

Система доменных имен. Основные понятия и принципы.

<http://school-collection.edu.ru/catalog/rubr/13899a9b-11fc-4a07-861c-1cf294b8f895/113185/>

DNS (англ. *Domain Name System* — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства). Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Система доменных имен состоит из множества доменных имен, серверов доменных имен, клиентов DNS (Resolver-ы).

У каждого сервера имеется своя зона ответственности, иными словами, каждый DNS сервер хранит таблицы соответствия некоторой группы имен ip-адресам (прямые зоны) и ip-адресов группам имен (обратные зоны).

Корневой сервер хранит адреса серверов верхних уровней TLD-серверов (например, ru, ua, uk, com, net и тд).

Серверы верхних уровней хранят адреса локальных DNS серверов.

Программа Resolver – это часть прикладного программного обеспечения. Ее задачи:

- получить имя от соответствующей программы (например, браузера)
- передать адрес DNS серверу
- получить ip-адрес от сервера
- передать адрес запросившей программе (в нашем примере, браузеру)

Как происходит прямой запрос:

- Resolver посылает имя локальному DNS серверу (например, <http://test.ru>). Если имя находится в зоне ответственности данного DNS сервера, последний находит в своей таблице ip-адрес и возвращает его Resolver-у. Resolver передает ip-адрес вызвавшей его программе. Если запрошенное имя находится вне зоны ответственности данного DNS сервера, сервер производит обращение к корневому серверу. Корневой сервер выдает ip адрес сервера верхнего уровня, ответственного за соответствующие зоны. По полученному адресу отправляется запрос серверу верхнего уровня, который возвращает адрес локального сервера ответственного за запрашиваемое имя. И, наконец, запрашивается имя у локального сервера, который выдает требуемый ip адрес. Адрес передается запросившему Resolver-у

Организация пространства имен DNS

При создании системы доменных имен был заложен иерархический принцип. Принцип иерархической организации основан на том, что узлы сети могут объединяться в логические группы - домены, которые, в свою очередь, могут входить в домены более высокого уровня.

Корень в системе доменных имен называется Root, который является условным, т.к. никем не администрируется.

Администрирование начинается с домена верхнего (первого) уровня. В 80-е годы 20 века были определены:

- gov – правительственные организации
- mil – военные организации
- edu – образовательные организации
- com – коммерческие организации
- net – сетевые организации

Когда интернет перешагнул границы США, появились национальные домены:

- UK – Великобритания
- JP – Япония
- DE – Германия
- RU – Россия (позднее)
- UA – Украина
- LA – Латвия

На втором уровне идут домены либо определяющие регион, либо организацию, либо проект (MSK – Москва, SPB – Санкт-Петербург, EDUSITE – проект «школьный сайт»).

Любая организация или частное лицо может получить свой собственный домен, если он к этому моменту уже не занят.

На следующем уровне имена могут быть закреплены за организациями входящими в регион, в проект или крупную организацию (например, SCH943 – школа №943 входящая в проект «Школьный сайт»)

Записывается доменное имя справа налево по мере убывания иерархии (например, SCH943.EDUSITE.RU – относится к зоне ru, к проекту «Школьный сайт» и принадлежит школе 943.

Порядок взаимодействия DNS-клиента с сервером для обеспечения разрешения имен определяется специальным протоколом DNS. Этот протокол предусматривает свой формат сообщения (пакета) и использует для доставки данных транспортные протоколы UDP и TCP как нижележащие.

Задачи, решаемые сервисом DNS, являются относительно простыми, поэтому DNS-сообщение устроено несложно: оно включает в себя:

- поле заголовка, определяющее тип сообщения (например, "запрос клиента", "ответ сервера" и т.д.);
- поле запроса, в котором клиент указывает разрешаемое имя и параметры запроса;
- поле ответа, в которое сервер помещает результат обработки запроса;
- два служебных поля передачи для управляющей и дополнительной информации.

Дополнительно:

- Любой узел может входить в несколько доменов и, следовательно, иметь несколько разных полностью определенных доменных имен.
- Для функционирования серверу имен не обязательно знать адреса всех остальных DNS-серверов Интернет. Достаточно располагать адресами серверов имен корневого домена.
- Сервер *может* хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
- **Домен** (англ. *domain* — область) — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная *ветвь* или *поддерево* в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости), корневым доменом всей системы является точка ('.'), ниже идут домены первого уровня (географические или тематические), затем — домены второго уровня, третьего и т. д.
- **Поддомен** (англ. *subdomain*) — подчиненный домен. (например, wikipedia.org — поддомен домена org, а ru.wikipedia.org — домена wikipedia.org).
- **Зона** — часть дерева доменных имен (включая **ресурсные записи**), размещаемая как единое целое на некотором сервере доменных имен (**DNS-сервере**), а чаще — одновременно на нескольких серверах.
- **DNS-сервер** — специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.
- **DNS-клиент** — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.
- Рекурсивный сервер получает только один запрос от клиента и самостоятельно производит остальные запросы, чтобы получить IP адрес. Таким образом, клиент остается в неведении об этой процедуре и внутренняя сеть становится чуть менее загруженной. Если DNS сервер не рекурсивный – клиенту приходится самому рекурсивно опрашивать сервера.