки оснастки DNS можно выполнить файл Adminpak.msi или установить службу DNS. При отсутствии службы DNS оснастка используется для управления удаленными серверами, на которых установлена служба DNS.

Создание зон прямого просмотра

Зона прямого просмотра позволяет генерировать прямые запросы поиска имени. Для работы службы DNS на сервере имен надо сконфигурировать не менее одной зоны прямого просмотра.

Чтобы создать новую зону прямого просмотра, щелкните папку Forward Lookup Zone (Зона прямого просмотра) и в меню Action (Действие) выберите команду New Zone (Создать новую зону). Создать зону Вам поможет мастер.

Тип зоны

- Интегрированная в Active Directory
- Основная
- Дополнительная

Имя зоны

Обычно зоне присваивается имя наивысшего домена в иерархии, охватываемой зоной, т. е. имя корневого домена зоны. Например, зоне, включающей домены microson.com и sales.microsoft.com, будет присвоено имя microsoft.com.

Файл зоны

Это имя файла БД, по умолчанию состоящее из имени зоны с расширением .dns. Например, если имя зоны — microsoft.com, файл БД по умолчанию будет называться microsoft.com.dns.

Создание зон обратного просмотра

Зоны обратного просмотра позволяют генерировать обратные запросы на поиск имени. Эти зоны не обязательны, однако они нужны для работы утилит устранения неполадок, например nslookup, и для фиксирования в файлах журнала служб IIS имени узла вместо его IP-адреса. Чтобы создать новую зону обратного просмотра, щелкните папку Reverse Lookup Zone (Зона обратного просмотра) и в меню Action (Действие) — команду New Zone (Создать новую зону).

Тип зоны

Соответствуют типам зон прямого просмотра: интегрированная в Active Directory, основная и дополнительная.

Зона обратного просмотра

Укажите идентификатор Вашей сети (network ID) или имя зоны обратного просмотра. Если в идентификаторе сети указан 0, он появится в имени зоны.

Файл зоны

Имя файла зоны по умолчанию определяется идентификатором сети и маской подсети. DNS обращает порядок октетов IP-адреса и добавляет суффикс in-addr.arpa. Например, имя файла зоны обратного просмотра для сети 169.254 будет 254.169.in-addr.arpa.dns. При передаче зоны с другого сервера можно импортировать существующий файл зоны. Перед созданием новой зоны этот файл надо поместить в папку целевого компьютера %systemroot%\System32\DNS.

Добавление записей о ресурсах

Создав зоны, можно добавлять записи о ресурсах при помощи оснастки DNS. Записи о ресурсах — это записи файла БД зоны. Каждая запись идентифицирует в БД конкретный ресурс. Чтобы добавить запись о ресурсе, щелкните требуемую зону и в меню Action (Действие) — команду Other New Record (Другие новые записи). В диалоговом окне Resource Record Type (Тип записи ресурса) можно создавать записи о любых ресурсах, перечисленных в списке Select A Resource Record Type (Выбор типа записи ресурса).

Существует множество типов записей ресурса. При создании зоны DNS автоматически добавляет две: Start of Authority (SOA) и Name \Server (NS). SOA определяет сервер имен, являющийся в этом домене полномочным источником данных. Первой записью файла БД зоны должна быть SOA. NS представляет собой список серверов имен, выделенных конкретному домену. Сконфигурировать записи этих двух типов можно в диалоговом окне свойств требуемой зоны прямого просмотра.

С другими типами записей ресурса, включая описание каждого типа, можно познакомиться в списке Select A Resource Record Type (Выбор типа записи ресурса) — при выборе типа внизу окна отображается его описание.

Настройка Dynamic DNS

Служба DNS включает возможность динамического обновления — Dynamic DNS (DDNS). При использовании DNS после изменений в конфигурации домена, в отношении которого сервер имен обладает полномочиями, надо вручную обновить файл БД зоны на первичном сервере имен. При использовании DDNS серверы имен и клиенты сети автоматически обновляют файлы БД зоны.

Можно определить список авторизованных серверов, которые будут выполнять динамическое обновление. Список может включать дополнительные серверы имен, контроллеры домена и другие серверы, выполняющие регистрацию клиентов в сети, например серверы WINS или DHCP.

Запись A, или *запись ресурса адреса узла,* содержит привязку ≠1P-адрес/имя≠; PTR-запись, или *запись ресурса указателя,* содержит привязку ≠IP-ад рес/имя≠ для компьютера, отсылающего подтверждение регистрации, Службой, фактически генерирующей динамические обновления DNS, является клиент DHCP. Клиентская служба DHCP выполняется на каждом компьютере с Windows 2000 независимо от того, настроен ли он как клиент DHCP.

DDNS и DHCP

DDNS взаимодействует со службой DHCP для поддержки синхронизированных привязок «IP-адрес/имя», соответствующих сетевым узлам. По умолчанию служба DHCP позволяет клиентам добавлять в зону свои записи A, сама же служба DHCP добавляет в зону запись PTR. По истечении срока аренды IP-адреса служба DHCP удаляет из зоны обе эти записи.

Настроить зону для поддержки DDNS позволяет оснастка DNS. Щелкните требуемую зону и в меню Action (Действие) — команду Properties (Свойства). На вкладке General (Общие) диалогового окна свойств выберите в списке Allow Dynamic Updates (Динамическое обновление) пункт Yes (Да).

Чтобы настроить сервер для отсылки динамических обновлений, вызовите оснастку DHCP и определите для сервера DHCP соответствующие серверы DNS.

Настройка клиента DNS

Установив и настроив службу DNS на компьютерах с Windows 2000 Server, можно приступить к настройке клиентов DNS. Сначала убедитесь, что на клиенте установлен пакет протоколов **TCP/IP.** Установив TCP/IP на клиентах, откройте диалоговое окно его свойств, позволяющее настроить систему для автоматического получения адреса DNS (это обеспечивает сервер DHCP) или вручную указать IP-адреса предпочтительного и дополнительного серверов DNS. Для настройки дополнительных параметров DNS щелкните кнопку Advanced (Дополнительно). Чтобы задать параметры DNS, в диалоговом окне Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) перейдите на вкладку DNS. Вам потребуется указать IP-адреса одного или несколько серверов DNS. Они необходимы для работы службы DNS. Здесь можно сконфигурировать и параметры, обеспечивающие разрешение имен узлов, для которых не было указано полное доменное

имя, и настроить параметры регистрации **DDNS.**

Устранение неполадок DNS

Мониторинг сервера DNS

Оснастка DNS позволяет осуществлять мониторинг службы DNS. Выберите сервер имен и в меню Action (Действие) щелкните команду Properties (Свойства). В диалоговом окне свойств перейдите на вкладку Monitoring (Наблюдение), Для проверки работы сервера имен можно выполнить запросы двух типов:

- **Simple query (Простой запрос)** — этот локальный тест использует локальный клиент DNS

для создания запроса к серверу имен;

- **Recursive query (Рекурсивный** запрос) — пересылает рекурсивный запрос другому серверу имен.

Установка параметров ведения журнала

Оснастка DNS позволяет настроить дополнительные параметры ведения журнала. Открыв диалоговое окно свойств сервера имен, перейдите на вкладку Logging (Ведение журнала). Здесь доступно 11 параметров: Query (Запрос), Notify (Уведомление), Update (Обновление), Questions (Вопросы), Answers (Ответы), Send (Отправить), Receive (Получить), UDP, TCP, Full Packets (Полных пакетов) и Write Through (Запись с помощью). Информация, соответствующая выбранным параметрам, будет заноситься в файл журнала.