第十一章、DNS部署与安全

author：杨哥团队-史密斯

1、DNS

Domain Name Service
域名服务

作用：为客户机提供域名解析服务器

2、域名组成

2.1、域名组成概述

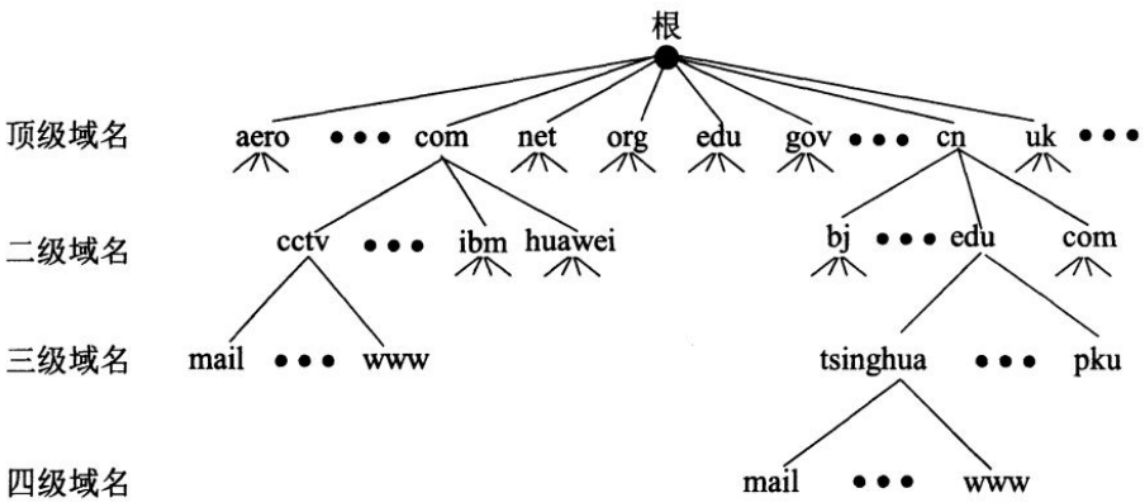
如"www.sina.com.cn"是一个域名，从严格意义上讲，"sina.com.cn"才被称为域名(全球唯一)，而"www"是主机名。

"主机名.域名"称为完全限定域名(FQDN)。一个域名下可以有多个主机，域名全球唯一，那么"主机名.域名"肯定也是全球唯一的。

以"sina.com.cn"域名为例，一般管理员在命名其主机的时候会根据其主机的功能而命名，比如网站的是www，博客的是blog，论坛的是bbs，那么对应的FQDN为www.sina.com.cn，blog.sina.com.cn，bbs.sina.com.cn。这么多个FQDN，然而我们只需要申请一个域名即"sina.com.cn"即可。

2.2、域名组成

树形结构



根域　.

顶级域

　　国家顶级域 cn jp hk uk

　　商业顶级域

com 商业机构

gov 政府机构

mil 军事机构

edu 教育机构

org 民间组织架构

net 互联网

一级域名

二级域名

。。。。

```
如：www.baidu.com.

.为根域

.com为顶级域

baidu为一级域名

www为主机名
```

```
FQDN=主机名.DNS后缀

FQDN（完整合格的域名）
```

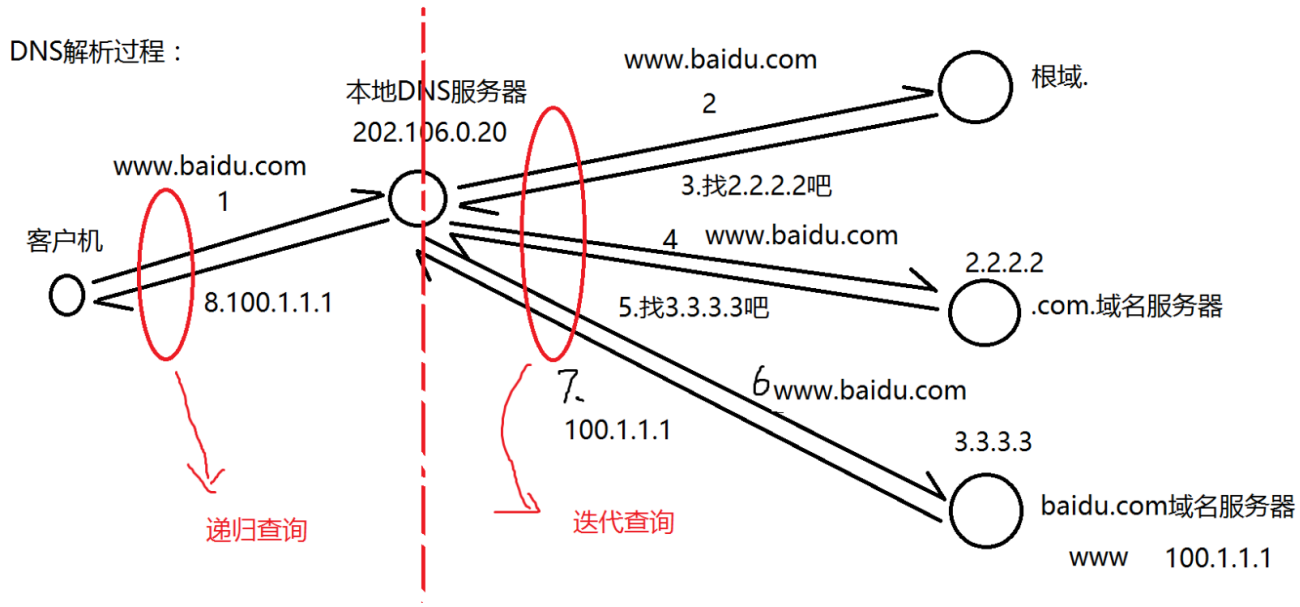
3、监听端口

```
TCP53

UDP53
```

4、DNS解析种类

4.1、按照查询方式分类：

```
1）递归查询：客户机与本地DNS服务器之间

2）迭代查询：本地DNS服务器与根等其他DNS服务器的解析过程
```



4.2、按照查询内容分类：

1）正向解析：已知域名，解析IP地址

2）反向解析：已知IP地址，解析域名

5、DNS服务器搭建过程

1）要求网卡IP是静态IP地址。

2）安装DNS服务器插件（也就是安装并开启TCP及UDP53端口）

3）创建区域文件（负责一个域名后缀的解析，如baidu.com为域名后缀，一台DNS服务器内可存放多个区域文件）

4）新建A记录

6、DNS客户机如何解析

1）指向DNS

2）手工解析域名：

```
nslookup  域名
```

```
C:\Users\wencoll>nslookup www.baidu.com
服务器:  gjjline.bta.net.cn
Address:  202.106.0.20

非权威应答:
名称:    www.a.shifen.com
Addresses:  61.135.169.121
          61.135.169.125
Aliases:  www.baidu.com
```

```
nslookup

域名
```

```
C:\Users\wencoll>nslookup
默认服务器:  gjjline.bta.net.cn
Address:  202.106.0.20

> www.baidu.com
服务器:  gjjline.bta.net.cn
Address:  202.106.0.20

非权威应答:
名称:    www.a.shifen.com
Addresses:  61.135.169.121
          61.135.169.125
Aliases:  www.baidu.com

>
```

7、DNS服务器处理域名请求的顺序

1）DNS高速缓存（必须学会如何查看及清空）

2）DNS区域配置文件

3）DNS转发器

4）根提示

8、辅助DNS服务器

9、清除DNS缓存

9.1、客户机上清除缓存

```
ipconfig  /flushdns
```

9.2、服务器上清除缓存

```
windows服务器：dns工具--查看--高级，调出缓存来，然后右键清除缓存
```

10、域名解析记录类型：

A记录： 正向解析记录

CNAME记录：别名

PTR记录：反向解析记录

MX：邮件交换记录

NS：域名服务器解析

11、反向DNS

nslookup手工解析时，会进行一个反向解析

12、DNS服务器分类

主要名称服务器
辅助名称服务器
根名称服务器
高速缓存名称服务器

13、客户机域名请求解析顺序

1.DNS缓存----2.本地hosts文件--3.找本地DNS服务器

14、服务器对域名请求的处理顺序

1.DNS高速缓存--2.本地区域解析文件--3.转发器--4.根

15、练习

1.主要DNS服务器: 员工要指向DNS，练习清空DNS缓存，练习nslookup手工解析

2.反向解析

3、辅助DNS服务器：成功更新区域解析记录1

4、.转发器/根

5、（选做）将xp与2003桥接能上网，部署2003位DNS服务器，xp指向2003，并能实现XP正常上网

6、别名