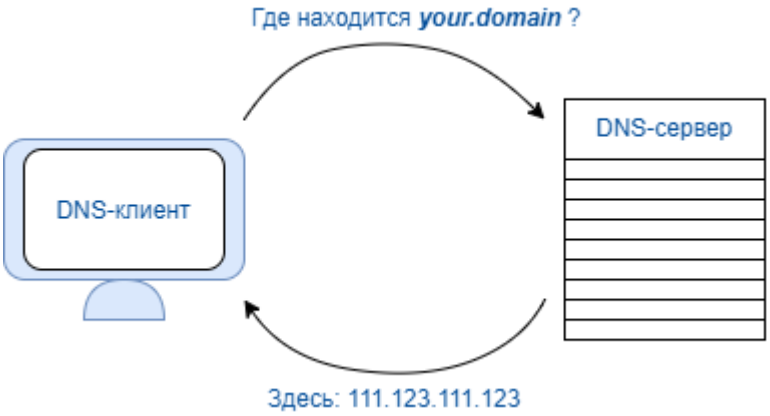
Лабораторная работа 3. Службы DNS. Установка и настройка в ОС Windows.

Теоретический материал.

DNS (Domain Name System - система доменных имен) представляет собой распределенную систему хранения и обработки информации о доменных зонах. Она необходима, в первую очередь, для соотнесения IP-адресов устройств в сети и более адаптированных для человеческого восприятия символьных имен. Предоставление информации об IP-адресах хостов по символьному адресу - не единственная задача DNS. Система работает с разными типами ресурсных записей, позволяющими реализовывать весьма широкий круг задач: переадресация между доменными именами, балансировка нагрузки между хостами, привязка специфических сервисов (напр., эл. почты) к домену.



Система доменных имен является одной из фундаментальных технологий современной интернет-среды, так как информация об IP-адресе запрашиваемого узла - обязательное условие получения ответа на любой интернет-запрос. Но IP-адрес представляет собой числовое значение вида "1.23.45.67", неподходящее для комфортного восприятия человеком. К тому же основной принцип распределения IP-адресов в сети - уникальность. Важно и то, что сетевой адрес - не самый устойчивый параметр. Он может изменяться (напр., при смене хоста, обслуживающего запрашиваемый узел, смене хостинг-провайдера, и т.п.). Все перечисленные особенности делают систему навигации по сетевым адресам сложной для человека.

DNS обеспечивает преобразование запрашиваемого клиентом символьного имени домена в IP-адрес (адреса) обслуживающего эту доменную зону

сервера (серверов). Изначально, до разрастания сети интернет, адреса преобразовывались согласно содержимому файла "hosts", составлявшегося централизованно и автоматически рассылавшегося на каждую из машин в сети. По мере роста глобальной сети такой метод перестал оправдывать себя - появилась потребность в новом механизме, которым и стала DNS, разработанная в 1983 году Полом Мокапетрисом.

Ключевыми характеристиками DNS являются:

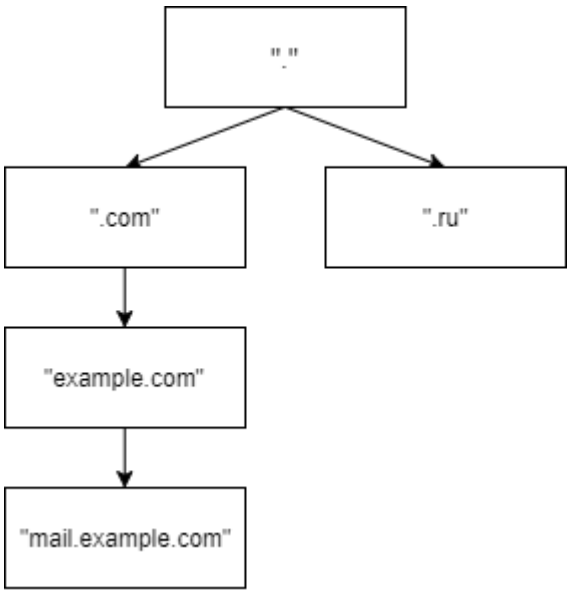
- **Распределенность хранения и управления** - каждый DNS-сервер обязан хранить информацию только по делегированным ему доменам, а ответственность за различные узлы дерева доменных имен несут разные лица
- **Кэширование данных** - DNS-сервер может временно хранить некоторое количество информации о неделегированных ему доменах для уменьшения уровня общей нагрузки
- **Иерархическая структура** - узел, ответственный за доменную зону, может самостоятельно делегировать нижестоящие узлы другим DNS-серверам
- **Резервирование** - хранение и обработка информации об одних и тех же узлах обычно обеспечивается несколькими DNS-серверами, изолированными физически и логически. Такой подход обеспечивает доступность информации даже при сбое одного или нескольких узлов.

Иерархия и делегирование доменных имен

Домен представляет собой именованную ветвь в дереве имен, включающую в себя сам узел (напр., домен первого уровня ".com"), а также подчиненные ему узлы (напр., домен второго уровня "example.com", домен третьего уровня "mail.example.com" и т.д.). Для обозначения иерархической принадлежности доменных имен принято использовать понятие "**уровень**" - показатель положения узла в дереве доменов. Чем ниже значение уровня, тем выше иерархическое положение домена

- **"."** - домен нулевого уровня
- **".ru"** - домен первого (верхнего) уровня

- **"example.com"** - домен второго уровня
- **"mail.example.com"** - домен третьего уровня
- Этот список можно продолжать



Обратите внимание на домен нулевого уровня **"." (dot - точка)**, также называемый корневым. На практике точку обычно не указывают ("example.com" вместо "example.com."), т.е. указание корневого домена не является обязательным условиям разрешения IP-адреса. Большинство клиентских программ (интернет-браузеров и т.д.) добавляют домен нулевого уровня автоматически и не отображают его пользователю. Доменное имя, не включающее обозначение домена нулевого уровня называется относительным, включающее же точку на конце - полностью определенным **(FQDN - Fully Qualified Domain Name)**.

Доменная зона - часть иерархического дерева доменных имен (напр. ".ru"), целиком переданная на обслуживание определенному DNS-серверу (чаще нескольким) с целью делегирования другому лицу ответственности за этот и все подчиненные домены ("anyaddress.ru", "any.anyaddress.ru").

Делегирование - передача ответственности за определенную ветвь дерева доменных имен другому физическому или юридическому лицу. Именно эта процедура практически реализует важный принцип работы DNS - распределенность хранения записей и обработки запросов. Сам процесс делегирования представляет собой добавление в ресурсные записи родительской зоны (".ru"), так называемых "склеивающих" ("glue") NS-записей для делегируемой дочерней зоны ("example.com"), указывающих на

DNS-сервера принимающей домен стороны (например, DNS-сервера нашей компании). С этого момента все ресурсные записи домена второго уровня "example.com" и всех его дочерних доменов (например, "mail.example.com" и т.д.) хранятся на DNS-серверах этой компании, а родительская зона ".ru" хранит только указывающие на эти сервера NS-записи.

DNS-сервер - хост, хранящий ресурсные записи и обрабатывающий DNS-запросы. DNS-сервер может самостоятельно разрешать адреса, относящиеся к зоне его ответственности (в примере выше это зона example.com), или передавать запросы по зонам, которые он не обслуживает, вышестоящим серверам.

DNS-клиент - набор программных средств для работы с DNS. Сам DNS-сервер периодически также выступает в качестве клиента.

Основные типы ресурсных записей

Ресурсная запись (RR - Resource Record) - единица хранения и передачи информации в DNS, включающая в себя следующие элементы (поля):

- **Имя (Name)** - имя домена, к которому относится запись
- **TTL (Time To Live)** - допустимое время хранения записи неответственным сервером
- **Тип (Type)** - параметр, определяющий назначение и формат записи в поле данных (Rdata)
- **Класс (Class)** - тип сети передачи данных (подразумевается возможность DNS работать с типами сетей, отличных от TCP/IP)
- **Длина поля данных (Rdlen)**
- **Поле данных (Rdata)** - содержание и формат поля зависят от типа записи

Ниже представлены типы ресурсных записей, используемые чаще всего:

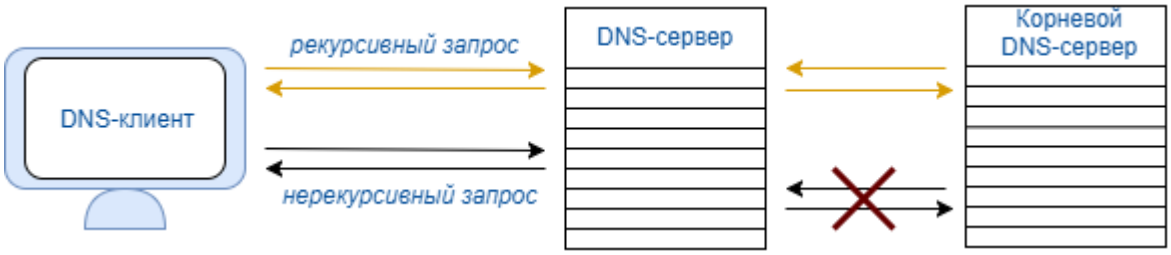
- **A (IPv4 Address Record - адресная запись)** - связывает доменное имя с IPv4-адресом хоста
- **AAAA (IPv6 Address Record)** - связывает доменное имя с IPv6-адресом хоста (аналогично A-записи)

- **CNAME (Canonical Name Record - каноническая запись имени)** - используется для перенаправления на другое доменное имя
- **MX (Mail Exchange - почтовый обменник)** - ссылается на почтовый сервер, обслуживающий домен
- **NS (Name Server - сервер имен)** - ссылается на DNS-сервер, ответственный за домен
- **TXT** - текстовое описание домена. Зачастую требуется для выполнения специфических задач (например, подтверждения права собственности на домен при привязке его к почтовому сервису)
- **PTR (Point to Reverse - запись указателя)** - связывает ip-адрес машины с доменом, используется преимущественно для проверки сторонними почтовыми сервисами отправляемых через эту машину электронных писем на отношение к домену, указанному в параметрах почтового сервера. При несоответствии этих параметров письмо проверяется более тщательно по другим критериям.

Рекурсивные и нерекурсивные DNS-запросы

Рекурсией называется модель обработки запросов DNS-сервером, при которой последний осуществляет полный поиск информации, в том числе о доменах, неделегированных ему, при необходимости обращаясь к другим DNS-серверам.

DNS-запросы (DNS queries) от клиента (сервера) к серверу бывают рекурсивными и нерекурсивными. В первом случае DNS-сервер, принявший запрос, опрашивает все узлы в порядке убывания уровня зон, пока не получит положительный ответ или информацию о том, что запрашиваемый домен не существует. В случае с нерекурсивными запросами сервер даст положительный ответ только при запросе узла, входящего в доменную зону, за которую этот сервер ответственен. Отсутствие рекурсии может быть обусловлено не только типом запроса, но и запретом на выполнение таких запросов со стороны самого DNS-сервера.



Кэширование - еще одна важная характеристика DNS. При последовательном обращении сервера к другим узлам в процессе выполнения рекурсивного запроса DNS-сервер может временно сохранять в кеш-памяти информацию, содержащуюся в получаемых им ответах. В таком случае повторный запрос домена не идет дальше его кэш-памяти. Предельно допустимое время кэширования содержится в поле TTL ресурсной записи.

Список источников:

1. https://1cloud.ru/help/dns/dns_basics