网络服务—DNS 域名系统服务

1. DNS 介绍

1.1什么是域名？

域名（Domain Name），简称域名、网域，是由一串用点分隔的名字组成的 Internet 上某一台计算机或计算机组的名称，用于在数据传输时标识计算机的电子方位。具有独一无二，不可重复的特性。

1.2什么是 DNS？

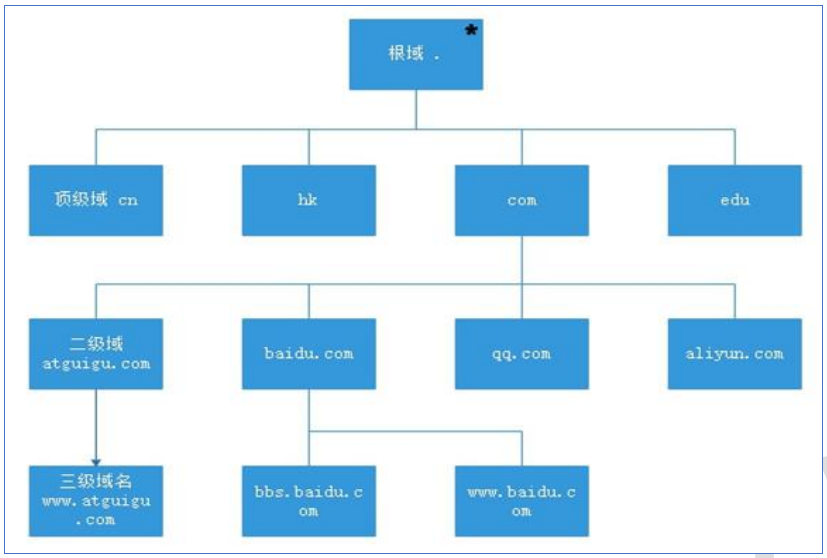
域名系统（Domain Name System，缩写：DNS）是互联网的一项服务。域名解析是把域名指向网站空间 IP，让人们通过注册的域名可以方便地访问到网站的一种服务。IP 地址是网络上标识站点的数字地址，为了方便记忆，采用域名来代替 IP 地址标识站点地址。域名解析就是域名到 IP 地址的转换过程。域名的解析工作由 DNS 服务器完成。可以理解为 DNS 就是翻译官。
正向解析：域名 --> IP 地址
反向解析：IP 地址 --> 域名

1.3域名的组成和分类

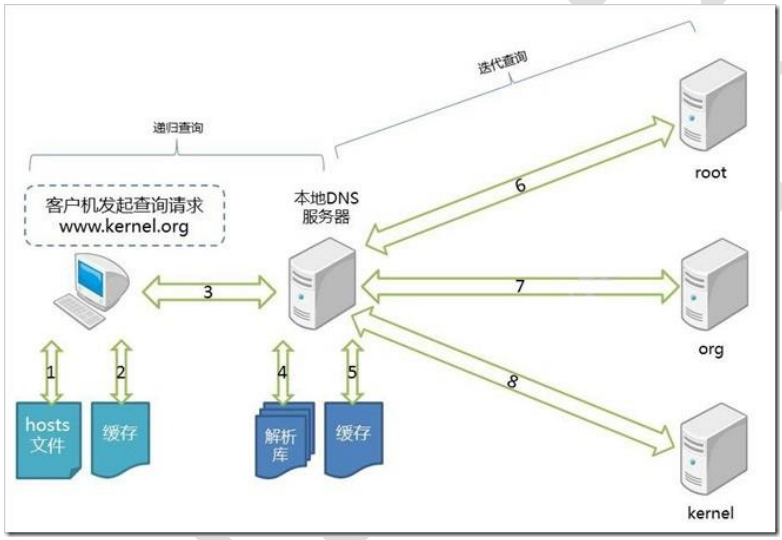
常见格式：www.atguigu.com
完整格式：www.atguigu.com.

. ： 根域，可省略不写
com： 顶级域，由 ICANN 组织指定和管理
分类：
国家地区域名：cn（中国）、hk（香港）、sg（新加坡）等
通用顶级域名：com（商业机构）、org（非营利组织）、edu（教育机构）等
新通用顶级域名：red（红色、热情）、top（顶级、高端）等
atguigu：二级域（注册域），可由个人或组织申请注册
www： 三级域（子域），服务器网站名代表
主机名：s1.www.atguigu.com. 中的 s1 就是主机名，一般用来表示具体某一台主机

拓展：com.cn属于“二级域名”，是 cn 顶级域的子域



2. 域名解析过程



1. 客户机首先查看查找本地 hosts 文件，如果有则返回，否则进行下一步
2. 客户机查看本地缓存，是否存在本条目的缓存，如果有则直接返回，否则进行下一步。
3. 将请求转发给指向的 DNS 服务器。
4. 查看域名是否本地解析，是则本地解析返回，否则进行下一步。
5. 本地 DNS 服务器首先在缓存中查找，有则返回，无则进行下一步。
6. 向全球 13 个根域服务器发起 DNS 请求，根域返回 org 域的地址列表。
7. 使用某一个 org 域的 IP 地址，发起 DNS 请求，org 域返回 kernel 域服务器地址列表。
8. 使用某一个 kernel 域 IP 地址，发起 DNS 请求，kernel 域返回 www.kernel.org 主机的 IP 地址，本地 DNS 服务收到后，返回给客户机，并在本地 DNS 服务器保存一份。

3. DNS 软件信息

软件名称：

bind

服务名称：

named

软件端口：

UDP 53　数据通信（域名解析）

TCP 53　数据同步（主从同步）

配置文件：

主配置文件：/etc/named.conf（服务器运行参数）

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };
        recursion yes;
```

设置服务器监听网卡（可以写具体某一个IP，也可以写成any）

数据文件位置

设置可以访问服务器的客户端IP（可用any）

区域配置文件：/etc/named.rfc1912.zones（服务器解析的区域配置，正反向区域定义信息）

```
zone "localhost.localdomain" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};
```

正向区域配置文件标签，修改为要解析的域

DNS服务器类型（master/slave）

正向数据配置文件名称（默认保存在/var/name/下）

允许数据更新的列表（填写IP地址）

反向区域配置文件标签，仅修改IP位置，并且将IP反写

例如：　0.168.192.in-addr.arpa

数据配置文件：/var/named/xx.xx（主机名和 IP 地址的对应解析关系，及主从同步信息）

```
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
```

域名有效解析生存周期（一般指缓存时间）

@：代表域名本身

SOA：SOA标记(起始授权机构的资源记录，描述了域名的管理员、电子邮件地址，和一些时间参数)

配置文件修改版本(如:20190826)

更新频率（从向主的查询周期）

更新失败的重试时间周期

无法更新时的失效周期

缓存服务器无法更新时的失效时间

设置DNS服务器的域名

IPv4的 域名IP解析记录

IPv6的 域名IP解析记录

记录类型：

A：	地址记录，用来指定域名的 IPv4 地址的记录
CNAME：	将域名指向另一个域名，再由另一个域名提供 ip 地址，就需要添加 CNAME 记录
TXT：	可填写任何东西，长度限制 255。绝大多数的 TXT 记录是用来做 SPF 的（反垃圾邮件）
NS：	域名服务器记录，如果需要把子域名交给其他 DNS 服务商解析，就需要添加 NS 记录。
AAAA：	地址记录，用来指定域名的 IPv6 地址的记录

MX：	邮件交换记录，如果需要设置邮箱，让邮箱能收到邮件，就需要添加 MX 记录。

4. DNS 实验搭建

4.1DNS 服务搭建

先关闭服务器和客户机上的防火墙和 SELinux

1. 软件安装
   yum -y install bind
2. 配置主配置文件（/etc/named.conf）
3. 配置区域文件（/etc/named.rfc1912.zones）
   注：先对区域文件进行备份，删除多余的模板，只留下一个正向和一个反向（反向修改时，网络位的反写格式，如 192.168.100.2-->100.168.192.）
4. 配置数据文件/var/named/
   A． 先复制生成正向解析文件和反向解析文件
   B． 编辑正向解析文件（**注意域名结尾的 “.”**）
   C． 编辑反向解析文件（**注意域名结尾的 “.”**）
5. 重启 DNS 服务
   service named restart
6. 客户端测试
   在网卡配置文件中添加 DNS 服务器的地址，然后用 nslookup 测试。

4.2主从 DNS 服务器

实验目的：

减轻主服务器的压力

先关闭服务器和客户机上的防火墙和 SELinux

实验准备：

一台主服务器、一台从服务器、一台测试机

搭建过程：

1. **搭建主服务器步骤（同上，不截图了）：**
   a. 安装 bind 软件
   b. 主配置文件的修改
   c. 区域配置文件的修改
   d. 配置数据文件
      正向数据文件
      反向数据文件（可选做）
   e. 启动 named 服务

注意：主 DNS 的区域配置文件中 **allow-updata** 参数添加从服务器 IP 地址。

2. **搭建从服务器步骤：**
   a. 安装 bind 软件

b. 修改主配置文件/etc/named.conf

c. 配置区域文件（/etc/named.rfc1912.zones）

注意：从配置文件的类型需要修改为 slave，并且需要填写主服务器的地址，如下

```
type slave;
masters { 192.168.0.10; };        #大括号两侧留有空格
文件保存位置修改为 file “slaves/atguigu.localhost”;
```

d. 重启服务

e. 在测试机上填写从服务器的 IP，并使用 nslookup 测试

4.3DNS 缓存服务器

先关闭服务器和客户机上的防火墙和 SELinux

实验作用：

加快解析速度，提高工作效率

实验软件：

dnsmasq

配置文件：

```
/etc/dnsmasq.conf
    domain=域名                    #需要解析的域名
    server=ip                      #主 DNS 服务器 IP
    cache-size=15000               #声明缓存条数
```

重启服务：

service dnsmasq restart

测试效果：

在测试机上填写 DNS 缓存服务器的 ip 地址

4.4智能 DNS（分离解析）

实验原理：DNS 分离解析即将相同域名解析为不同的 IP 地址。现实网络中一些网站为了让用户有更好的体验效果解析速度更快，就把来自不同运营商的用户解析到相对应的服务器这样就大大提升了访问速度

实验环境：

一台内网测试机（单网卡）

一台网关+DNS（双网卡）

一台外网测试机（单网卡）

一台 web 服务器（双网卡）

先关闭服务器和客户机上的防火墙和 SELinux

实验步骤：

1. 安装 bind 软件
2. 内核配置文件开启路由转发，修改/etc/sysctl.conf
3. 修改主配置文件/etc/named.conf

```
view lan {
        match-clients { 192.168.10.0/24; };
        zone "." IN {
                type hint;
                file "named.ca";
        };
        include "/etc/lan.zones";
};

view wan {
        match-clients { any; };
        zone "." IN {
                type hint;
                file "named.ca";
        };
        include "/etc/wan.zones";
};
#include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

注意：不同的解析放在了各自的区域配置文件（便于区分和维护更新）

4. **生成自己定义的区域文件（反向解析省略掉了）**

   cp -a named.rfc1912.zones lan

   cp -a named.rfc1912.zones wan

5. **配置数据文件**

   配置内网的正向解析文件

   配置外网的正向解析文件

6. **重启服务**

   service named restart

7. **效果测试**

   内网客户端网卡配置

   将 dns 和网关都指为网关服务器的内网口地址

   外网客户端网卡配置

   将 dns 和网关都指为网关服务器的外网口地址