Лекция 8. ПРОТОКОЛ DNS

Основные положения

1. **Назначение сервиса Domain Name System**

   Сервис DNS, работающий по одноимённому протоколу, это сервис прикладного уровня, поддерживающий пространство символьных имен хостов, которое удобнее для пользователей, чем пространство IP адресов.

   К задачам DNS относятся:

   a. отображение двух пространств имен друг на друга,
   b. обнаружение сервисов в IP сети,
   c. хранение конфигурационных данных приложений.

   DNS была описана Полом Мокапетрисом (Paul Mockapetris) в 1984 в двух документах RFC-882 и RFC-883, которые позже эти документы были заменены на RFC-1034 и RFC-1035.

   В настоящее время работа DNS описывается RFC-4032, -4034, -4035, -2137, -2052, -2136, -1996, -1918, -1793, -1712-13, -1706, -1664, -1611-12, -1536-37, -1401, -1383, -1183, -1101, -1034-35 и др.

   К основным принципам работы DNS относятся:

   a. Иерархическая древовидная структура
   b. Распределённость администрирования
   c. Распределённость хранения информации
   d. Резервирование
   e. Кеширование информации

2. **Номера портов и формат пакета**

   Сообщения DNS инкапсулируются или в сообщения UDP или в сегменты TCP. В любом случае DNS сервер работает по порту №53. Если используется DNS поверх TLS то номер порта меняется на 853. Клиенты с серверами взаимодействуют по UDP, сервера при передаче конфигурационной информации между друг-другом – TCP.

   Формат заголовка DNS представлен на рис.

Идентификатор (16 бит)	Флаги (16 бит)
Число запросов (16 бит)	Число откликов (16 бит)
	Число записей в секции доп.информации
Секция запроса	
Секция отклика	
Секция сервера имен	
Секция доп информации	

Сообщение DNS

   Позволяет связать между собой запрос и отклик. Поле флаги определяет характер запрашиваемой процедуры, а также кодировку отклика. Поля Число откликов определяют число записей соответствующего типа, содержащихся в сообщении. Так число запросов задает число записей в секции запросов, где записаны запросы, требующие ответов. Каждый вопрос состоит из символьного имени домена, за

которым следует тип запроса и класс запроса. Перечислим по порядку значения флагов:

- 1 бит, операция: 0 Запрос или 1 Отклик,
- 4 бита Тип запроса: 0 стандартный, 1 инверсный, 2 запрос состояния сервера,
- 1 бит (AA): 1 при отклике от сервера (RR), в ведении которого находится домен, упомянутый в запросе.
- 1 бит (TC): 1 при укорочении сообщения. Для UDP это означает, что ответ содержал более 512 октетов, но прислано только первые 512.
- 1 бит (RD): 1, если для получения ответа желательна рекурсия.
- 1 бит (RA): 1, если рекурсия для запрашиваемого сервера доступна.
- 3 бита - зарезервировано на будущее. Должны равняться нулю.
- 4 бита - тип отклика (rcode): 0 нет ошибки, 1 ошибка в формате запроса, 2 сбой в сервере, 3 имени не существует.

3. Основные понятия

Домен (доменное имя) — область пространства иерархических имён сети Интернет, которая обозначается уникальным доменным именем, обслуживается набором серверов доменных имён (DNS) и централизованно администрируется.

DNS-клиент – программа-клиент, которая по запросу приложений обращается к DN-серверу за разрешением имени.

DNS-сервер - программа-сервер предназначенная для:

a. Хранения данных о доменных именах
b. Разрешения доменных имен (определение IP адреса) по запросу клиентов

DNS сервера бывают:

a. Основными и резервными
b. Рекурсивными и не рекурсивными
c. Кэширующими

Зона – файл, в котором описано соответствие хостов домена и их IP-адресов. В Интернет за каждую зону DNS должно отвечает не менее двух серверов.

Ресурсная запись — единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определённому доменному имени, узлу в дереве имён), тип и поле данных, формат и содержание которого зависит от типа.

Разрешение имени – процесс определение IP адреса по доменному имени (или наоборот), осуществляемы DNS-сервером в ответ на запрос DNS-клиента.

4. Пространство имен

Пространство имен DNS строится исходя из следующих принципов:

a. Пространство имен - дерево в корне которого находится домен точка.
b. Названия доменов верхнего уровня регламентируются ICANN и могут быть национальными (ru, uk) и тематическими (org, net, com, home).
c. Лист дерева домена – ресурсная запись.
d. Имена двух соседних доменов или ресурсной записи и домена, ее содержащего не могут совпадать.
e. Максимальный размер FQDN — 255 байт включая корневой домен «.», с ограничением в 63 байта на каждое имя домена.
f. Поддерживаются национальные кодировки.
g. Существуют зарезервированные имена доменов – test, invalid и др.

По этому дереву определяются IP адреса по доменному имени. Эти зоны называются зонами прямого просмотра.

5. **Зоны обратного просмотра**

   Существуют зоны обратного просмотра. Они позволяют по IP адресу найти доменное имя.

   Для этого служат специальные домены в зоне arpa.

   Для IPv4-адрес 192.168.0.1 превращается в 1.0.168.192.in-addr.arpa., а для IPv6-адрес 2001:db8::567:89ab превратится в адрес: b.a.9.8.7.6.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

   Эти зоны содержат записи PTR, которые содержат ссылку на обычные записи в зонах прямого просмотра.

6. **Ресурсные записи**

   Существуют множество типов ресурсных записей:

   a. SOA (Start of Authority/начальная запись зоны) - конфигурационная запись домена, управляющая кэшированием и синхронизацией копии зоны,
   b. A — (address record/запись адреса) - запись адреса в протоколе IPv4,
   c. AAAA (IPv6 address record) аналогична записи A, но для IPv6,
   d. CNAME (canonical name record/каноническая запись имени (псевдоним)), например WWW,
   e. MX (mail exchange) – конфигурация почтовых серверов,
   f. NS (name server/сервер имён) – записи о доменных серверов в доменах,
   g. PTR (pointer) – указатели на DNS имена в зонах обратного просмотра,
   h. SRV (server selection) – записи, указывающие на службы, например LDAP
   i. TXT – текстовые записи, например SPF и DKIM, которые защищают от подделки домена при отправке писем

7. **Корневые сервера**

   Корневые серверы DNS — DNS-серверы, обеспечивающие работу корневой зоны DNS в сети Интернет. Позволяют получить список DNS-серверов для любого домена верхнего уровня.

   Корневые серверы DNS управляются двенадцатью организациями. Их уполномочивает ICANN (Корпорация по управлению доменными именами и IP-адресами -Internet Corporation for Assigned Names and Numbers).

   IP адреса корневых серверов содержатся как параметр конфигурации любого DNS сервера.

8. **Разрешение имен**

   У клиента в качестве параметра есть IP адрес DNS сервера. Разрешение имени проходит в следующие этапы:

   a. Клиент дает запрос своему DNS серверу
   b. Пусть DNS сервер рекурсивный и он должен вернуть клиенту уже IP адрес, тогда он:
   c. Обращается к корневому серверу, тот ему возвращает IP адрес DNS сервера домена первого уровня,
   d. После этого DNS сервер обращается к домену первого уровня, а тот возвращает IP адрес домена второго уровня и т.д.

e. Когда достигнут домен, который содержит ресурсную запись, он вернет нашему DNS серверу значение IP адрес искомого доменного имени.
f. А наш DNS сервер вернет DNS клиенту ответ.

9. Регистрация имени

В доменах первого уровня и некоторых доменах второго уровня (например spb) недостаточно прописать ссылки на NS сервера дочернего домена, нужно получить на это право.

Процесс занятия доменного имени называется Регистрацией имени.

Регистрация доменного имени — занесение регистратором в реестр информации о доменном имени и его администраторе. Реестр — центральная база данных домена, содержащая информацию о зарегистрированных доменных именах, Администраторах доменов, иную информацию, необходимую для регистрации доменов. В реестр записи о домене заносятся Регистратором доменных имён — уполномоченным юридическим лицом. Для доменов ru, su, РФ – 38 регистраторов уполномочены АНО «Координационный центр национального домена сети Интернет».

Основные термины

1. Домен (доменное имя) — область пространства иерархических имён сети Интернет, которая обозначается уникальным доменным именем, обслуживается набором серверов доменных имён (DNS) и централизованно администрируется.
2. DNS-клиент – программа-клиент, которая по запросу приложений обращается к DN-серверу за разрешением имени.
3. DNS-сервер - программа-сервер предназначенная для:
4. Хранения данных о доменных именах
5. Разрешения доменных имен (определение IP адреса) по запросу клиентов
6. Рекурсивный сервер – DNS сервер, который возвращает клиенту IP адрес хоста.
7. Не рекурсивный сервер - DNS сервер, который возвращает клиенту IP адрес следующего DNS сервер.
8. Зона – файл, в котором описано соответствие хостов домена и их IP-адресов. В Интернет за каждую зону DNS должно отвечает не менее двух серверов.
9. Ресурсная запись — единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определённому доменному имени, узлу в дереве имён), тип и поле данных, формат и содержание которого зависит от типа.
10. Разрешение имени – процесс определение IP адреса по доменному имени (или наоборот), осуществляемы

Дополнительная литература

1. https://www.rfc-editor.org
2. http://rfc.com.ru
3. http://book.itep.ru/4/44/dns_4412.htm
4. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020 г.
5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2019 г.