



第 8 章 应用层(1)

课程名称： 计算机网络

主讲教师： 姚焱

课程代码： U10M11016.02

第45-46讲

E-MAIL : yaoye@nwpu. edu. cn

2021 – 2022 学年第一学期



第 8 章 应用层

- 8. 1 域名系统 DNS
- 8. 2 万维网 WWW (HTTP)
- 8. 3 文件传输系统 (FTP)
- 8. 4 远程终端系统 TELNET
- 8. 5 电子邮件系统
- 8. 6 动态主机配置系统 (DHCP)

引言

- 在TCP/IP模型中，通常将OSI参考模型的5~7层，即会话层、表示层和应用层都归结为应用层。
- 应用层为具体的网络应用服务提供编程接口，以协议、命令形式提供给用户；



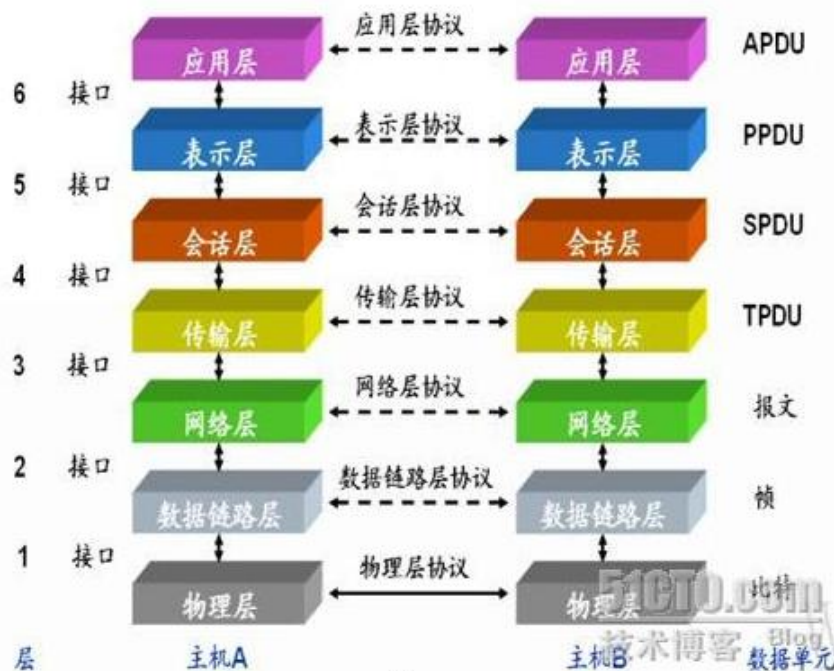
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6
Cache-Control: max-age=0
Connection: keep-alive
Host: www.baidu.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36
```

```
ftp> mget *.php
200 Type set to A.
mget i.php? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 收到 18 字节, 用时 0.07秒 0.27千字节/秒。
mget index.php? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 收到 418 字节, 用时 0.06秒 6.63千字节/秒。
mget wp-activate.php?
```

引言

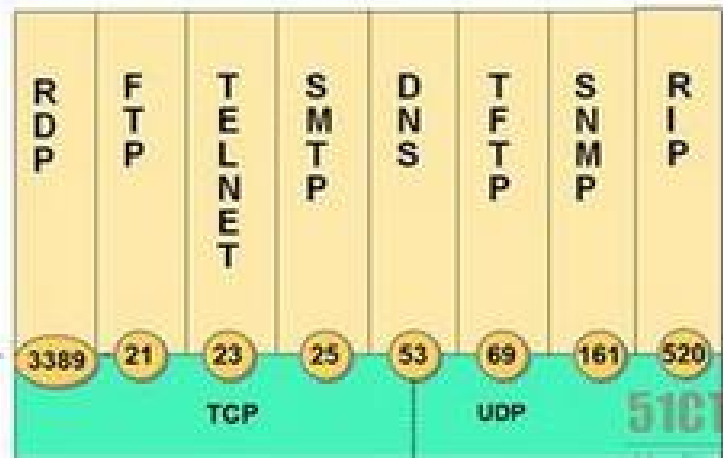
- 应用层**具体实现**是每个应用层协议
- 应用层协议:规定应用层进程通信时所遵循通信规程。
- 用户程序也可直接调用传输层提供的数据传输服务;

用户程序



应用层协议的特点

- 应用层协议仍属于网络体系结构一部分
 - 在实现方式上，可以由网络操作系统实现并提供服务，也可由用户编写应用程序实现。
- 由于网络应用需求是多种多样，每一种网络应用都可能对应一种应用层协议。
 - 常见应用协议HTTP，SMTP，TELNET，FTP，SNMP，DNS，DHCP等应用层的许多协议都是基于客户/服务器方式。





第 8 章 应用层

第一节：域名系统(DNS)

Domain Name System



问题提出？

- LAN内通信时首先明确“和谁通信”，物理地址；二层转发机制实现通信；
- 不同网络间通信：IP地址；三层路由机制；
- IP地址在记忆和使用方面不直观，因此互联网上采用了域名来表示主机IP地址，方便用户使用和记忆。
 - 222. 24. 192. 45：80 - www.nwpu.edu.cn：80
- 域名与IP地址的映射？
 - 域名系统DNS (Domain Name System)：提供域名到IP地址映射服务。



域名系统 DNS

1. 域名空间
2. 资源记录
3. 域名服务器
4. 域名解析方法

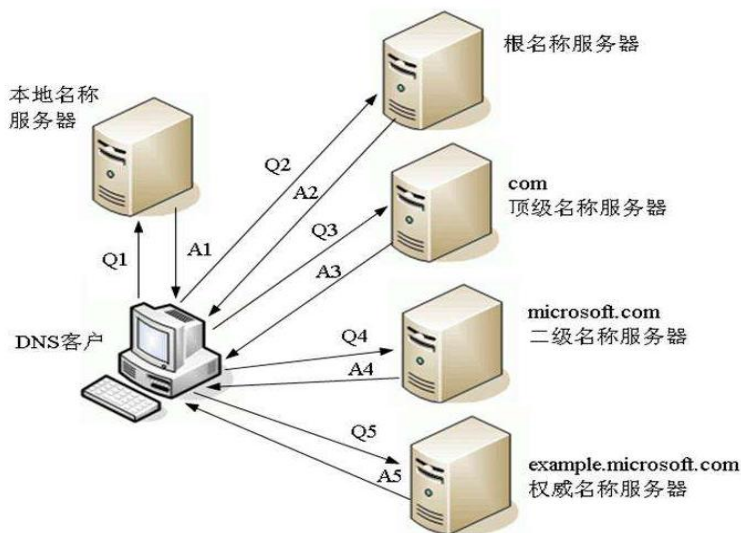
1. 域名空间

- 许多网络应用服务会直接使用**域名系统** DNS（如WEB，FTP，邮件服务等），但用户不会觉察到。
 - www.nwpu.edu.cn
 - <ftp://ftp.nisi.nwpu.edu.cn>
 - mail.nwpu.edu.cn

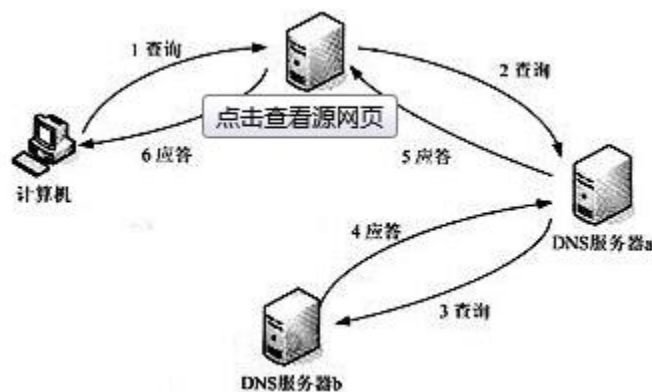


1. 域名空间

- 域名到IP地址解析是由若干个域名服务器程序完成。
- 域名服务器程序部署在网络端节点上运行，运行该程序的计算机称为域名服务器。



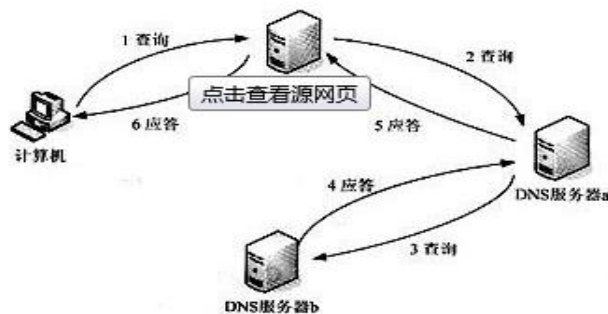
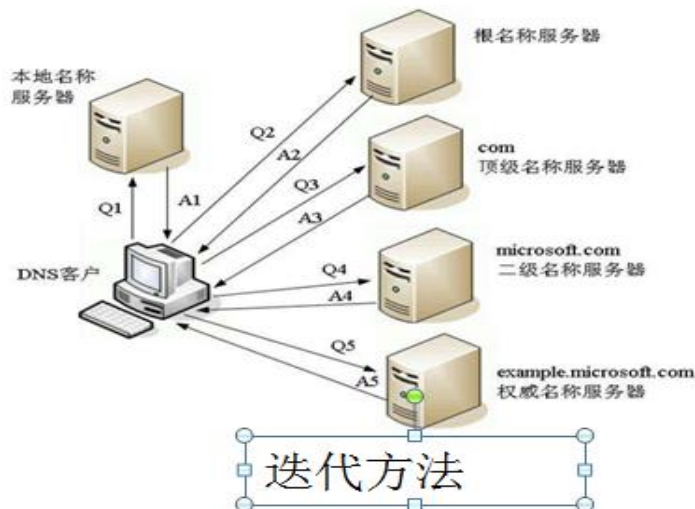
迭代方法



递归方法

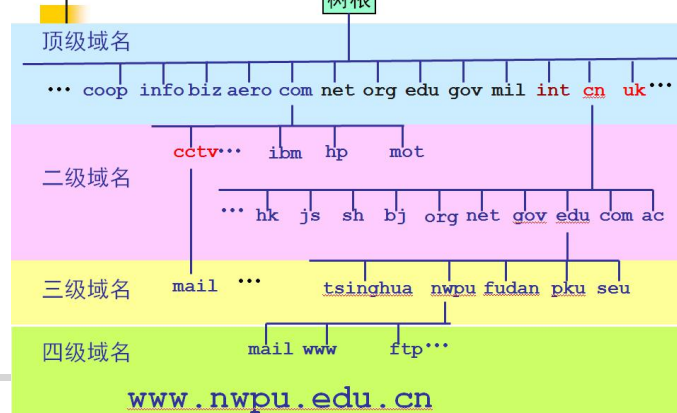
1. 域名空间

- 解析过程：当一台PC需要将域名解析为IP时，用户网络系统首先调用DNS客户进程（解析器：resolver）发送DNS请求报文，以UDP用户数据报形式发送给**本地域名服务器**；
 - 如果**本地域名服务器**查找到对应IP后，以DNS应答形式发送告诉- DNS客户进程-应用程序；
 - 否则，**本地域名服务器**以**客户**形式向其他域名服务器发送DNS查询请求，直到找到对应IP地址为止。



递归方法

1. 域名空间

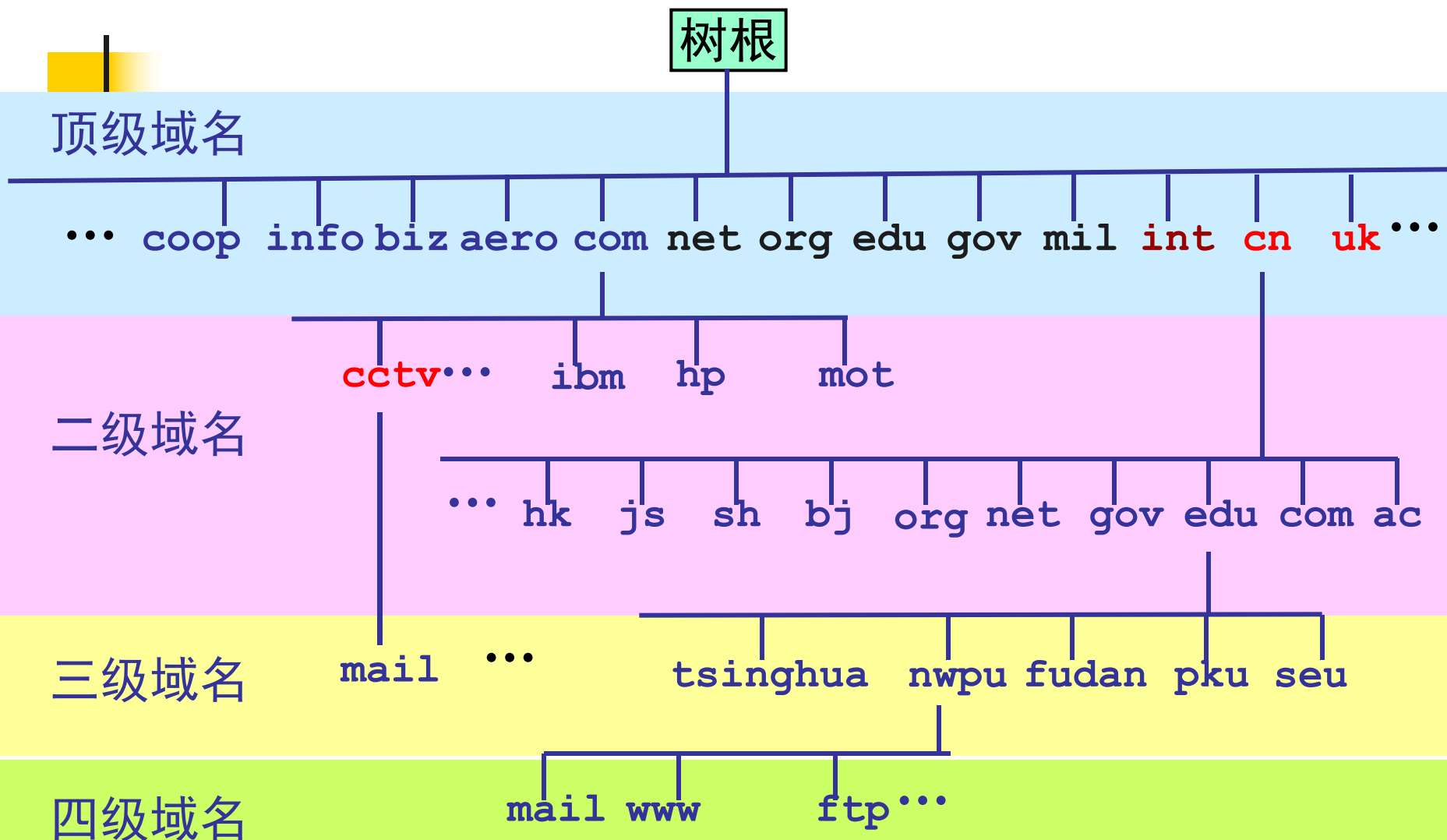


- 域名如同IP地址分配一样，要解决**如何分配**和**存储**。
 - 因特网采用**层次树状结构实现**域名分配、命名以及管理
 - 任何一个连接在因特网上的主机或路由器，都可以有一个惟一域名；
 - 域名由若干个**不同级别域名-标号**（labeo）组成，各标号之间用点隔开：各标号分别代表不同级别域名。

... . 三级域名. 二级域名. 顶级域名（一级）

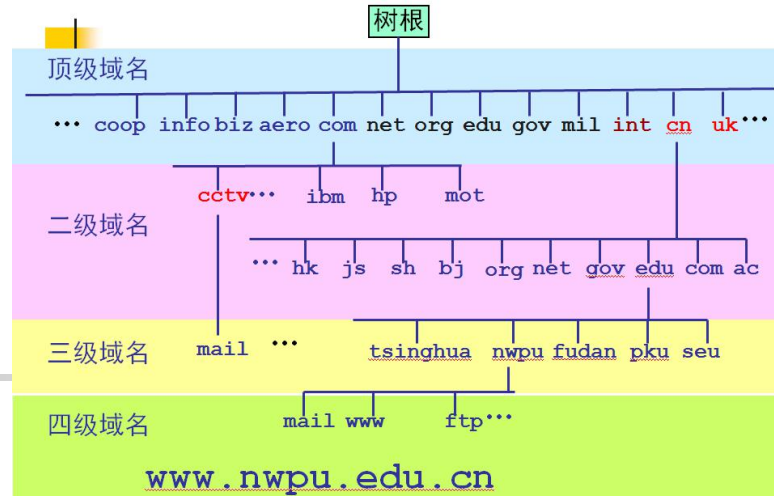
- 域名空间采用树形结构来组织和管理，一个完整的域名是从**叶子节点向上直到根**的不同级别域名组成的字符串，不同级别域名之间用“.”隔开。

因特网的域名空间 :倒立的树



`www.nwpu.edu.cn`

1. 域名空间



■ DNS标准规定

- **不同级别域名**由英文字母和数字组成；
- **不同级别域名**不超过63个字符，为了便于记忆，一般不超过12个；
- 多个**级别域名**构成的完整域名不超过255个字符；
- 每一级域名由其**上一级域名管理机构**管理，而最高的顶级域名由ICANN管理；

■ DNS标准没有规定

- 没有规定：一个域名包含多少个下一级域名；
- 2006年12月统计，现在顶级域名TLD (Top Level Domain) 已经有265个，分为三大类：
 - **国家顶级域名** (nTLD)，**通用顶级域名** (gTLD) 和**基础结构域名** (infrastructure domain)。



顶级域名 TLD

(Top Level Domain)

(1) 国家顶级域名 nTLD: 如: .cn 表示中国, .us 表示美国, .uk 表示英国等; 2006.12月统计共247。

(2) 通用顶级域名 gTLD, 2006.12月统计共18。

最常见的通用顶级域名共有7个:

.com (公司和企业)

.net (网络服务机构)

.org (非赢利性组织)

.edu (美国专用的教育机构)

.gov (美国专用的政府部门)

.mil (美国专用的军事部门)

.int (国际组织)



其他11个通用顶级域名

- .aero : 航空运输企业; .biz : 公司和企业
- .coop : 合作团体; .museum : 博物馆
- .name : 个人;
- .pro : 用于会计、律师和医师等（有证书专业人员）
- .travel : 旅游业;
- .jobs : 人力资源管理者;
- .mobi : 移动产品与服务用户和提供者;
- .info : 各种情况;
- .cat : 加泰隆人的语言和文化团体;



顶级域名 TLD (续)

(3) 基础结构域名：该顶级域名只有一个(即 arpa)，用于反向域名解析，因此又称为反向域名。

■ 国家顶级域名下注册的二级域名由各个国家自行确定。

- 我国将教育和企业机构二级域名定为：.edu, .com;
- 顶级域名为.jp日本将教育和企业机构二级域名定为 .ac, .co;

■ 我国将二级域名划分为两类：“类别域名”和“行政区域名”

- “类别域名”共7个：ac（科研机构）； com（工、商、金融等企业）； edu（教育机构）； gov（政府机构）； mil（国防机构）； net（提供互联网服务的机构）； org（非营利性组织）；
- “行政区域名”共34个：省、自治区和直辖市等，如bj(北京)；
- 我国修订的域名管理允许用户在.cn顶级域名下大公司可直接申请二级域名（66万）如某公司abc原来只能申请：abc.com.cn --- abc.cn;

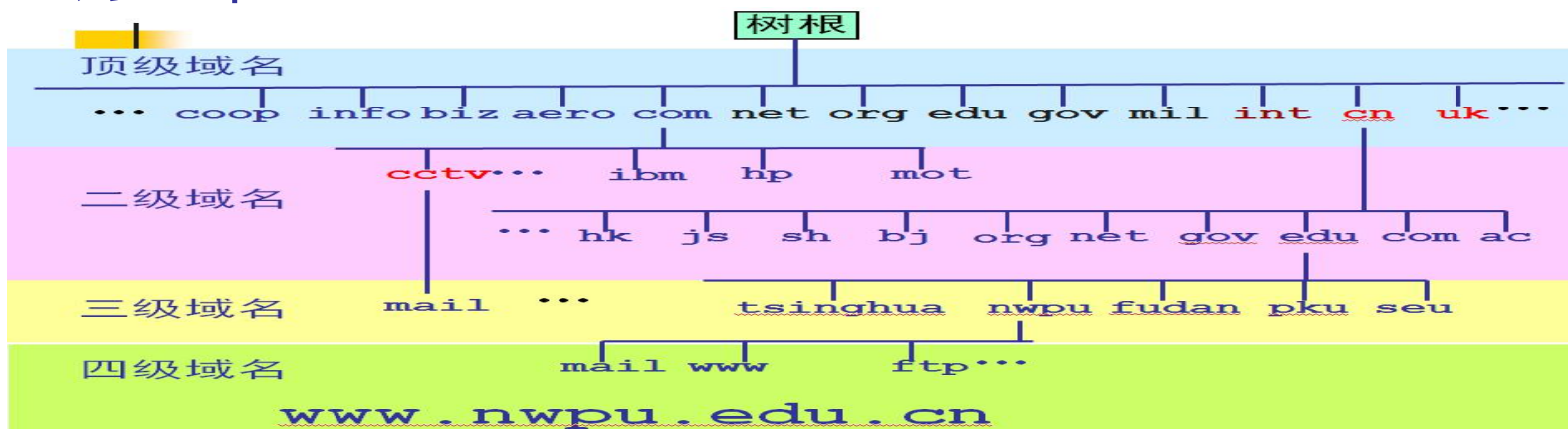


1. 域名空间

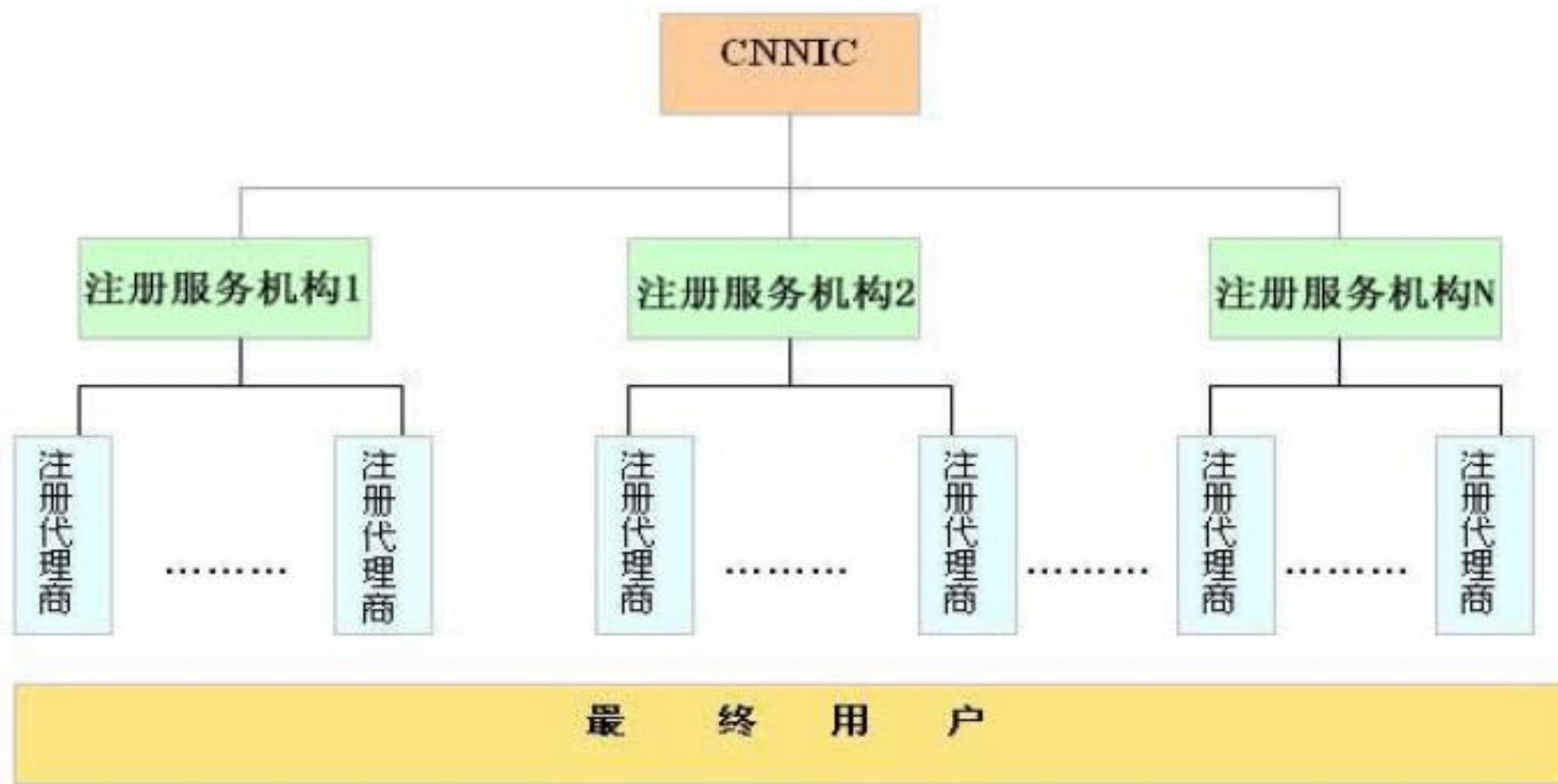
- 域名从右到左，不同级别域名分别是表示**顶级域名**、**组织类型**、**组织名称**、**分组织名称**和**计算机名称**等各级域名。
 - www.nisi.nwpu.edu.cn：从右到左分别表示：顶级域名cn表示中国，edu表示是教育机构，nwpu表示一个学校的名称，nisi表示是该学校中一个院系或研究所名称，www表示是一个Web服务器。
 - WWW.NAVY.MIL：从右到左分别表示：美国军队，海军，WWW表示是一个WEB服务器。
 - 域名中**大小写字母可以混合使用**，但作为一般原则，最好全部使用**小写字母**。

1. 域名空间

- 域名空间中，每一级域名由上级组织机构管理，并可授权下一级组织管理更下一级域名，依次类推。
- 层次树形结构的优点是各个组织在其内部可以自由地选择域名，只要保证该组织内域名的惟一性即可，而不必担心与其它组织内的域名相冲突。
- 我国的顶级域名管理中心是中国互联网络信息中心CNNIC, 网址为<http://www.cnnic.net.cn/>



- 中国互联网信息中心（CNNIC）作为.CN域名注册管理机构，不直接面对最终用户提供域名注册相关服务，域名注册服务将转由CNNIC认证的域名注册服务机构及其代理提供。
- 在CNNIC制定法律法规、监督代理商、查看申请域名手续。





中国互联网络信息中心
China Internet Network Information Center

关于CNNIC 下载中心 诚聘英才 站点地图

ENGLISH VERSION

首页 CN域名 中文通用域名 通用网址 IP/AS分配 信息服务 政策法规 国际研究 技术前沿

WHOIS查询

输入您想要查询的CN域名、
中文域名、通用网址信息：

查询

帮助

政策法规

- 中国互联网络域名管理办法
- 信息产业部关于中国互联网络域名体系的公告
- 中国互联网络信息中心域名注册实施细则
- 中国互联网络信息中心域名争议解决办法
- 通用网址注册办法
- 通用网址争议解决办法

更多

相关机构

网月

CN 域名



中国国家顶级域名，走向网络世界的通路，域名资源丰富，形式简洁。

我要注册 用户FAQ

更多

中文通用域名



含有中文文字的新一代域名，更适合中国人使用习惯的互联网门牌号码。

我要注册 用户FAQ

更多

通用网址



新兴的互联网地址资源，自然语言直达网站页面，便捷的网站推广工具。

我要注册 用户FAQ

更多

IP/AS 分配



加入CNNIC联盟，申请IP地址、自治系统号码及反向域名解析。

我要申请 用户FAQ

更多

CNNIC 动态与公告

更多



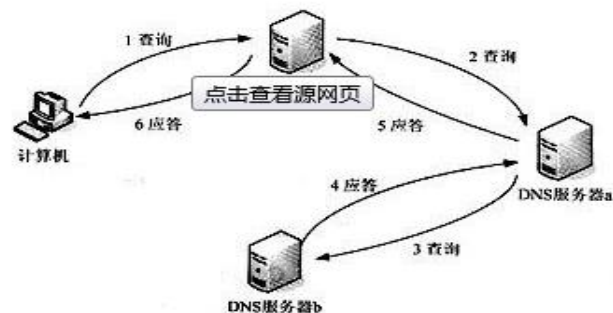
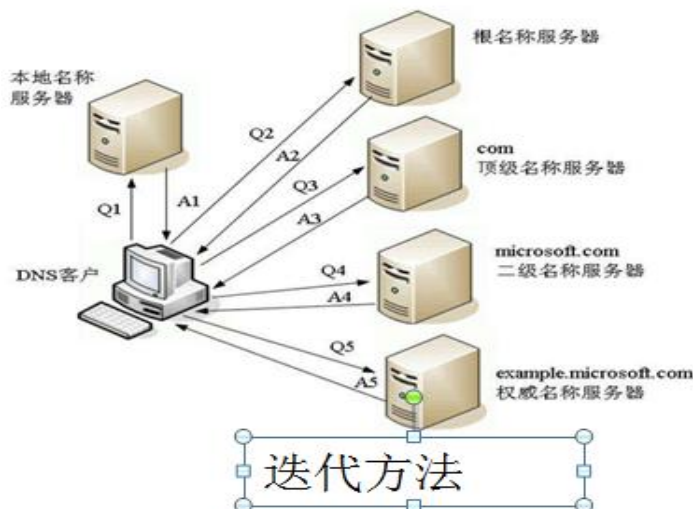
域名系统 DNS

1. 域名空间
2. 资源记录
3. 域名服务器
4. 域名解析

2. 资源记录

- 用户申请到域名之后，在域名服务器中通过资源记录来记录域名与IP的映射相关信息。
- 资源记录内容

Domain_name	Time_to_live	Type	Class	Value
-------------	--------------	------	-------	-------



递归方法



2. 资源记录

- 资源记录内容

Domain_name	Time_to_live	Type	Class	Value
-------------	--------------	------	-------	-------

- **Domain_name**: 资源记录所在的域名，它是作为查询的主关键字，具有唯一性，返回所匹配记录。
- **Time_to_live**: 资源记录的生存期，用32位整数来表示资源记录存活时间。



2. 资源记录

Domain_name	Time_to_live	Type	Class	Value
-------------	--------------	------	-------	-------

- Type: 资源记录类型，主要有下列记录类型：
 - A:** 一个主机的IP地址，32位整数，这是最重要的记录类型。
 - CNAME: 规范名，指示一个别名的规范名。
 - HINFO: 主机描述，指示一个主机的CPU和OS类型。
 - MX: 邮件交换，指示一个愿意接收特定域电子邮件的域名。
 - NS: 域名服务器，指示一个可信的域名服务器。
 - PTR: 指针，指向另一个域名空间部分的指针。
 - SOA: 认证开始，指示一个可信区域(Zone)的开始。



2. 资源记录

Domain_name	Time_to_live	Type	Class	Value
-------------	--------------	------	-------	-------

- Class: 信息类别, 对于Internet信息, 其值为IN; 对于非Internet信息, 则为其它值。
- Value: 它可以是数字或字符串, 其语义取决于资源记录类型。



2. 资源记录

■ 资源记录例子：

Domain_name	Time_to_live	Type	Class	Value
nwpu.edu.cn	86400	MX	IN	mail.nwpu.edu.cn
nwpu.edu.cn	86400	MX	IN	pop3.nwpu.edu.cn
www.nwpu.edu.cn	86400	HINFO	IN	Intel Linux
www.nwpu.edu.cn	86400	A	IN	192.202.200.150
ftp.nwpu.edu.cn	86400	A	IN	192.202.200.160
www.nwpu.edu.cn	86400	CNAME	IN	web.nwpu.edu.cn

其中，86400为24小时的秒数： $86400=24*60*60$ 。



域名系统 DNS

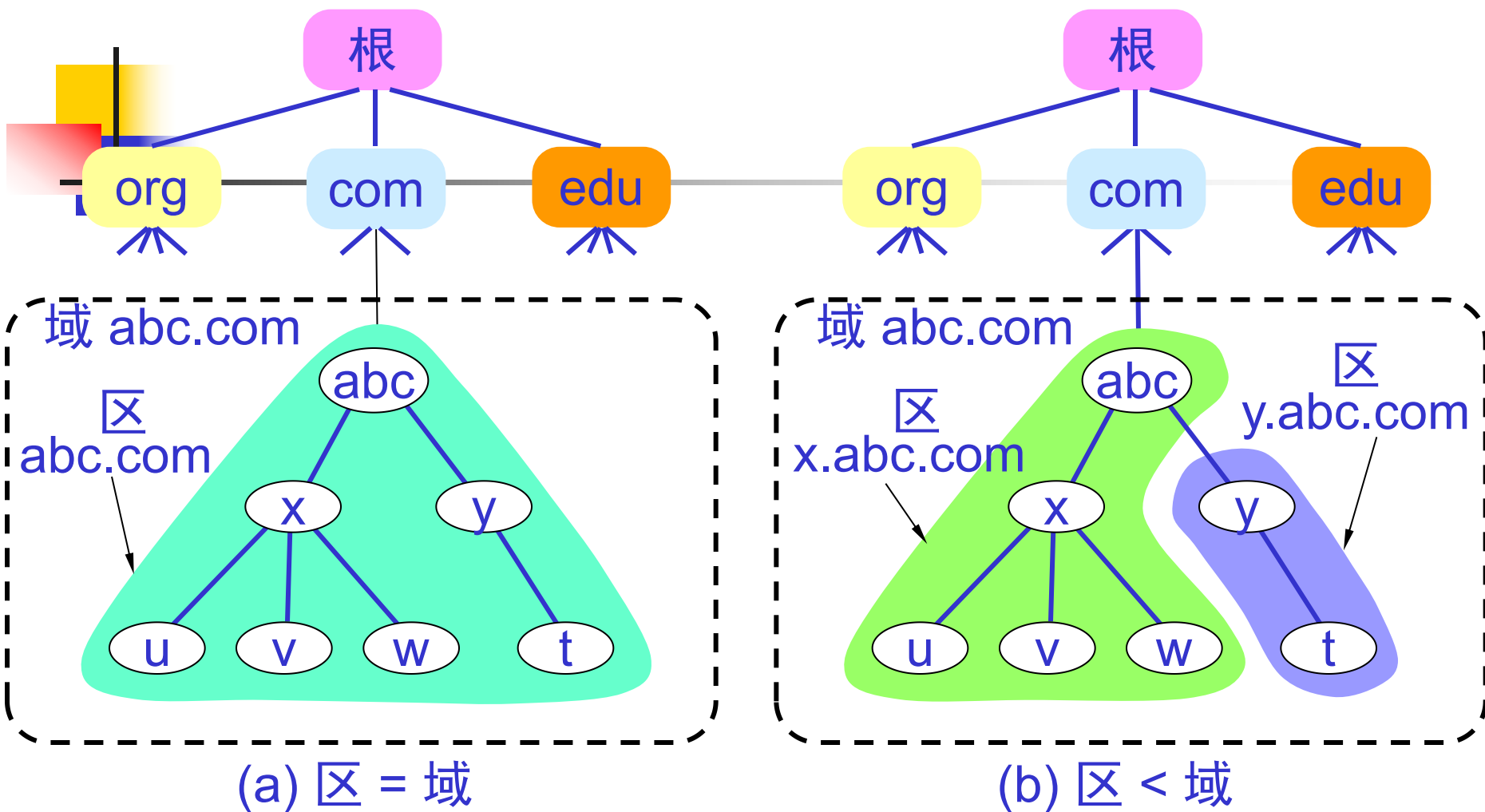
1. 域名空间
2. 资源记录
3. 域名服务器
4. 域名解析



3. 域名服务器

- 一个域名服务器负责管辖的（或有权限的）域名范围叫做**区(zone)**。
- 各单位根据具体情况来划分本单位域名服务器**管辖范围，可以划分几个区；**
- 每一个区设置相应的**权威域名服务器**，用来保存该**区**中的所有主机的域名到IP地址的映射。
- DNS 服务器的管辖范围原则上**不是以“域”为单位，而是以“区”为单位。**

区的不同划分方法举例



■ 区为单位

- 根域名服务器DNS管理所有一级：DNS.org, DNS.com, DNS.edu;
- 所有一级域名服务管理二级，如DNS.com管理DNS.abc.com



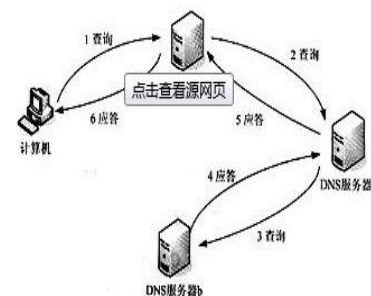
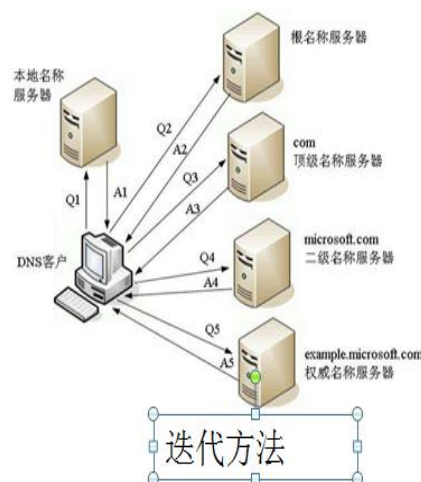
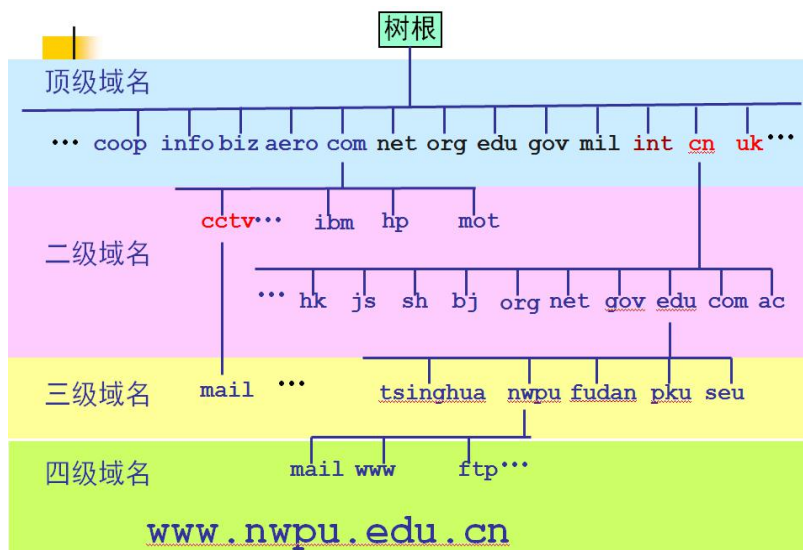
域名服务器有以下四种类型

- 根域名服务器
- 顶级域名服务器
- 权威域名服务器
- 本地域名服务器

根域名服务器

——最高层次的域名服务器——

- 根域名服务器是最重要的域名服务器；任意一个根域名服务器都知道**所有的顶级域名服务器的域名和IP地址**。
- 不管是哪一个**本地域名服务器**，若要对因特网上任何一个域名进行解析，只要自己无法解析，就**首先求助于根域名服务器**。



递归方法

根域名服务器

——最高层次的域名服务器——

- 在因特网上共有13 个不同 IP 地址的根域名服务器，它们的名字是用一个英文字母命名，从a 一直到 m（前13 个字母）。
- 负责运营和维护根域名服务器的组织大都在美国，根域名服务器大部分部署在美国、欧洲；
- 根域名服务器具体内容见[RFC 2870]

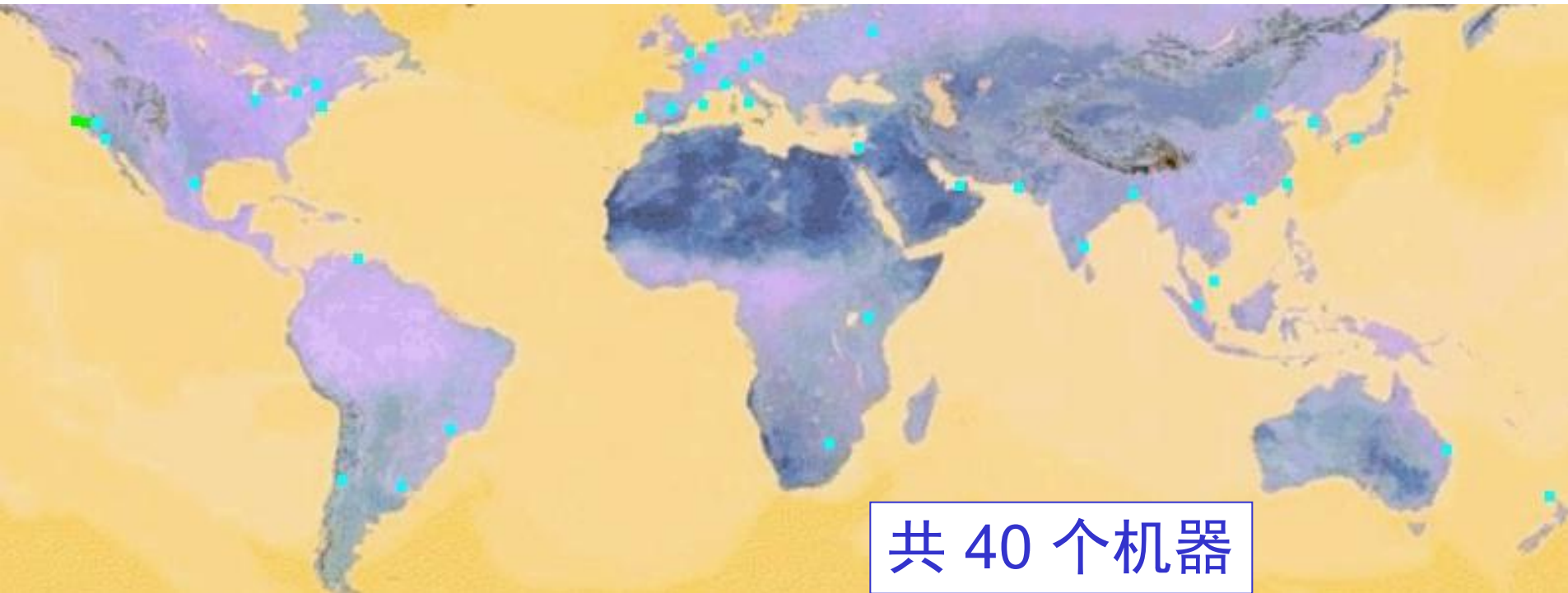




根域名服务器共有 13 套装置 (不是 13 个机器)

- 这些根域名服务器相应的域名分别是
a.rootservers.net
b.rootservers.net
...
f.rootservers.net (40个, 中国有三个: 北京、香港和台北)
...
m.rootservers.net
- 到 2006 年底全世界已经部署了123个根域名服务器, 分布在世界各地。
- 目的是为了更方便用户, 使世界上大部分 本地域名服务器都能就近 (任播技术) 找到一个根域名服务器。

举例：根域名服务器 f 的地点分布图

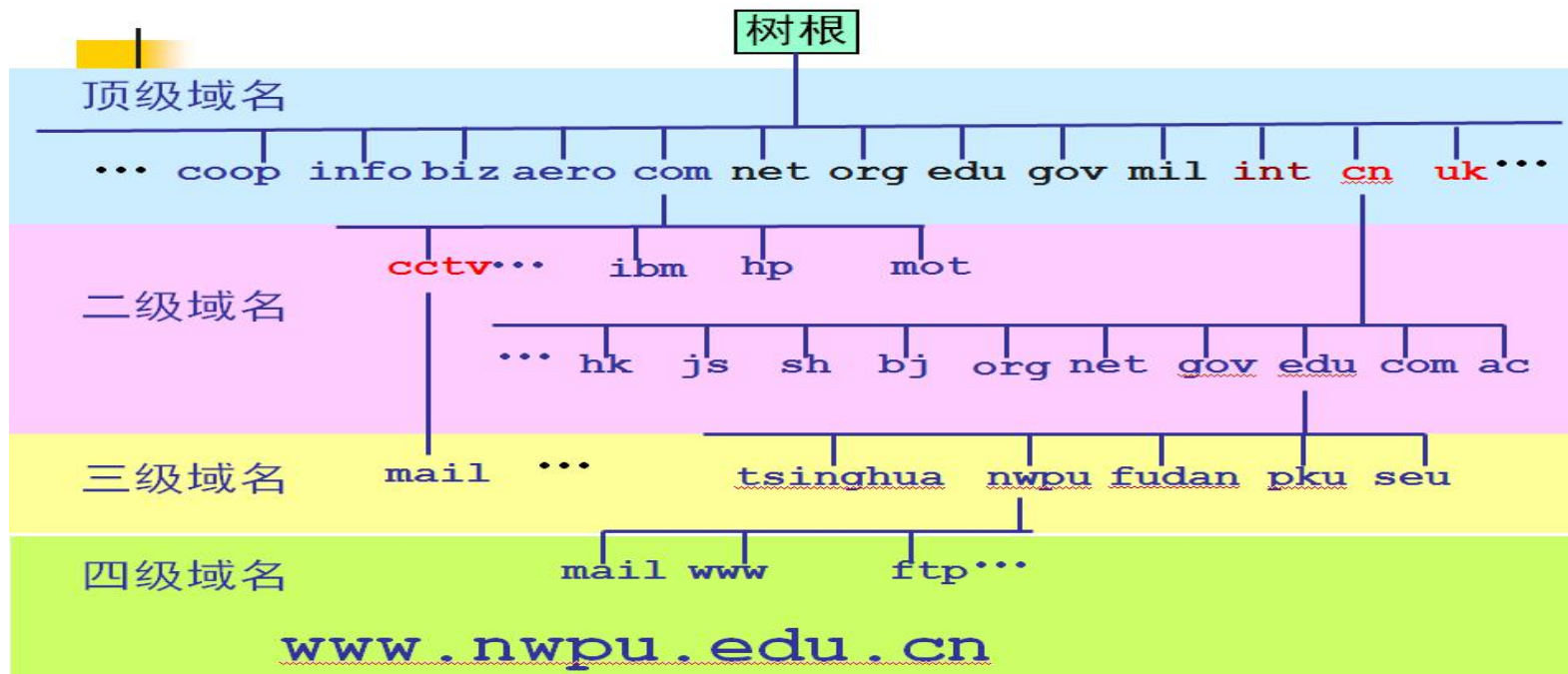


- 根域名服务器并不直接把域名转换成 IP 地址。
- 使用迭代查询时，根域名服务器把下一步应当找的顶级域名服务器的 IP 地址告诉本地域名服务器。

顶级域名服务器

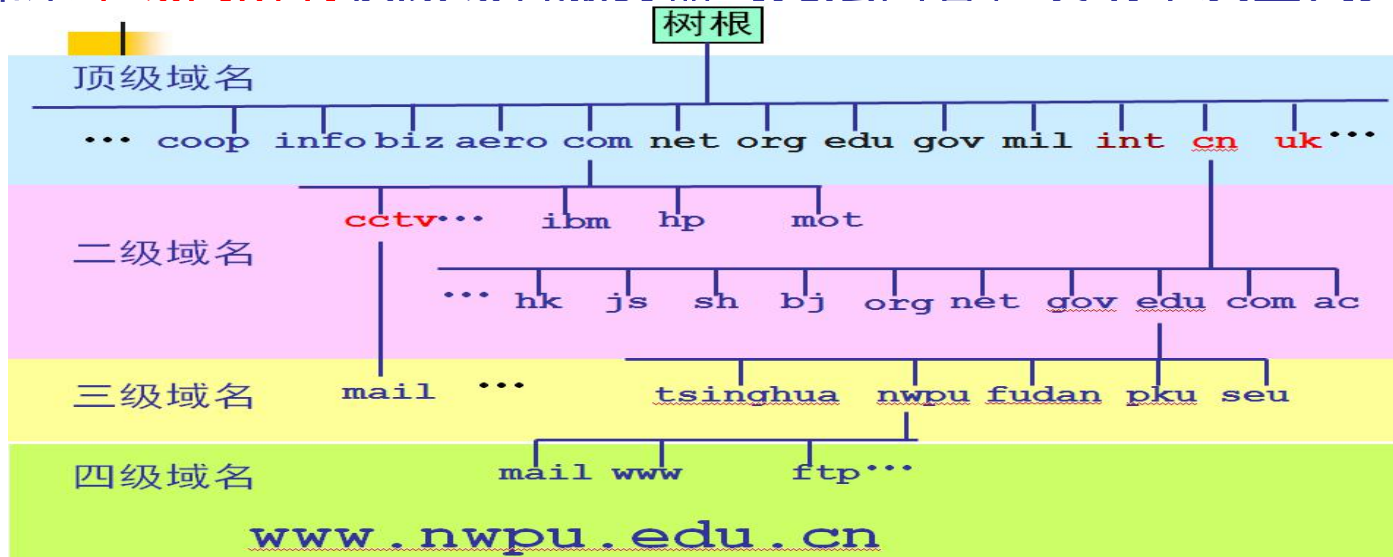
(即 TLD 服务器)

- 负责管理在该顶级域名服务器注册的所有二级域名服务器的域名和对应的IP地址。
- 当收到 DNS 查询请求时，就给出相应的回答（二级域名服务器的域名对应的IP地址）。



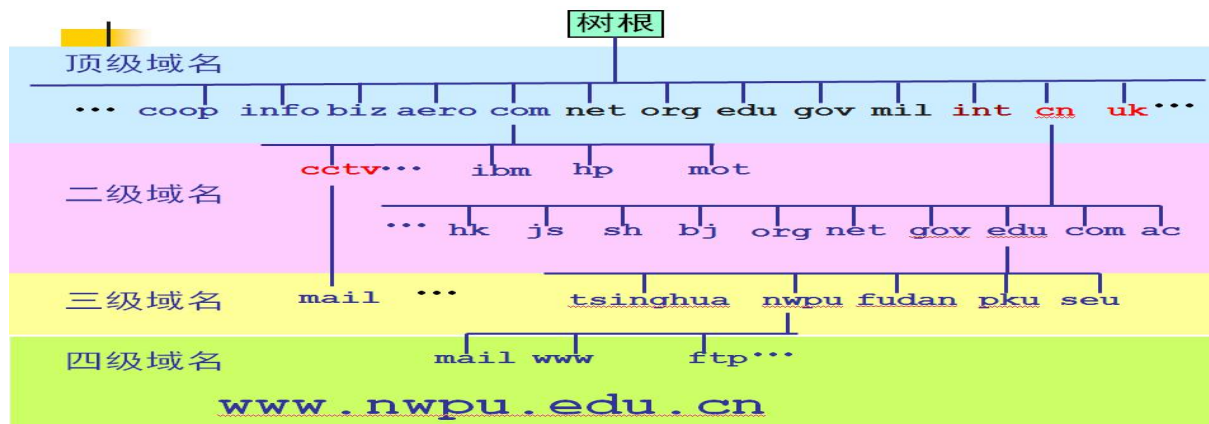
权威域名服务器

- 是负责一个区的域名服务器，知道具体的域名对应的IP地址，或本域内其他权威域名服务器的IP地址。
- 当一个权威域名服务器还不能给出最后的查询回答时（域名对应IP地址），就会告诉发出查询请求的 DNS 客户进程，下一步应当找哪一个本域内其他权威域名服务器。
- 如果本域内所有权威域名服务器均无法回答，表明本次查询失败。



本地域名服务器

- 本地域名服务器对域名系统非常重要。
- 当一个主机发出 DNS 查询请求时，这个查询请求报文就发送给本地域名服务器，相对别的网络PC来讲，该域名服务器是权威域名服务器。
- 每一个因特网服务提供者 ISP，或一个大学，甚至一个大学里的系，都可以拥有一个本地域名服务器；
- 本地域名服务器有时也称为默认域名服务器，距离本地用户最近。
- 本地PC和所要查询的域名在一个ISP网络内，则该本地域名服务器即可完成任务，不需要其他域名服务器。





提高域名服务器的可靠性

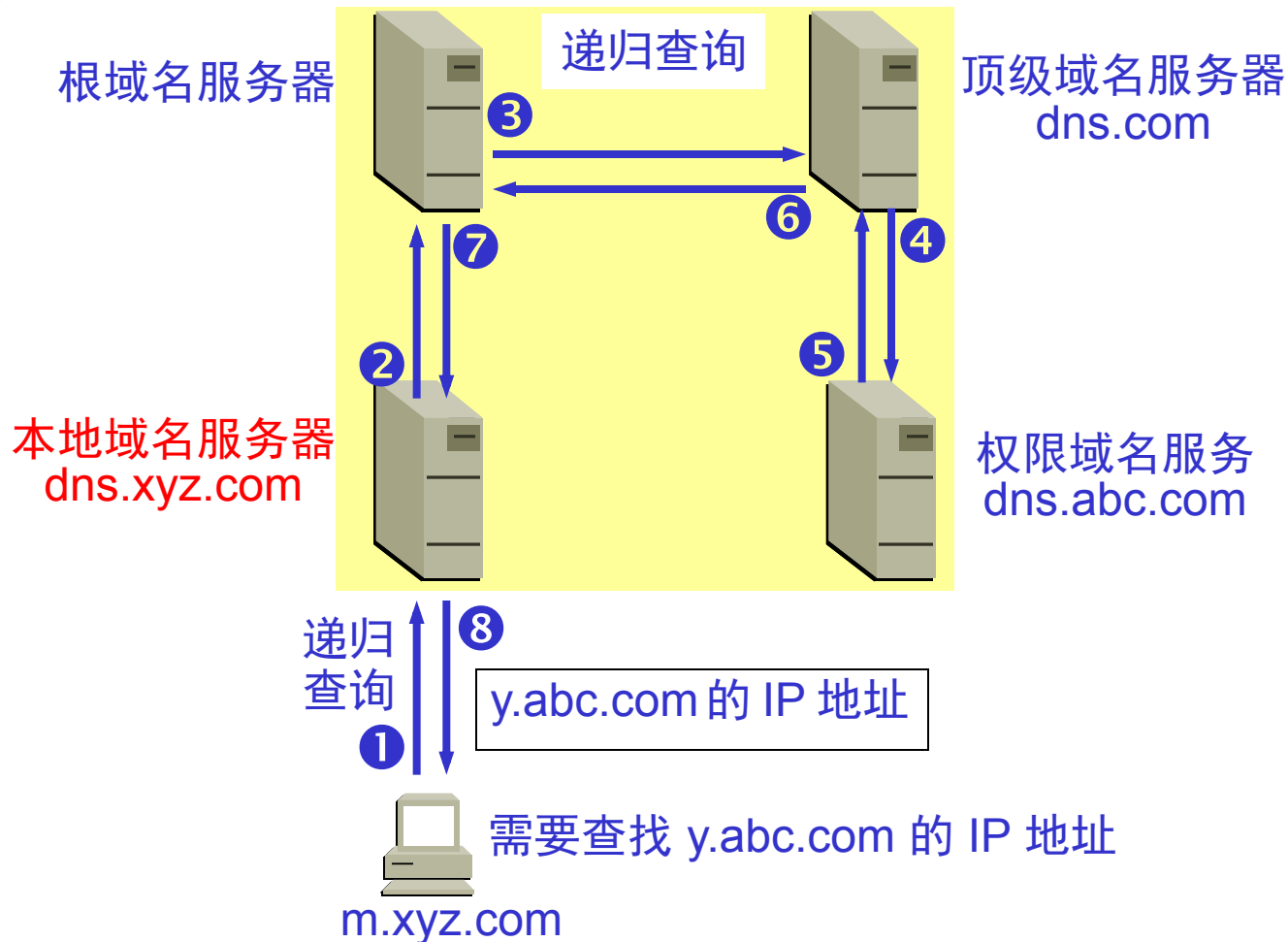
- 所有DNS 域名服务器时同时部署多个，其中的一个是主域名服务器，其他的是辅助域名服务器。
- 当主域名服务器出故障时，辅助域名服务器可以保证 DNS 的查询工作不会中断。
- 更新数据记录只能在主域名服务器中进行，主域名服务器定期把数据推送到辅助域名服务器；这样就保证了主和辅助域名服务器之间数据记录一致性。



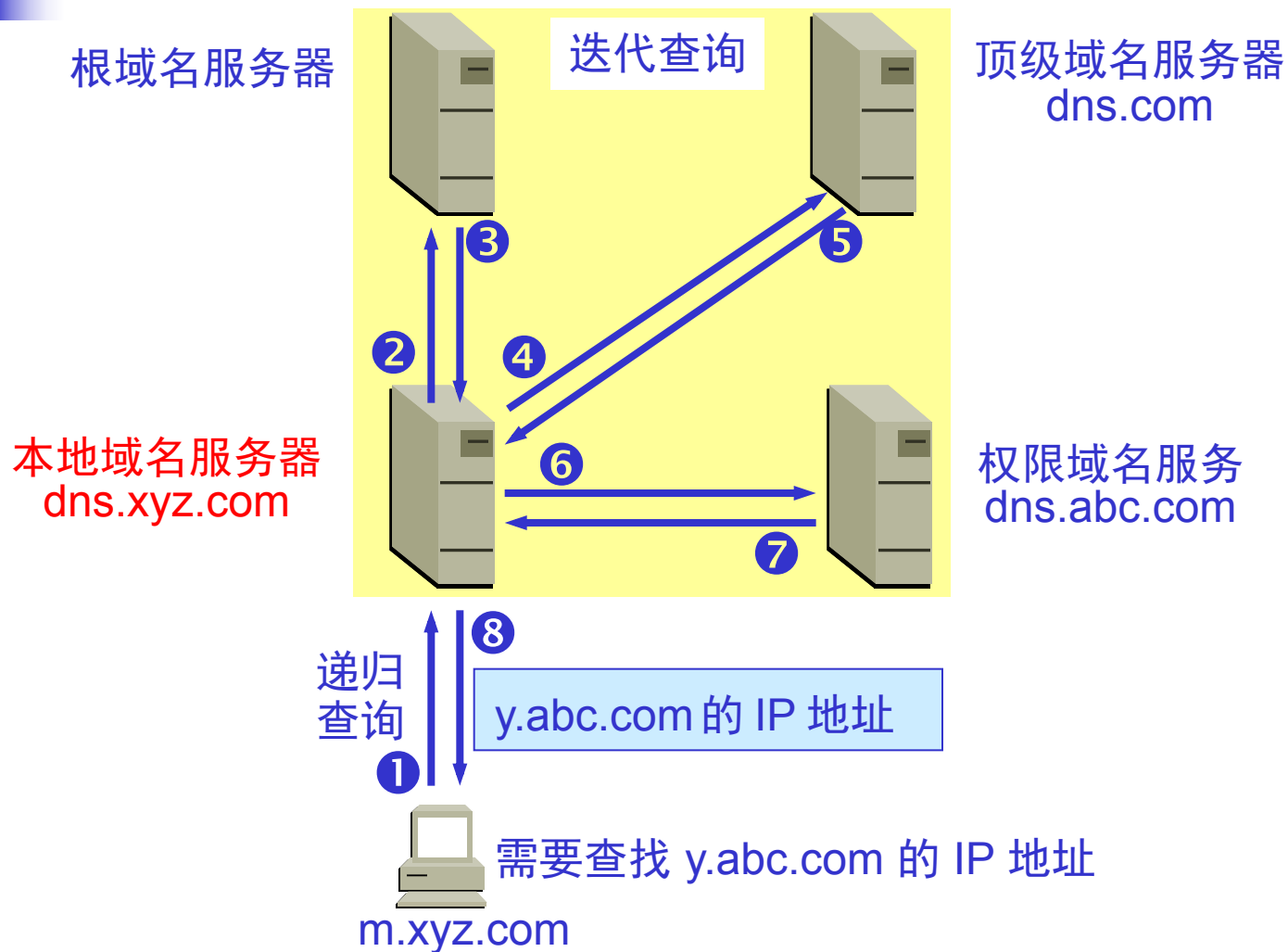
域名系统 DNS

1. 域名空间
2. 资源记录
3. 域名服务器
4. 域名解析方法

本地域名服务器采用递归查询 (比较少用)



本地域名服务器采用迭代查询



域名的高速缓存

- 每个主机及域名服务器都维护一个DNS高速缓存，存放最近获得域名到IP地址映射的记录。
 - 如果本地域名服务器已经缓存了域名对应IP地址，可大大减轻根域名服务器负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少，提高查询效率。
 - 如果其他域名服务器缓存了查询结果，可提高查询效率。

```
管理员: C:\Windows\system32\cmd.exe
A <主机>记录 . . . . : 192.35.51.30

记录名称. . . . . : b.gtld-servers.net
记录类型. . . . . : 1
生存时间. . . . . : 79
数据长度. . . . . : 4
部分. . . . . : 其他
A <主机>记录 . . . . : 192.33.14.30

www.cntv.cn
-----
记录名称. . . . . : www.cntv.cn
记录类型. . . . . : 5
生存时间. . . . . : 26
数据长度. . . . . : 8
部分. . . . . : 答案
CNAME 记录 . . . . : g1.ctc.cctvedn.net.lxdns.com

query.aliyun.com
-----
记录名称. . . . . : query.aliyun.com
记录类型. . . . . : 5
```

```
C:\>ipconfig /flushdns

Windows IP 配置

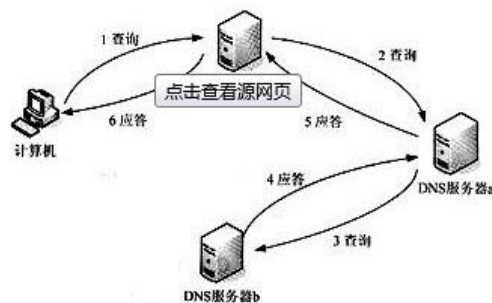
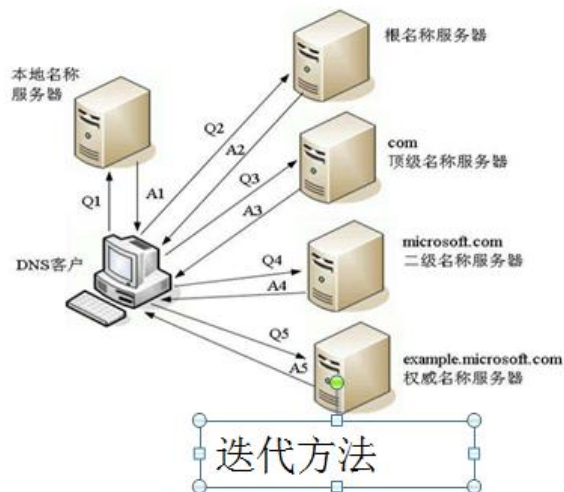
已成功刷新 DNS 解析缓存。
```

Dos>ipconfig /flushdns

Dos>ipconfig /displaydns

域名的高速缓存

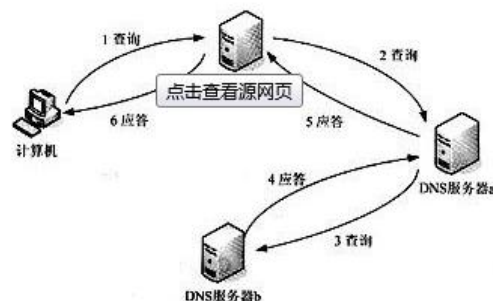
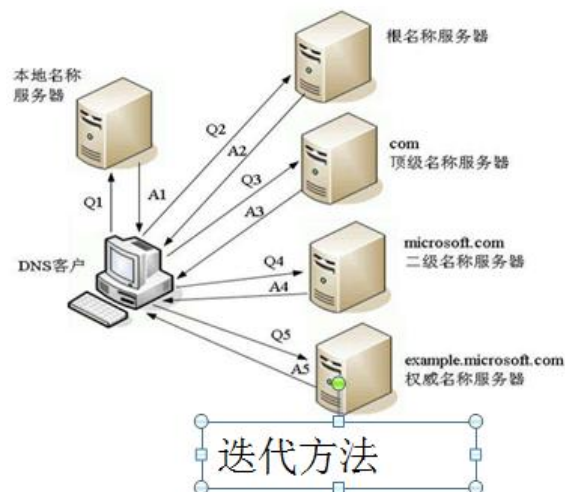
- 尽管域名到IP地址映射基本保持不变，为保持高速缓存内容正确，域名服务器应为缓存每项记录设置生命期（例如，每个记录存放两天）；如果过期则删除缓存相应记录；
- 当域名服务器刚从缓存中删除一项记录，又被请求查询该项信息时，则必须从该域名服务器开始，重新按照“递归”或“迭代”方法查询。



递归方法

域名的高速缓存

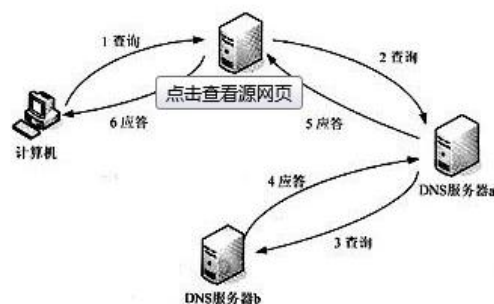
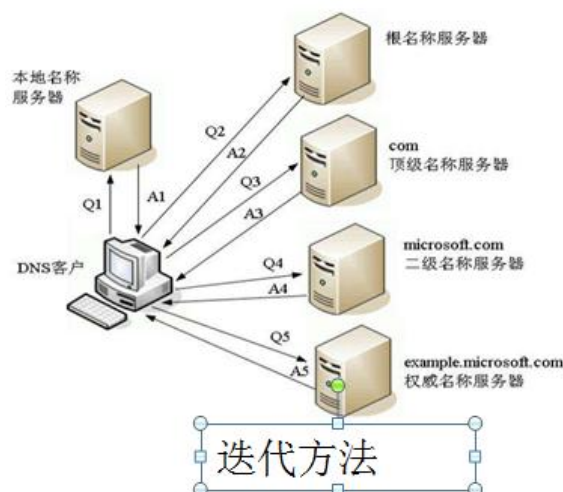
- 当权威域名服务器回答一个查询请求时，在响应中都指明绑定有效生命期值；增加此时间值可减少网络开销，而减少此时间值可提高域名查询的准确性。
- 各级域名服务器存在DNS高速缓存，主机也存在；用于缓存最近获得的域名到IP地址的映射关系。

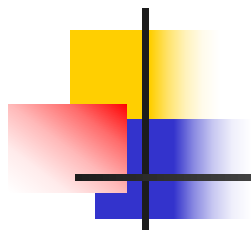


递归方法

域名的高速缓存

- 高速缓存的存在，给黑客进行网络攻击提供了方便
 - 黑客可假冒合法域名服务器发送虚假的域名到IP地址映射应答，并被接收者缓存错误记录；
 - 黑客可利用恶意代码直接修改高速缓存中域名到IP地址映射信息。





问题：假设一个用户在域名为
ncti.xjtu.edu.cn的计算机上发出查
询www.nisi.nwpu.edu.cn域名请求, 请
分别用迭代法和递归法解释域名查询
流程?



DNS查询顺序

- (1) “系统所在盘
:\Windows\system32\drivers\etc\hosts文件
- (2) 查找DNS高速缓存
 - ipconfig /displaydns
 - Ipconfig /flushdns
- (3) 查找本地DNS服务器
- (4) 根DNS服务器（迭代或递归）



作业：递归法

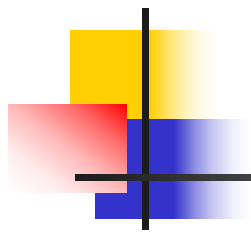
- 假设一个用户在域名为ncti.xjtu.edu.cn的计算机上发出查询“www.nisi.nwpu.edu.cn”的命令，则DNS的工作过程如下：
 - 用户向本地域名服务器发出请求，查询www.nisi.nwpu.edu.cn的地址；
 - 本地域名服务器向根域名服务器(DNS)发出查询www.nisi.nwpu.edu.cn地址请求；
 - DNS向DNS.cn发出查询www.nisi.nwpu.edu.cn地址的请求；
 - DNS.cn向DNS.edu.cn发出查询www.nisi.nwpu.edu.cn地址请求；
 - DNS.edu.cn向DNS.nwpu.edu.cn发出查www.nisi.nwpu.edu.cn地址的请求；
 - DNS.nwpu.edu.cn向DNS.nisi.nwpu.edu.cn发出查www.nisi.nwpu.edu.cn地址的请求；
 - DNS.nisi.nwpu.edu.cn域名服务器发送应答，沿相反路径，到达本地域名服务器，再发送给用户。



作业：迭代法

■ 假设一个用户在域名为ncti.xjtu.edu.cn的计算机上发出查询“www.nisi.nwpu.edu.cn”的命令，则DNS的工作过程如下：

- 用户向本地域名服务器发出请求，查询www.nisi.nwpu.edu.cn的地址；
- 本地域名服务器向根域名服务器DNS发出查询www.nisi.nwpu.edu.cn地址的请求；根域名服务器返回给本地域名服务器一个IP地址，指向DNS.cn域名服务器
- 本地域名服务器向DNS.cn发出查询www.nisi.nwpu.edu.cn地址的请求；DNS.cn返回给本地域名服务器一个IP地址，指向DNS.edu.cn域名服务器；
- 本地域名服务器向DNS.edu.cn发出查询www.nisi.nwpu.edu.cn请求；DNS.edu.cn将DNS.nwpu.edu.cn域名服务器IP地址返回给本地域名服务器；
- 本地域名服务器向DNS.nwpu.edu.cn发出查询www.nisi.nwpu.edu.cn请求；DNS.nwpu.edu.cn将DNS.nisi.nwpu.edu.cn域名服务器IP地址返回给本地域名服务器；
- 本地域名服务器向DNS.nisi.nwpu.edu.cn发出查询www.nisi.nwpu.edu.cn请求；DNS.nisi.nwpu.edu.cn将www.nisi.nwpu.edu.cn域名对应的IP地址返回给本地域名服务器；
- 本地域名服务器将该IP地址返回给用户DNS客户进程。



结束！