第7章　网络应用

教材目录

- **域名服务（7.1）**
  - 主机名和域名
  - 域名注册和管理
  - 域名解析服务
  - Internet域名和URL
- 传统应用（7.2）
  - FTP
  - Email
  - WWW

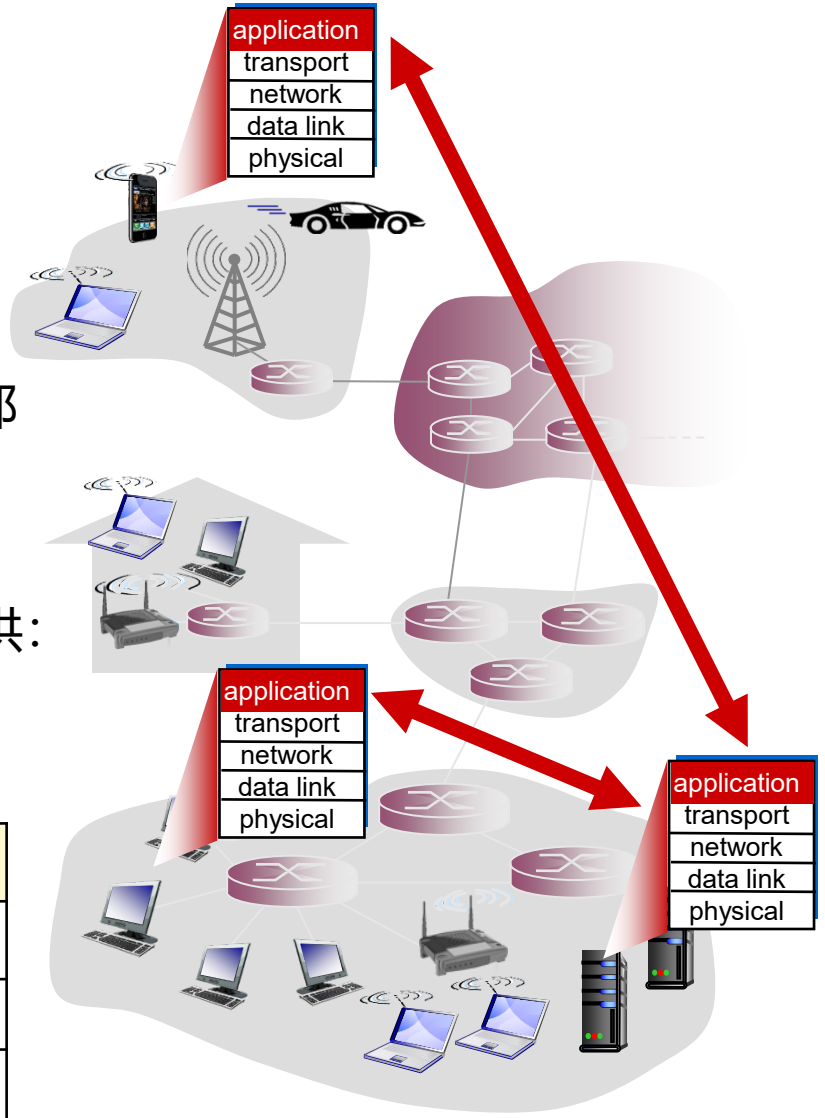
主要内容

- 应用层概述：socket地址(IP地址+端口号)
- DNS (Domain Name Service)
  - 域名解析服务
  - 域名空间
  - 域名服务器
  - 资源记录
  - 域名解析过程
  - DNS协议

应用层

- 层次模型的最高层
- 端系统中运行了各种网络应用，为用户提供网络应用服务
- 网络核心设备处并不需要实现应用层协议
- 中间件（Middleware，比如防火墙、负载均衡设备和代理等）有时会被部署以提升应用的性能
- 应用层为一些常用的网络应用定义了通用的协议，比如HTTP、SMTP等
- 应用层建立在运输层之上，使用运输层提供的服务，运输层为端系统提供：
  - 尽力递交的不可靠的数据传输服务UDP
  - 可靠的数据传输服务TCP

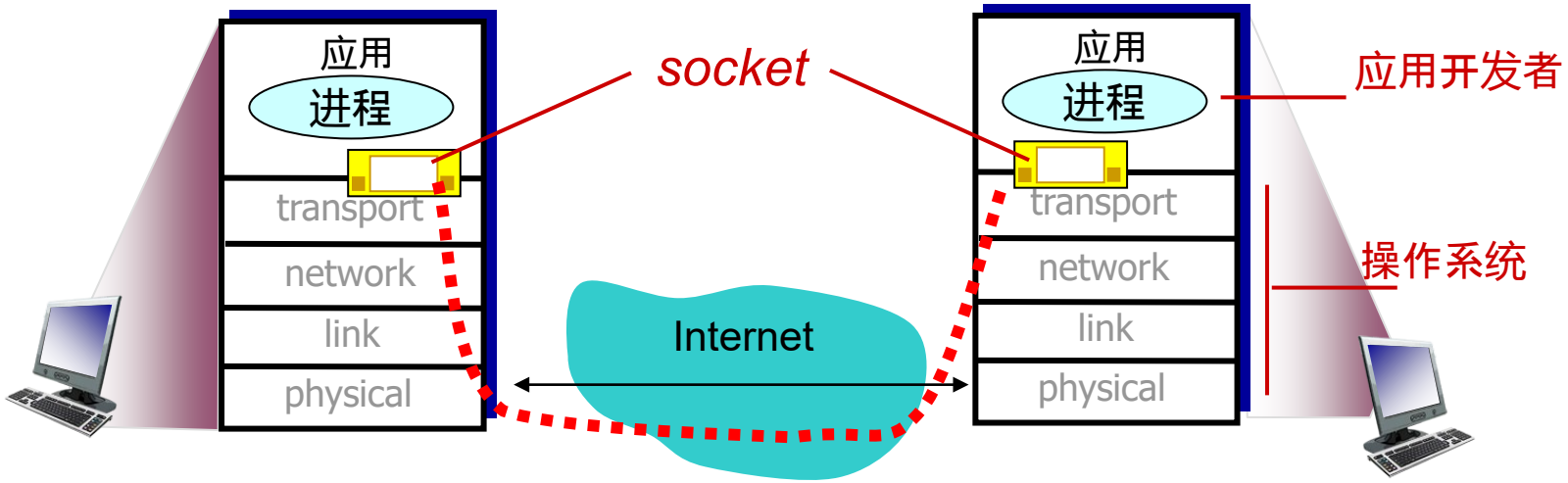
应用	应用层协议	底层运输层协议
电子邮件	SMTP/POP3/IMAP	TCP
远程终端访问	Telnet, SSH	TCP
Web	HTTP	TCP
文件传输	FTP	TCP
文件传输	TFTP	UDP
流媒体	HTTP, RTP	TCP or UDP
IP电话	SIP, RTP, 厂商私有(Skype)	TCP or UDP



应用层:Socket

- 应用层协议一般采取**客户-服务器C/S(Client-Server)**架构
  - 客户方主机的网络应用程序（进程）主动发送请求给服务方主机的网络应用程序（进程），请求对方提供相应的服务
- 进程通过Socket发送和接收消息
  - 一个进程可以同时使用多个Socket
  - 每个Socket通过IP地址+端口号唯一标识
  - 一条TCP连接或者UDP会话对应着本机上的Socket和远方的Socket之间建立的一条逻辑通道 (协议TCP或UDP，本地IP地址，本地端口号，远端IP地址，远端端口号

- IP地址：哪个网络接口（网卡）
- 端口号：哪个进程



网络层：IP地址

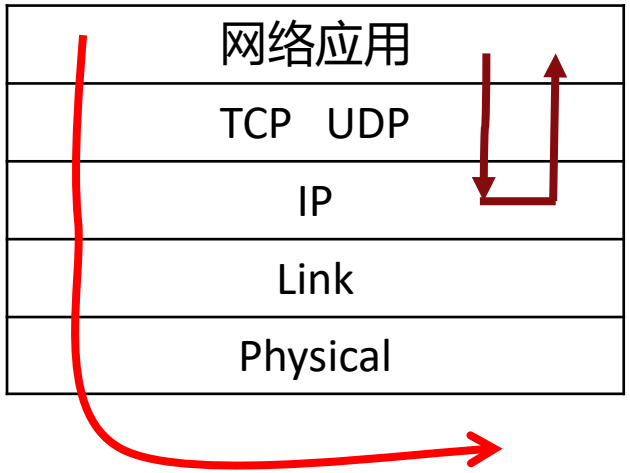
- 每个节点(主机和路由器)的网络接口(网卡）都有一个IP地址：**ID + Locator**
  - 唯一标识连接到IP网络的接口
  - 描述该接口所在的位置（网络）
    - IP地址分为网络号和主机号，网络号标识某个"物理"网络，主机号标识该网络中的主机
    - 路由时只需了解如何到达接口所在的(物理)网络，而不必了解该网络的每一台主机
    - 第二层物理网络可以直接递交给其所在物理网络中的其他节点
    - 需要将IP地址映射为物理地址→ARP协议
      - 网卡地址为48比特的整数，描述时一般将每个字节转换为十六进制，中间以-或:隔开
- 目前的Internet(采用IPv4协议)使用的IP地址为**32比特的整数**，采用**点十进制方法描述**
  - 每个字节转换为十进制数字，中间以.隔开

11001010	01111000	11100000	01010001
ca	78	e0	51
202	120	224	81

ping 0xca78e051
ping 202.120.224.81

IP地址：回环地址(loopback address)

- 一台主机可以有多个网络接口，每个接口有不同的IP地址
- **127.0.0.1**(实际上127.x.x.x)为回环(loopback)地址，对应名字localhost
  - 任何发送到该地址的IP分组不会发送到实际的网卡上，而是由IP模块递交给高层相应的协议(TCP或者UDP)模块
  - 可测试协议栈，可用于主机内不同进程间的通信




```
demo@mars2:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:e9:b7:0f
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::e6bc:e568:cc49:4197/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4796 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2179 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6010324 (6.0 MB)  TX bytes:164340 (164.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:410 errors:0 dropped:0 overruns:0 frame:0
          TX packets:410 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39299 (39.2 KB)  TX bytes:39299 (39.2 KB)
```

- Windows命令：
  - **ipconfig: 查看地址信息，/all 查看详细信息，/displaydns查看DNS缓存**
  - route/netstat/arp
- Linux的ip命令提供了查看和修改网络配置的功能，用于替代ifconfig/arp/route等
  - ip link: 网络接口
  - **ip address: 网络接口IP地址**
  - ip route: 路由表，替代route
  - ip neighbor: 邻居，替代arp

TCP/UDP：端口号（port number）

- 进程通过socket使用底层(TCP/UDP)提供的服务，端口号(16比特整数）表示对应着上层的哪个进程
- 注意TCP/IP协议中IP地址和端口号都是采用**网络字节顺序**，即大端(big-endian)顺序
  - 大端指的是多字节整数存储或传输时高字节（MSB）在前的方式。小端为低字节在前
  - Intel X86/ARM CPU采用小端存储

小端	50	00	0x0050=80
大端	50	00	0x5000=20480

- RFC 6335： BCP，给出了服务名(方便记忆端口号)和端口号的分配建议，建议将端口分为3个部分

系统端口, well-known (常需要超级用户权限)	[0, 255]	通用网络应用, IANA分配	HTTP:80, SMTP 25, SSH 22
	[256, 1023]	早期表示厂商应用， IANA分配	https 443 rtsp 554
用户端口或Registered端口	[1024,49151]	IANA分配	X-Window: 6000, RDP: 3389
动态端口	[49152-65535]	用户可自由使用	

- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
  当前IANA分配的端口号与服务名的映射
- /etc/services 操作系统的服务映射文件

主要内容

- 应用层概述：socket地址(IP地址+端口号)
- DNS (Domain Name Service)
  - 域名解析服务
  - 域名空间
  - 域名服务器
  - 资源记录
  - 域名解析过程
  - DNS协议

DNS(Domain Name System) 域名系统

- Internet的名字和地址：
  - 网卡地址(MAC地址）：标识某一块网卡
  - IP地址：32比特整数，标识Internet上的某个主机，ID+Locator
  - 主机名字（域名）：方便记忆的一系列字符

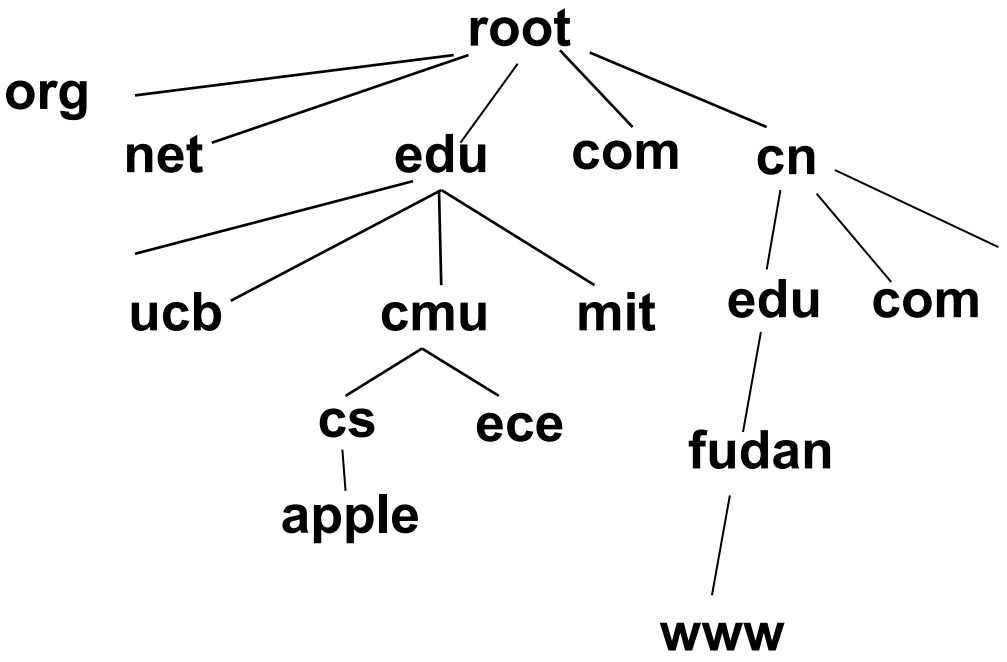
`gethostbyname(name)`
`gethostbyaddr(address)`

```
/* DNS host entry structure */
struct hostent {
   char    *h_name;        /* official domain name of host */
   char    **h_aliases;    /* null-terminated array of domain names */
   int     h_addrtype;     /* host address type (AF_INET) */
   int     h_length;       /* length of an address, in bytes */
   char    **h_addr_list;  /* null-terminated array of in_addr structs */
};
```

- 名字和地址之间的映射：
  - ARP：IP地址→网卡地址
- DNS: [1987年 RFC 1034/1035]
  - **域名与值（如IP地址）之间的映射**
  - **主机别名**：一个主机可以有多个名字，其中一个称为canonical名
  - 负载均衡：一个主机可以有多个IP地址，轮流返回其中某一个IP地址，或返回IP地址列表，轮流调整IP地址列表顺序
  - 目录服务：
    - 属于某个域的一个或者多个**邮件服务器**
    - 属于某个域的一个或者多个某种类型应用的服务器以及其他相关信息

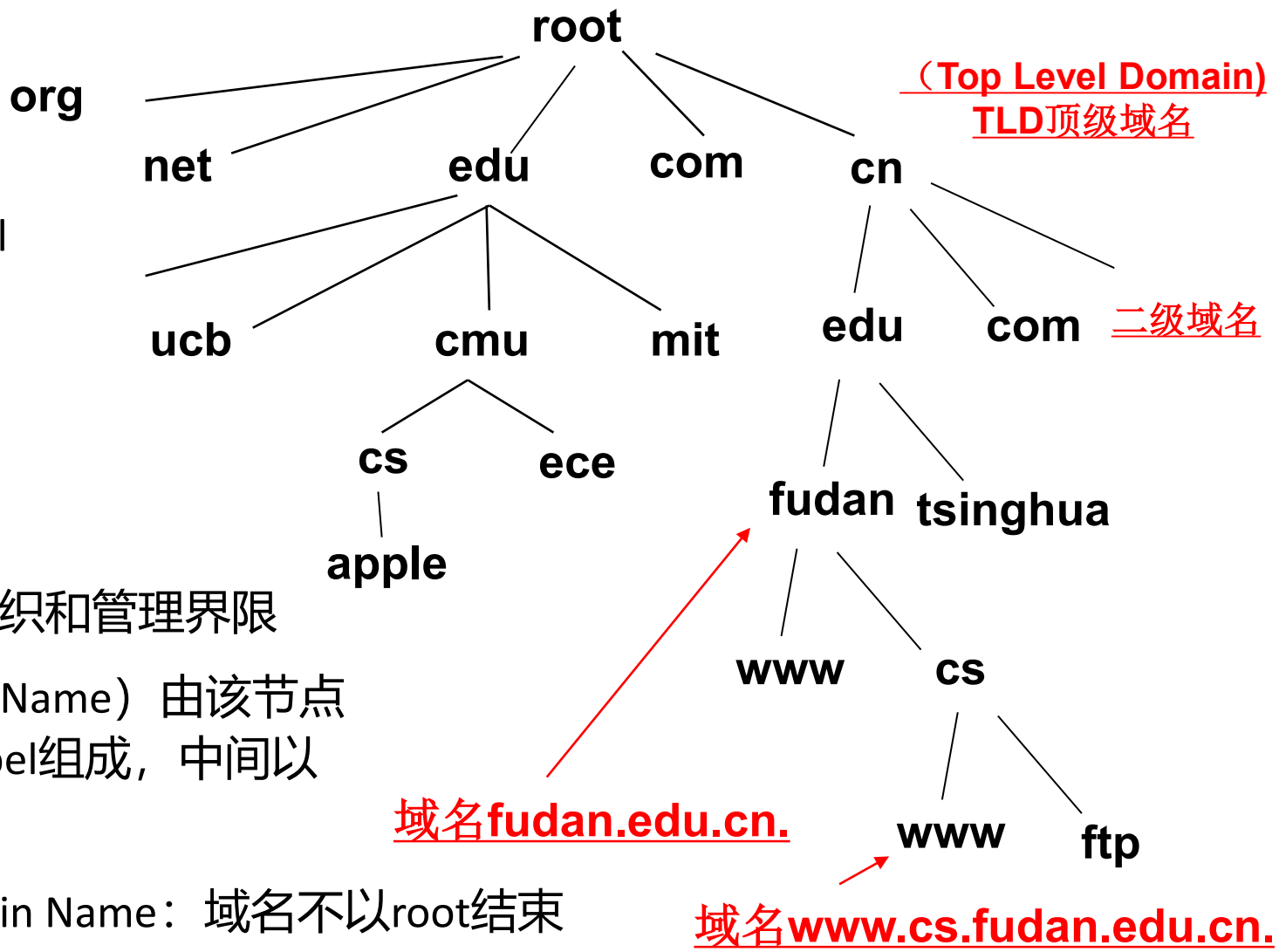
DNS历史：从主机文件→层次域名空间

- 平面(Flat)名字空间：
  - NIC(Network Information Center)维护一个"hosts.txt"文件，记录名字与IP地址的映射，主机通过FTP协议下载到本地 /etc/hosts.txt
  - 平面名字，命名空间不足
  - 缺乏伸缩性(scalability)，要求采用集中式管理和维护，会有网络通信瓶颈和可靠性问题
  - 静态名字映射，修改映射后将其分发到各个主机需要一定的时间
- 层次(hierarchical)名字空间
  - 采用域名树的方式描述名字空间，方便、易扩展
  - 只要保证节点下面的子节点的名字不同就可以了
  - 可以采用**分布式方法来维护整个名字空间**，易管理和维护，有较好的可靠性和效率
  - **不需要原子性和强一致性**，允许域名映射有暂时不一致的情况



域名层次结构

- 域名树最多128层，第0层为root
- 标记(Label):树中的每个节点有一个label
  - 最多63个字符，**大小写无关**
  - root为空字符串
- 域名：每个节点有一个域名
  - 域名最长255个字节
  - 域名定义的不是地理界限，而是组织和管理界限
- 绝对域名FQDN（Fully Qualified Domain Name）由该节点的label开始一直到root为止的一系列label组成，中间以dot(.)分隔
- 相对域名PQDN(Partially Qualified Domain Name：域名不以root结束
  - 常用于解析与当前主机在同一个域下面的名字
  - 需要提供域名后缀suffix
  - 解析名字name时：会尝试解析name、 name.suffix




```
# /etc/resolv.conf
nameserver 202.120.224.26
search fudan.edu.cn
```

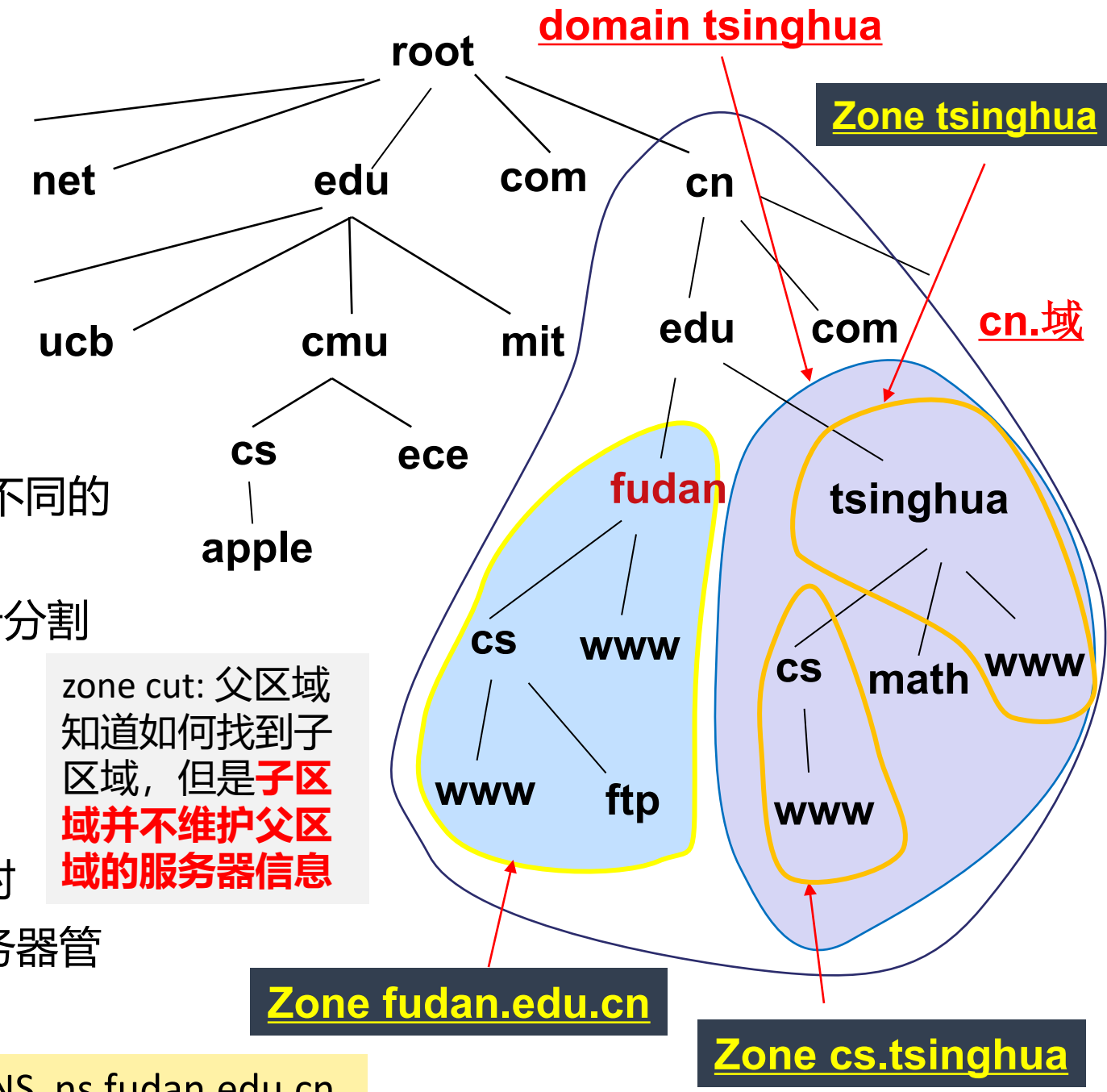
域名国际化

拓展的内容

- Internationalized Domain Names in Applications (IDNA) (RFC 5890, RFC 5891, RFC 3492)
- 域名系统本身不作任何修改
- 网络应用加入国际化域名支持
  - 将域名中包含了非7-bit ASCII字符（比如中文字符）的Label编码成7-bit ASCII字符，称为ACE编码(ASCII Compatible Encoding)
    - ACE前缀为xn–
    - RFC 3492描述了Punycode，将Unicode字符转换为ASCII
  - 中国.cn进行ACE编码后为 xn--fiqs8s.cn

域名的维护：域名服务器

- 域Domain：**domain fudan.edu.cn**
  - 域名树的一颗完整子树
  - 域的名字为该子树的**根节点的域名**
- 整棵域名树采用分布式方式管理
  - DNS服务器管理树的一部分
  - 首先将整棵树下的第一层子树分割交给不同的(TLD)DNS服务器管理
  - TLD域名服务器可将其管理的子树进一步分割授权给更下一层的域名服务器管理
  - 域名服务器管理的基本单位为区域 Zone:
    - 修剪的子树
    - 由域名服务器管理区域中名字的映射
    - 子树的某些分支授权给其他域名服务器管理，通过NS资源记录来定义



zone cut: 父区域知道如何找到子区域，但是**子区域并不维护父区域的服务器信息**

fudan.edu.cn NS ns.fudan.edu.cn

域名服务器

- 主和从域名服务器（Primary and Secondary Name Server）
  - 一个区域一般建议至少由两个以上域名服务器管理
  - 负载均衡和提高可靠性
  - 主域名服务器：维护区域的域名映射
  - 从域名服务器：从主服务器获得映射的拷贝（replica）
  - 主和从域名服务器都是该区域的**权威服务器** (authoritative server），拥有最权威和最新的映射
  - 一个DNS服务器可以充当多个区域的主或者从服务器
- 根域名服务器(Root Server): 有关根域名服务器的信息可以访问 www.root-servers.org
  - 负责管理root区域，将root域下面的所有子树授权给下一级的TLD服务器
  - 13个根服务器 {a-m}.root-servers.net，分布在不同的国家，由12个不同的组织维护
  - 这些根服务器在全球还有许多Mirrors，目前总共有1751个instance
    - 采用IP Anycast技术：与根服务器有相同的IP地址，通过BGP路由协议实现
    - DNS请求会路由到最近的根服务器或者根服务器的镜像
  - 每个域名服务器一般都知道根服务器的名字和IP地址的映射(root.hints, named.ca等文件)
  - 根域名服务器平均每天有约100 billion次查询，来源于 https://rssac002.root-servers.org/

Top-Level Domain顶级域名

- 通用域 "generic domains“ (gTLD)：表示域名的类别

Label	描述	Label	描述
com	商业组织	aero	航空
edu	教育组织	biz	商业或公司
org	非盈利组织	coop	合作组织
net	网络提供者	info	信息服务提供者
mil	军队	museum	博物馆
gov	政府	name	个人
int	国际组织	pro	职业组织

根和顶级域名等信息可访问：
https://www.iana.org/domains

中国互联网信息中心CNNIC，China Internet Network Information Center
负责管理.cn域名
https://www.cnnic.cn

- 国家域 "country code"(ccTLD)：表示国家和地区的代码
  - 一般两个字母，比如uk、us、de、fr和cn等
  - 第二级进一步可采取类别和地区label的方式来描述
- arpa (address and routing parameter area): 为Internet基础设施服务，https://www.iana.org/domains/arpa
  - in-addr.arpa用于反向域名解析（如IP地址→域名）
- 目前有超过1500个TLD

区域信息：资源记录(Resource Record)

- 区域的主服务器负责维护区域信息，由多条资源记录组成
  - 资源记录RR：**(name, ttl, class, type, value)**
  - 类(Class)：用于Internet时取值为IN
  - TTL(Time to Live)：该记录在缓存时的有效期(秒)，86400表示1天
  - DNS响应以RRset(资源记录集）的形式描述，由name/class/type相同，但是value不同的RR组成
- Type=SOA
  - name：域(区域)
  - value：start of authority
  - 区域的第一个RR
  - 关于区域的相关信息以及主从服务器之间保证区域信息同步的相关信息

```
$ dig fudan.edu.cn soa
;; ANSWER SECTION:
fudan.edu.cn.        3600    IN      SOA     ns.fudan.edu.cn. root.ns.fudan.edu.cn. 2000000547 18000 14400 3600000 86400
```

- 主域名服务器: ns.fudan.edu.cn
- 域名管理者：root@ns.fudan.edu.cn
- 序列号(serial)： 2000000547，永远递增，判别是否有修改

- 刷新间隔(refresh)：18000，表示5个小时同步一次
- 重试间隔(retry)：14400，表示无法同步时每4个小时重试
- 过期间隔(expire)：3600000，表示1000小时后还不能同步时，放弃
- 缺省TTL：86400，TTL的缺省值为24小时

区域信息：资源记录(Resource Record)

- Type=NS
  - **name**：域(区域)
  - **value**：管理该域的权威服务器
- type=A(或者AAAA)
  - **name**：主机名
  - **value**：IPv4地址(或IPv6地址)
- Type=CNAME “canonical name”
  - name：别名
  - value：正式的名字
- Type=MX，无mx记录时使用A/AAAA
  - name: 域
  - value: 管理该域中用户电子邮件的服务器，由优先级(更小数字意味更高优先级) 和服务器名组成

```
$ dig fudan.edu.cn ns
fudan.edu.cn.       600   IN   NS   ns.fudan.edu.cn.
fudan.edu.cn.       600   IN   NS   ns2.fudan.edu.cn.
fudan.edu.cn.       600   IN   NS   ns1.fudan.edu.cn.
```

```
$ dig www.fudan.edu.cn
www.fudan.edu.cn.   237   IN   A      202.120.224.81
www.fudan.edu.cn.   237   IN   A      202.120.224.129
$ dig www.fudan.edu.cn aaaa
www.fudan.edu.cn.   600   IN   AAAA   2001:da8:8001:2::129
www.fudan.edu.cn.   600   IN   AAAA   2001:da8:8001:2::81
```

```
$ dig www.baidu.com
www.baidu.com.          301   IN   CNAME   www.a.shifen.com.
www.a.shifen.com.       76    IN   CNAME   www.wshifen.com.
www.wshifen.com.        112   IN   A       103.235.46.39
```

```
$ dig qq.com mx
qq.com.   6766   IN   MX   10 mx3.qq.com.
qq.com.   6766   IN   MX   20 mx2.qq.com.
qq.com.   6766   IN   MX   30 mx1.qq.com.
```

区域信息：资源记录(Resource Record)

- Type= PTR
  - name：IPv4地址(a.b.c.d)，映射到in-addr域名(d.c.b.a.in-addr.arpa)
  - value：该name(IP地址)对应的域名

```
$ dig -x 8.8.4.4
4.4.8.8.in-addr.arpa.   0     IN     PTR     dns.google.
```

- type=HINFO
  - **name**：主机名
  - **value**：文本，描述CPU和OS
- 拓展：Type=SRV，MX的一般化
  - **name**：_service._protocol.domain
  - **value**：优先级 权重 端口号 主机
  - 描述该domain的采用protocol实现的服务service在指定主机的相应端口上

```
_http._tcp.example.com. SRV 10 5 80. www.example.com
```
- 说明基于TCP的HTTP服务在www.example.com的80端口上，优先级10，权重为5
- 优先级：数值越小，优先级越高
- 权重：相同优先级的记录，按照权重选择，提供负载均衡

- 拓展：type=TXT
  - **name**：主机名
  - **value**：文本，现在常用于反垃圾邮件处理(SPF/DKIM)，或者与SRV结合支持基于DNS的资源发现(**RFC 6763: DNS-Based Service Discovery**)，描述指定服务的相关信息（不包括IP地址和端口号）

Sender Policy Framework，Domain Keys Identified Mail

```
$ dig fudan.edu.cn TXT
fudan.edu.cn.        0     IN     TXT     "v=spf1 ip4:202.120.224.0/24 ip4:61.129.42.0/24 ip6:2001:da8:8001::/48
include:spf.icoremail.net include:spf.mail.qq.com ~all"
```

区域信息：Zone文件

- 第一个RR为SOA, 且只有一个SOA：主域名服务器、联系人以及主从域名服务器之间如何进行区域传输等
- NS RR：
  - 描述被授权管理该区域的域名服务器
  - 如果有子区域，则：
    - 通过NS RR 将子区域授权给另一个域名服务器管理
    - 如果有必要，通过A RR描述管理子区域的域名服务器的IP地址(glue record)
    - 拓展：管理子区域的域名服务器的域名属于子区域时需要glue record
      - 授权子区域的NS和glue record都是non-authoritative
      - NS记录在子区域中为authoritative
- 多个A或AAAA RR：描述域名和IP地址(IPv6地址）的映射
- MX记录：描述给该区域中的用户发送电子邮件时应该发给哪个邮件服务器
  - 如果没有MX RR，则域名所对应的IP地址就是邮件服务器的地址
- DNS服务器管理的区域信息的维护：
  - 管理员人工更新（修改区域文件），正在运行的DNS服务器重新读取区域文件
  - 拓展：DDNS(Dynamic DNS)：RFC2136/3007， 允许通过DNS消息交互来更新名字映射，即支持动态域名

glue record: 负责子区域的域名服务器与IP地址的映射属于子区域，同时在父区域出现

对于区域edu，这两条记录都是non-authoritative

zone edu:

fudan.edu.cn. NS ns.fudan.edu.cn

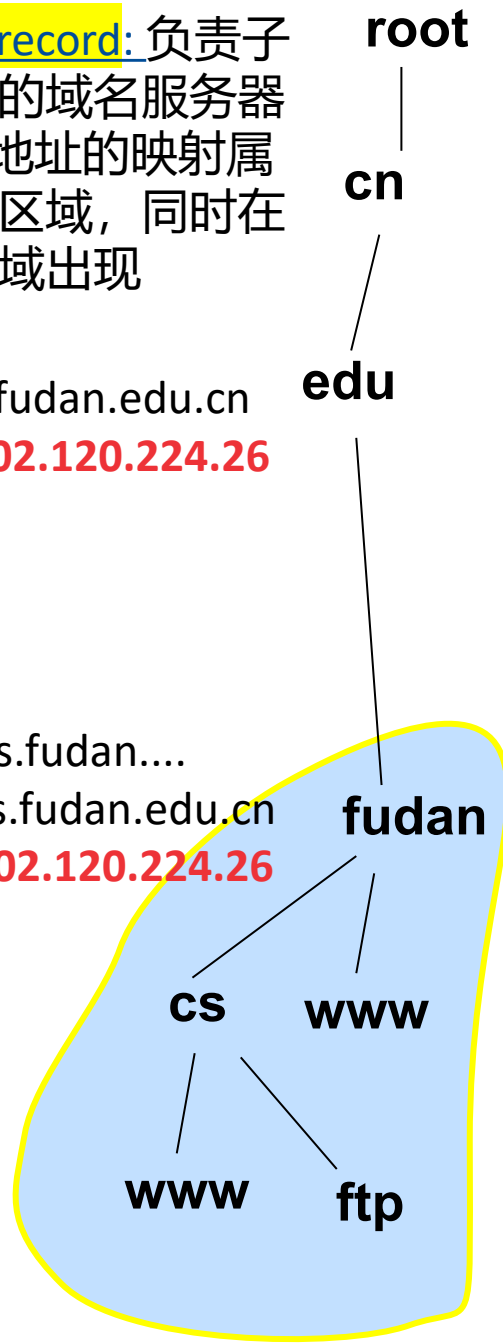
ns.fudan.edu.cn. A 202.120.224.26

zone fudan.edu.cn:

fudan.edu.cn. SOA ns.fudan....

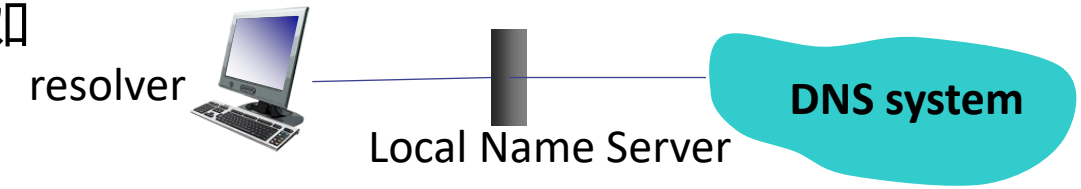
fudan.edu.cn. NS ns.fudan.edu.cn

ns.fudan.edu.cn. A 202.120.224.26



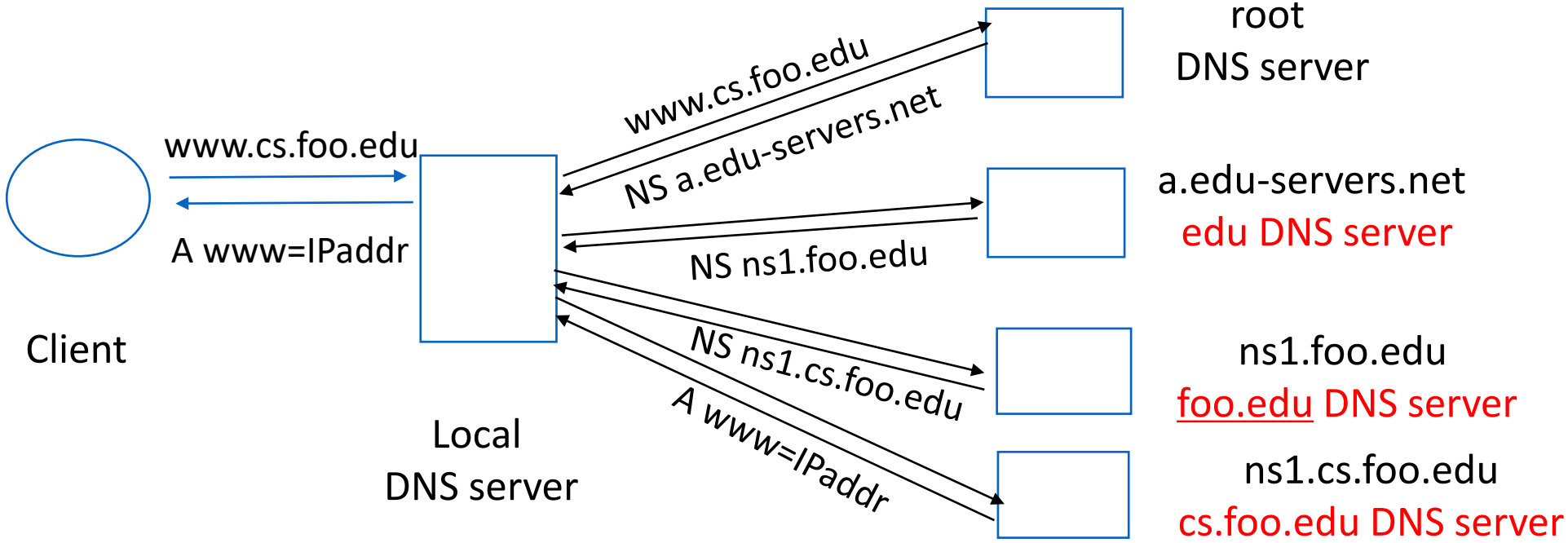
域名解析

- 主机一般会配置本地域名服务器，也称为**解析服务器，**为用户（主机）提供DNS解析服务
- 主机的应用程序访问resolver解析库，通过解析服务器访问DNS提供的服务
- 主机与本地域名服务器之间一般采用递归查询，本地域名服务器充当proxy功能，将DNS查询请求转发到维护域名空间的域名服务器，在得到解析结果后将其发送给主机
- 解析过程中的主机和服务器一般会将解析结果缓存
- 解析服务器严格来说不属于域名层次中的一部分，而是提供解析服务
- 域名服务器在负责管理域名树中的一部分(即管理某些区域)的同时，一般也可充当解析服务器
- 每个ISP（包括大公司、学校）至少有一个解析服务器
- 目前Internet也有许多(6万多）开放的解析服务器，比如
  - google提供的8.8.8.8和8.8.4.4
  - Level 3 Communications提供的4.2.2.{1-6}
  - OpenDNS提供的208.67.222.222和208.67.220.220
  - 阿里提供的223.5.5.5和223.6.6.6
  - 腾讯云DNS： 119.29.29.29



域名解析过程

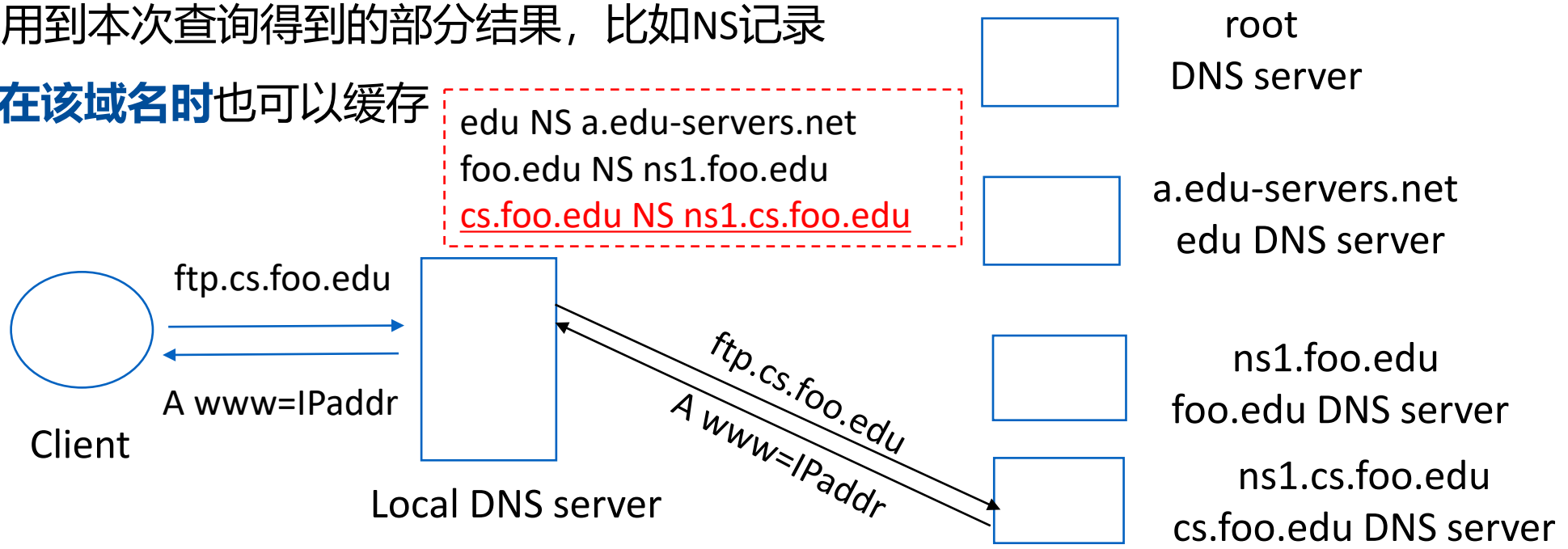
- 每次请求-应答过程中返回的是解析结果还是查找解析结果的指引(referral)
  - 递归(recursive)方式：发送请求给下一个服务器，对方给出解析结果
  - 迭代(iterative)方式：发送请求给下一个服务器，对方给出一个可能知道答案的域名服务器
- 本地域名服务器一般支持递归解析方式，主机一般采用递归解析方式
- 本地域名服务器以及其他域名服务器进一步可采取迭代或递归方式
  - 由于递归查找会带来大量开销，实践中一般采用迭代方式



域名缓存Cache

- DNS客户、途中的DNS服务器都会将解析结果缓存，**收到新的请求在缓存查找时采用最长后缀匹配**
- 缓存有一定的生存时间TTL
  - 最初的TTL由域名记录的拥有者控制
  - 在缓存中保存时相应地减少，TTL为0时从缓存中移走
- 成功的DNS响应被缓存
  - 下次查询同一域名可以快速响应
  - 其他查询可以用到本次查询得到的部分结果，比如NS记录
- DNS响应报告**不存在该域名时**也可以缓存

- 缓存提高了解析的速度，减少域名服务器的开销，提高了可靠性
- 但缓存的RR纪录可能已经过期，不一致



DNS协议

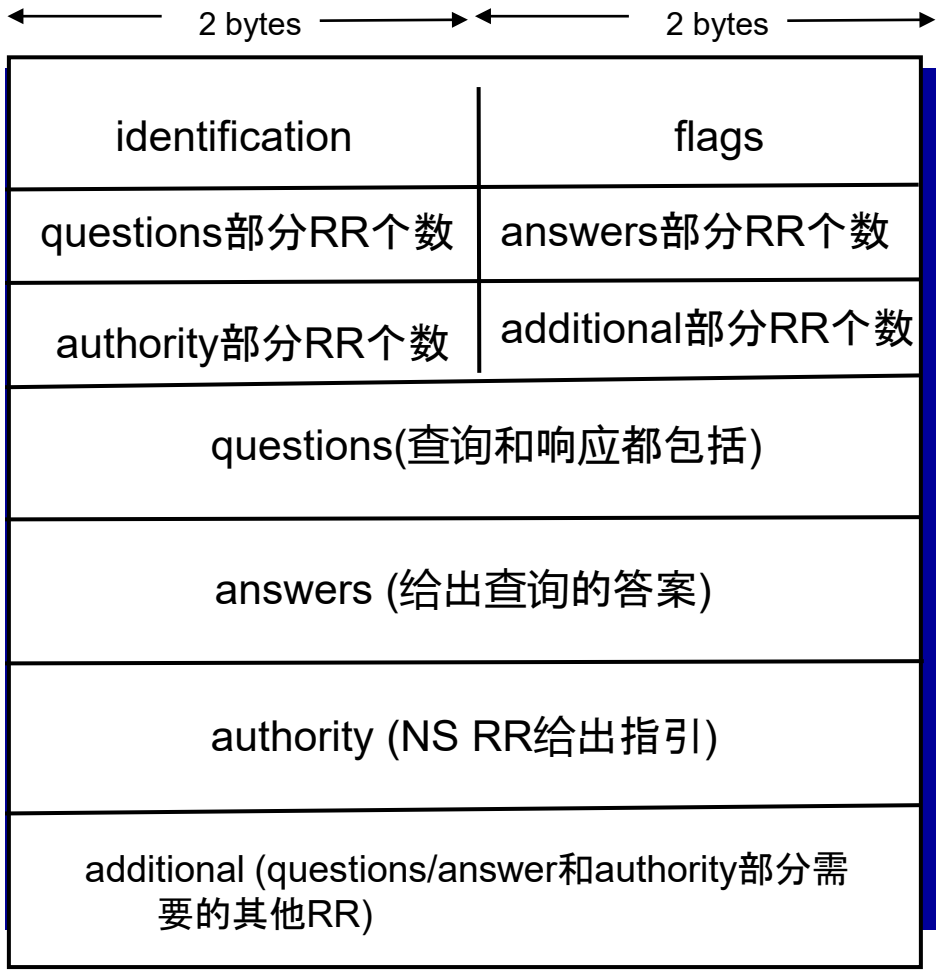
- DNS服务器采用端口号53，支持UDP和TCP协议
- 区域传输一般采用TCP
- DNS查询一般采用UDP，无需建立连接，可以支持更多的用户
  - 采用UDP传输的DNS消息限制为512字节，如果超过512字节，多余的部分会被截掉
  - 可采用TCP再次查询，首先发送两个字节的整数，给出了接下来发送的DNS消息的长度

拓展：DNS协议

- DNS查询和响应格式一致
- identification: 查询和响应之间的对应

flags

QR	查询=0，响应=1
OPCODE	4位, 描述操作方式: **标准查询**, 反向查询(可选），UPDATE等
AA	Authoritative Answer，=1表示来自于权威域名服务器
TC	Truncation，表示消息是否截取（超过512字节)
RD	Recursion Desired，发送查询时设置，是否采用递归查询
RA	Recursion Available，服务器是否支持递归查询
RCODE	4位返回码，是否成功, 如果失败时失败的原因
Z	保留，全0



- questions部分包括(NAME, TYPE, CLASS)
- 其他部分的RR记录包含(NAME, TYPE, CLASS, TTL, VALUE)
- EDNS0在additional部分引入OPT RR，给出了协商的DNS消息大小

DNS消息示例

```
> User Datagram Protocol, Src Port: 65113, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xc133
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v dns.weixin.qq.com: type A, class IN
        Name: dns.weixin.qq.com
        [Name Length: 17]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 65113
v Domain Name System (response)
    Transaction ID: 0xc133
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v dns.weixin.qq.com: type A, class IN
        Name: dns.weixin.qq.com
        [Name Length: 17]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v dns.weixin.qq.com: type CNAME, class IN, cname v6.dns.weixin.qq.com
        Name: dns.weixin.qq.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 600
        Data length: 5
        CNAME: v6.dns.weixin.qq.com
    v v6.dns.weixin.qq.com: type A, class IN, addr 123.151.190.252
        Name: v6.dns.weixin.qq.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 600
        Data length: 4
        Address: 123.151.190.252
    v v6.dns.weixin.qq.com: type A, class IN, addr 123.150.208.86
        Name: v6.dns.weixin.qq.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 600
        Data length: 4
        Address: 123.150.208.86
```

拓展：DNS扩展

- RFC 2845引入**基于共享密钥的TSIG**(Transaction and Request Authentication)，通过DNS消息中增加SIG RR对DNS消息签名，验证DNS消息的确是对方服务器发送的且没有被篡改。
  - TSIG可用于保护区域传输
  - TSIG也可用于DDNS，为动态域名更新提供保护
  - 最新的标准为RFC8945 Secret Key Transaction Authentication for DNS (TSIG)
- 1999年引入DNSSEC(DNS Security Extension)，提供DNS 资源记录的认证和完整性支持
  - 最新的规范为RFC 4033,4034,4035
  - 引入了RRSIG、 DNSKEY、 DS、 NSEC资源记录
  - 所有RR记录都采用Zone的私钥进行签名，得到配套的RRSIG RR
  - 要验证某个RR是否是原来Zone发布并且没有被篡改，通过配套的RRSIG RR包含的签名信息以及Zone的公钥进行验证
  - 如何得到Zone的公钥?
    - 手工配置
    - DNSKEY保存了Zone的公钥，而DS RR包含了公钥的hash值，用于证明DNSKEY是合法的
  - NSEC(Next Secure) RR用于证明某个域名不存在，或者没有该域名对应类型的RR

拓展： DNS扩展

- **EDNS0 (RFC 6891 Extension Mechanisms for DNS），了解一下**
  - IPv6引入AAAA记录， TXT RR赋予新的意义, 要求支持DNSSEC等，**DNS消息越来越大**
  - DNS消息通过UDP传递时可超过512字节，**建议4096字节。**通过DNS消息中增加OPT RR实现
  - 有些防火墙不允许使用UDP协议传输的超过512字节的DNS消息通过
- **RFC 7766 DNS Transport over TCP - Implementation Requirements，**建议所有实现支持TCP和UDP
  - 查询时可以采取TCP或UDP，而不是先尝试UDP，发现有截断时再尝试TCP
  - TCP更难进行伪装攻击，可以通过TLS提供隐私保护
  - 引入了在HTTP协议中采用的持续连接和管道化概念，在一次DNS查询后不是马上关闭TCP连接，而是保持活跃一段时间
- DNS加密：
  - DNS请求和响应明文传递，泄露隐私，可能的攻击 ---> DNS查询和响应进行加密
  - 2016年，DNS-over-TLS(DoT)，RFC 7858和RFC8310
  - 2018年，DNS-over-HTTPS(DoH)，RFC8484，目前占据主流
  - 2022年，DNS-over-QUIC(DoQ)，RFC9250