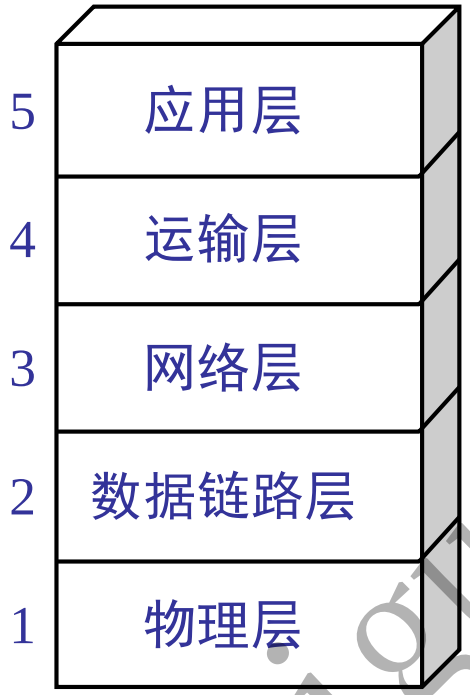
计算机网络

顾 军

计算机学院

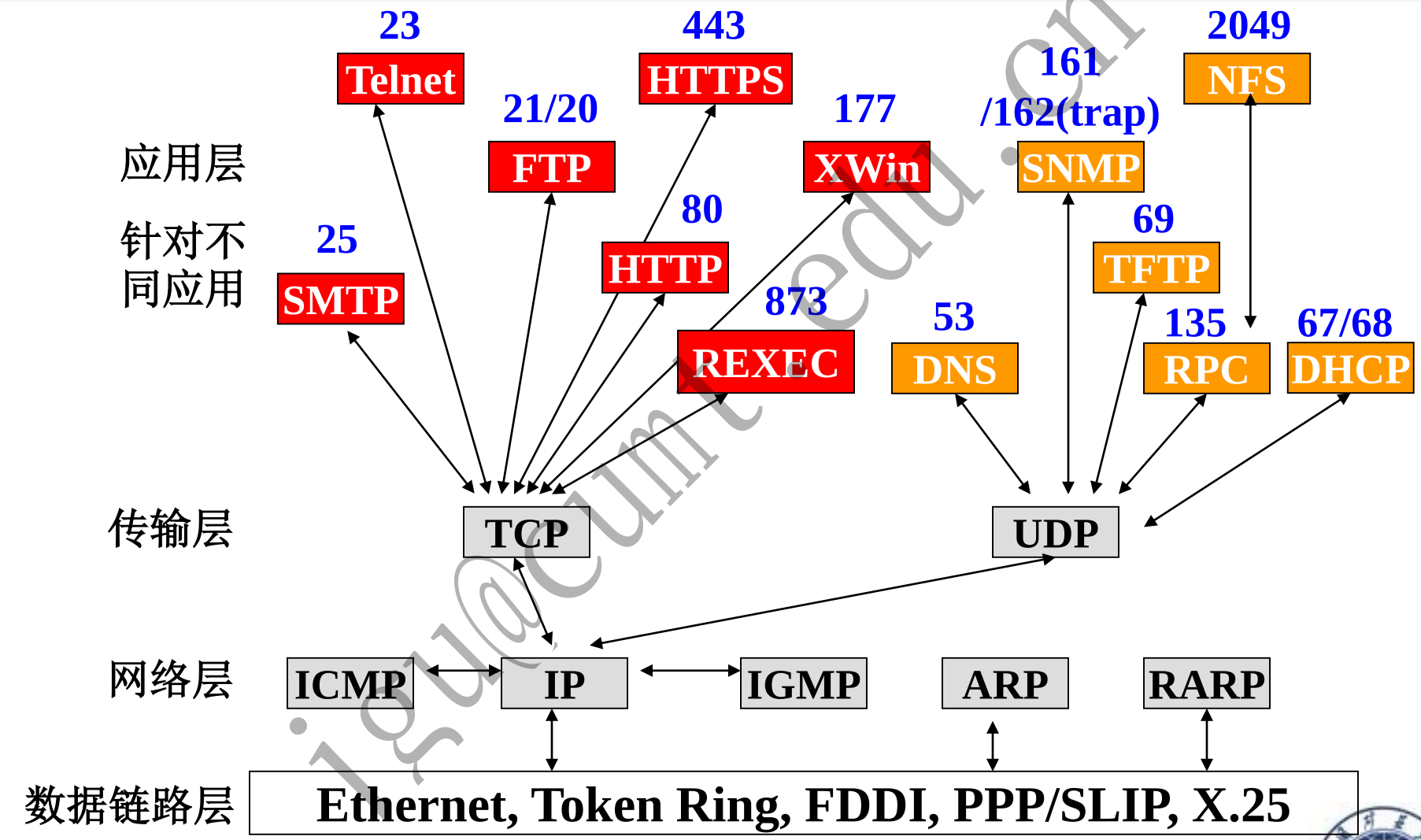
jgu@cumt.edu.cn

专题6：互联网提供了哪些高层应用

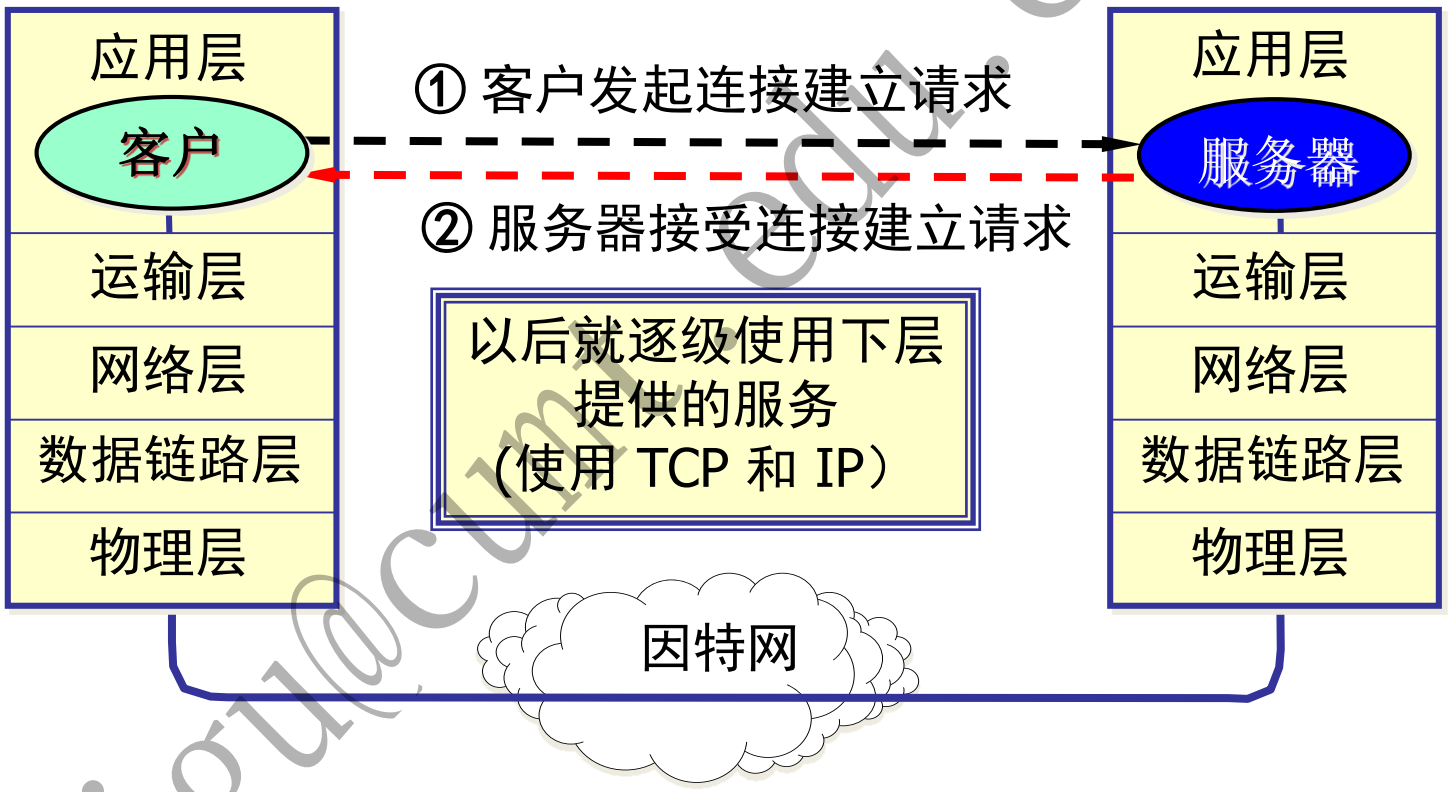


- 应用层(application layer)
- 运输层(transport layer)
- 网络层(network layer)
- 数据链路层(data link layer)
- 物理层(physical layer)

TCP/IP协议族中的应用层协议

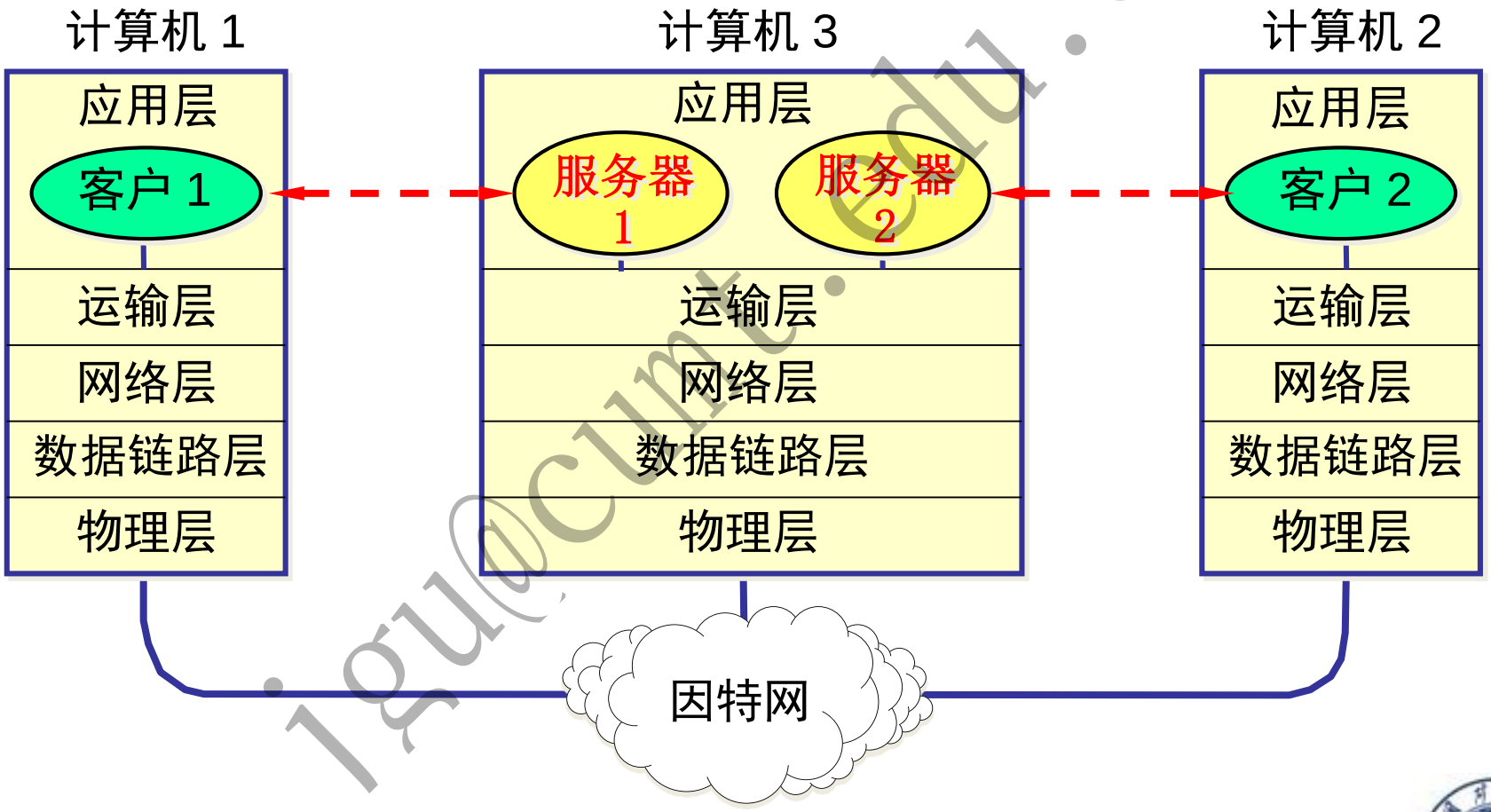


客户进程和服务器进程使用 TCP/IP 协议进行通信



C/S访问方式

功能较强的计算机
可同时运行多个服务器进程

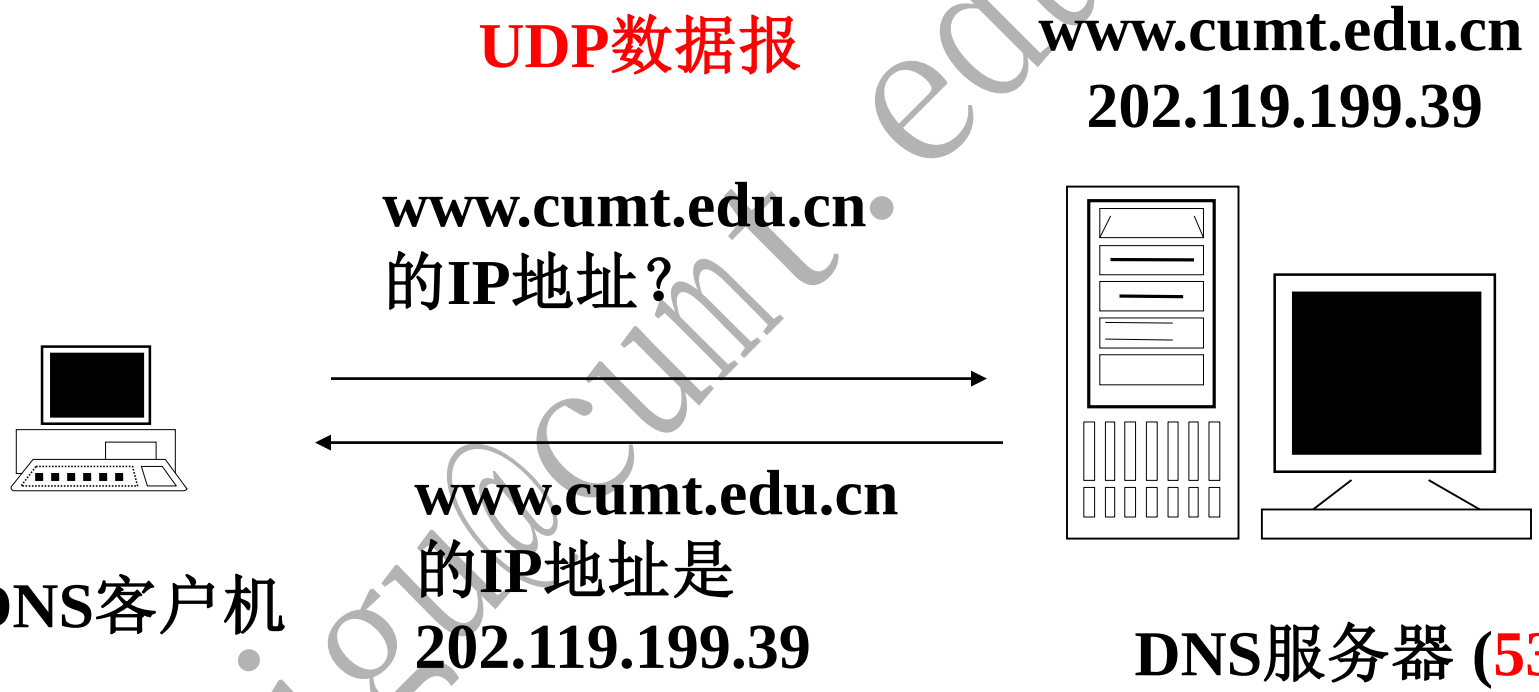


Q1：为什么敲入字符串也能访问对方计算机？

- IP 地址是定长的 32 位二进制数字，非常便于机器进行处理，但是不方便人的记忆和使用，而使用有助记忆的字符串可以弥补IP地址的不足。
- 任何一个连接在因特网上的主机或路由器，都有一个唯一的层次结构的名字，即域名。
- 域名只是个逻辑概念，并不代表计算机所在的物理地点。

域名系统的作用

域名系统DNS用来进行IP地址和主机名字之间的转换。



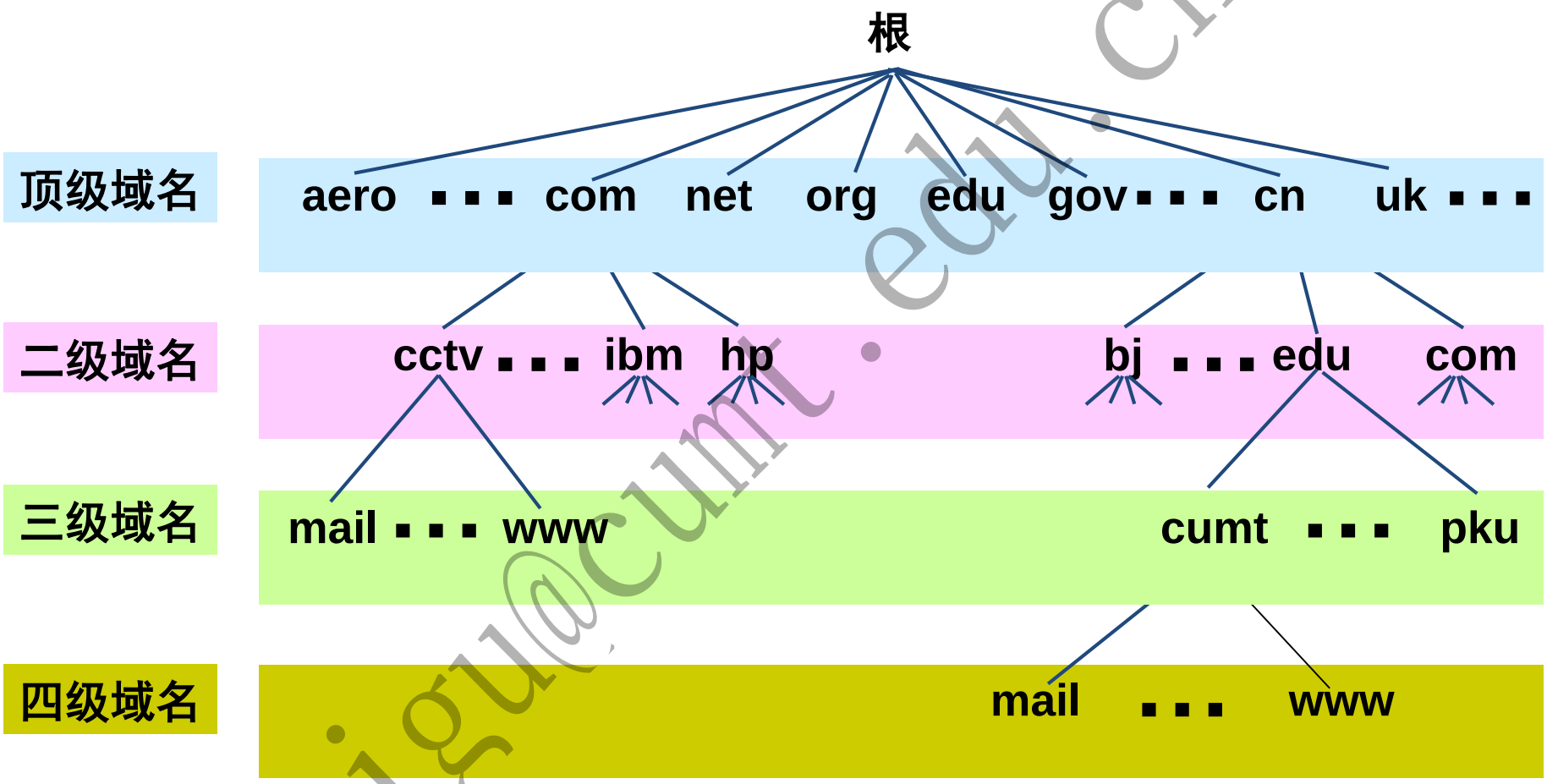
Q2：因特网的域名结构？

- 因特网采用了层次树状结构的命名方法。
- 域名的结构由标号序列组成，各标号之间用点隔开：

> ….三级域名．二级域名．顶级域名

- 各标号分别代表不同级别的域名。
  - 域名中的“点”和点分十进制 IP 地址中的“点”并无一一对应的关系。点分十进制 IP 地址中一定是包含三个“点”，但每一个域名中“点”的数目则不一定正好是三个。

因特网的域名空间



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，等等。

(2) 通用顶级域名 gTLD：最早的顶级域名是：

.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）

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

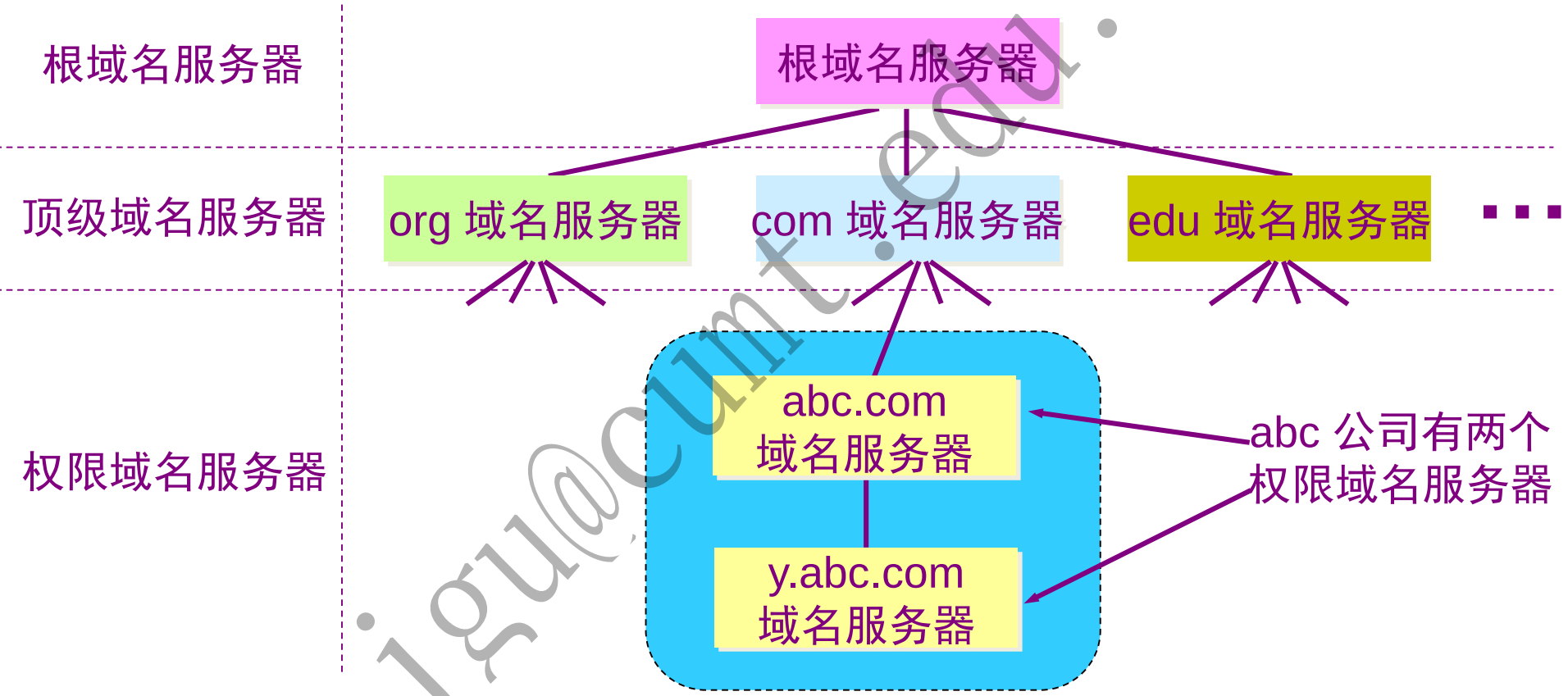
新增加了下列的通用顶级域名

- .aero （航空运输企业）
- .biz （公司和企业）
- .cat （加泰隆人的语言和文化团体）
- .coop （合作团体）
- .info （各种情况）
- .jobs （人力资源管理者）
- .mobi （移动产品与服务的用户和提供者）
- .museum （博物馆）
- .name （个人）
- .pro （有证书的专业人员）
- .travel （旅游业）

Q3：域名服务器的种类和作用？

- 名字到 IP 地址的解析是由若干个域名服务器程序完成的。域名服务器程序在专设的结点上运行，运行该程序的机器称为域名服务器。
  - 根域名服务器
  - 顶级域名服务器
  - 权限域名服务器
  - 本地域名服务器

树状结构的 DNS 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。所有的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。
- 所有根服务器均由美国政府授权的互联网域名与号码分配机构ICANN统一管理，负责全球互联网域名根服务器、域名体系和IP地址等的管理，美国政府对其管理拥有很大发言权。

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）。
- 这些根域名服务器相应的域名分别是

  a.rootservers.net

  b.rootservers.net

  …

  m.rootservers.net

根域名服务器全球分布图（视频截图）

目前在IPv4体系内，全球只有13台根服务器，并且没有一台在中国。

根域名服务器共有 13 套装置（不是 13 个机器）

- 到2016年2月，全世界已经在 588 个地点安装了根域名服务器，这样做的目的是为了方便用户，使世界上大部分 DNS 域名服务器都能就近找到一个根域名服务器。

举例：根域名服务器 L 的地点分布图（世界 150 个地点）

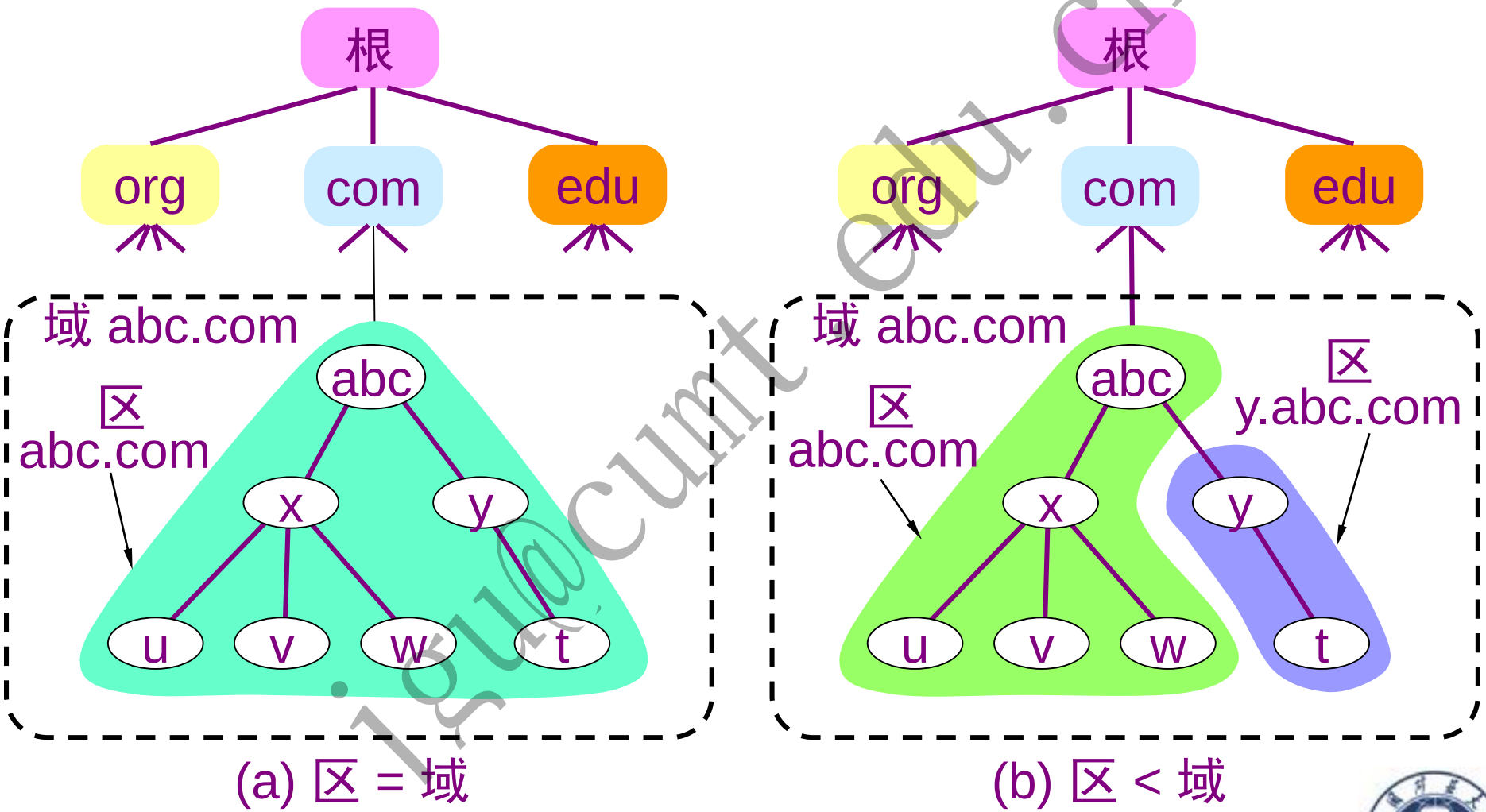
顶级域名服务器（即 TLD 服务器）

- 这些域名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。
- 当收到 DNS 查询请求时，就给出相应的回答（可能是最后的结果，也可能是下一步应当找的域名服务器的 IP 地址）。

权限域名服务器

- 一个服务器所负责管辖的（或有权限的）范围叫做区(zone)。
- 各单位根据具体情况来划分自己管辖范围的区。但在一个区中的所有节点必须是能够连通的。
- 每一个区设置相应的权限域名服务器，用来保存该区中的所有主机的域名到IP地址的映射。
- DNS 服务器的管辖范围不是以“域”为单位，而是以“区”为单位。

区的不同划分方法举例



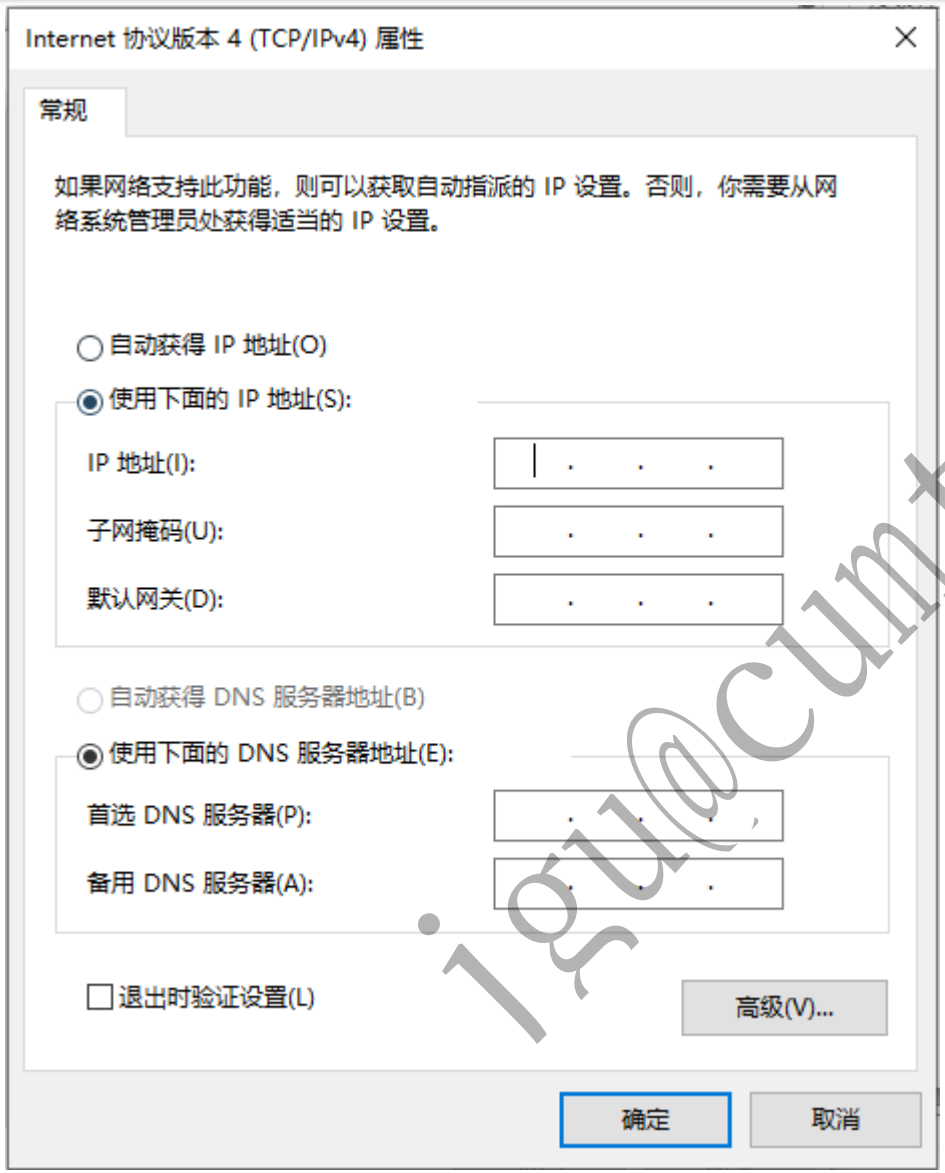
权限域名服务器

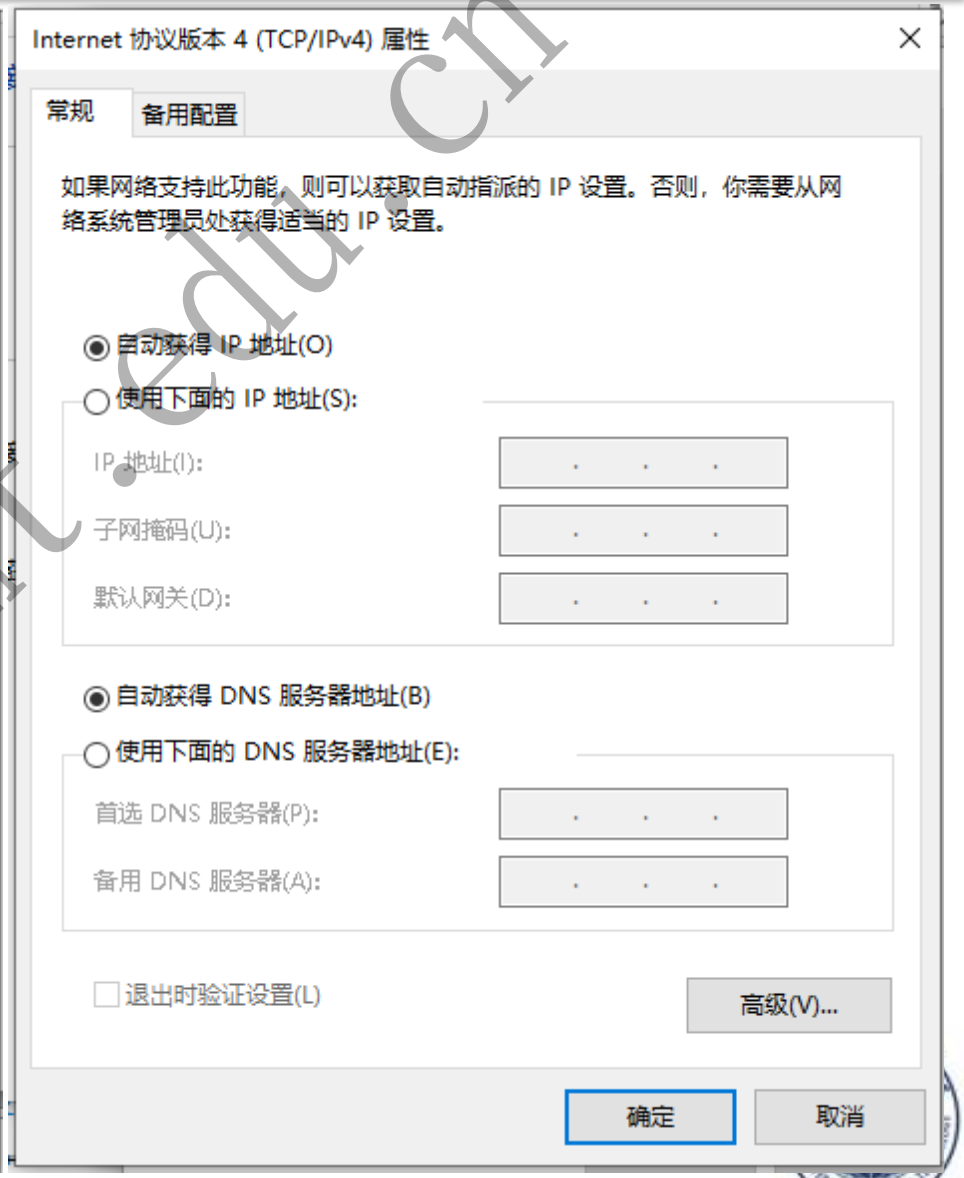
- 负责一个区的域名服务器。
- 当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。

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。
- 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，
- 这种域名服务器有时也称为默认域名服务器。

主机的IPv4协议属性配置





域名解析工具nslookup(name server lookup)

nslookup用于查询DNS的记录，查询域名解析是否正常，在网络故障时用来诊断网络问题，有两种模式: 交互 & 非交互

直接查询： nslookup domain [dns-server]

//如果没有指定dns服务器，就采用系统默认的dns服务器

默认服务器: UnKnown，表示命令不知道现在使用的是哪一个 DNS 服务器;

通过路由器的内网侧 IP 地址192.168.1.1上网

“非权威应答” 的提示表示所查询的域名不使用当前所用的DNS查询服务器

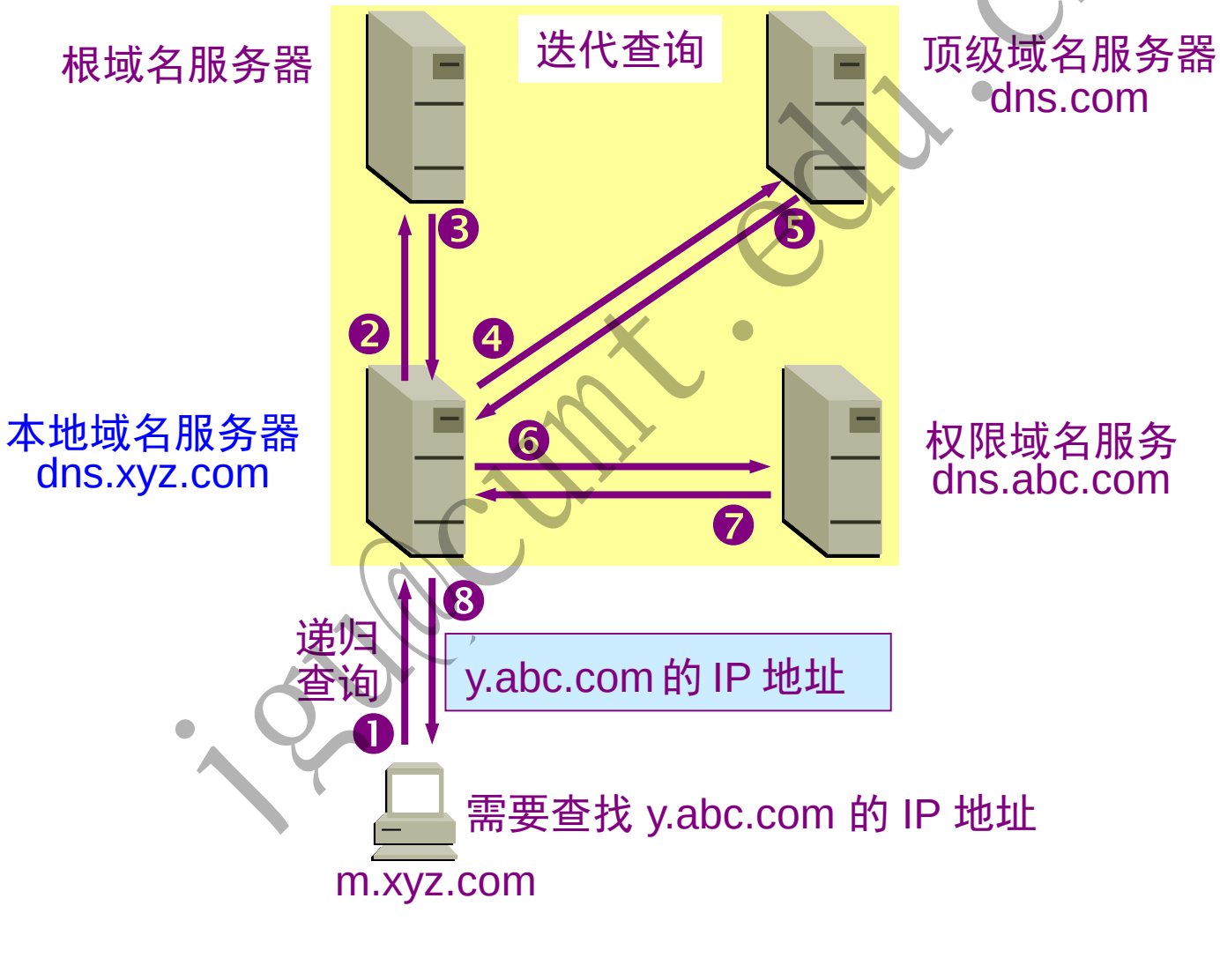
```
C:\>nslookup www.cumt.edu.cn
服务器:  UnKnown
Address:  192.168.1.1

非权威应答:
名称:    sudy.cumt.edu.cn
Address:  58.218.185.156
Aliases:  www.cumt.edu.cn
```

只要不是从要查询的DNS服务器的实际存储中获得的域名解析应答信息，都称为非权威应答，也就是从本地域名服务器缓存中获取的域名解析结果。

Q4：如何解析域名？

- 主机向本地域名服务器的查询一般都是采用递归查询。如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。
- 本地域名服务器向根域名服务器的查询通常是采用迭代查询。当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。

本地域名服务器采用迭代查询



本地DNS的迭代查询过程

1、主机m.abc.com先向本地服务器dns.xyz.com进行递归查询。

2、本地服务器采用迭代查询。它先向一个根域名服务器查询。

3、根域名服务器告诉本地服务器，下一次应查询的顶级域名服务器dns.com的IP地址。

4、本地域名服务器向顶级域名服务器dns.com进行查询。

5、顶级域名服务器dns.com告诉本地域名服务器，下一步应查询的权限服务器dns.abc.com的IP地址。

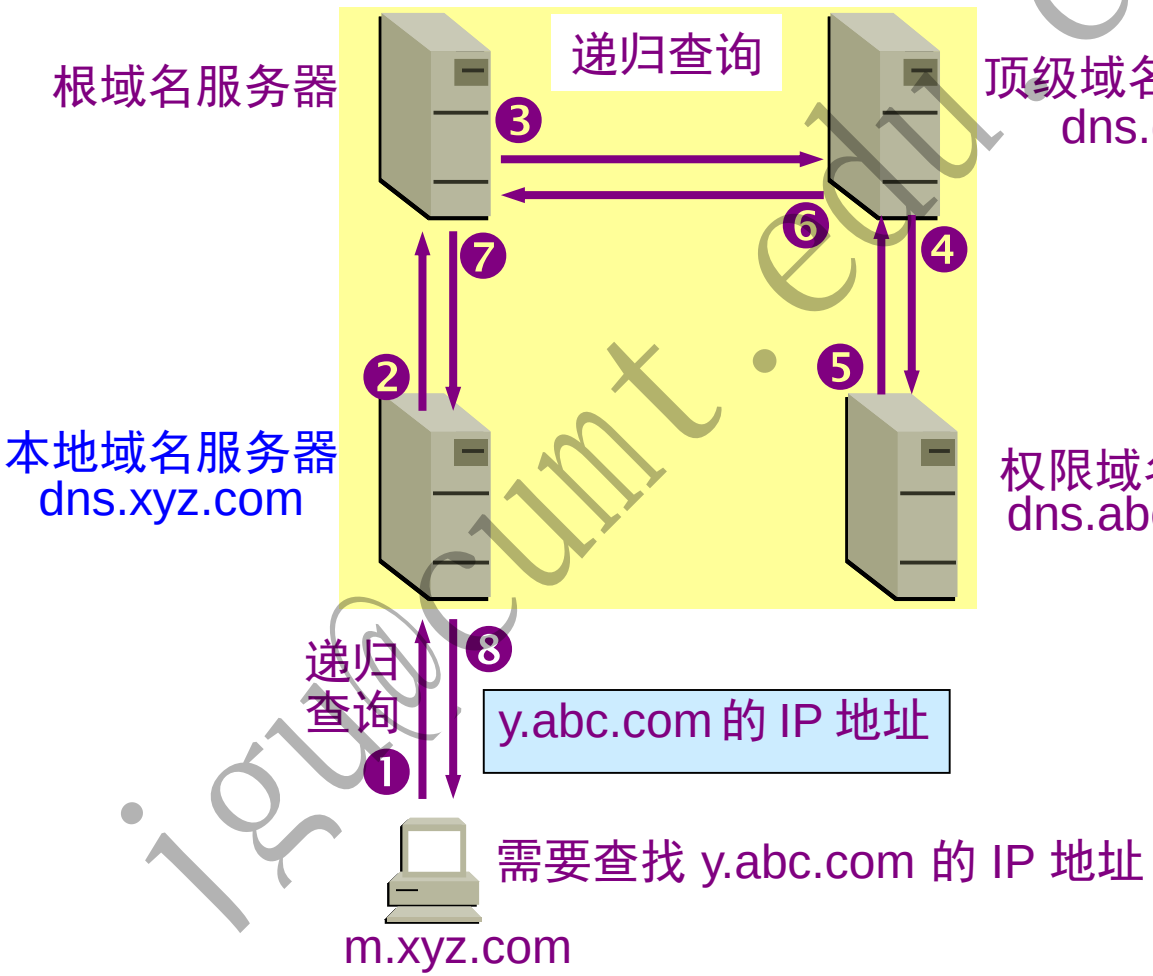
6、本地域名服务器向权限域名服务器dns.abc.com进行查询。

7、权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的IP地址。

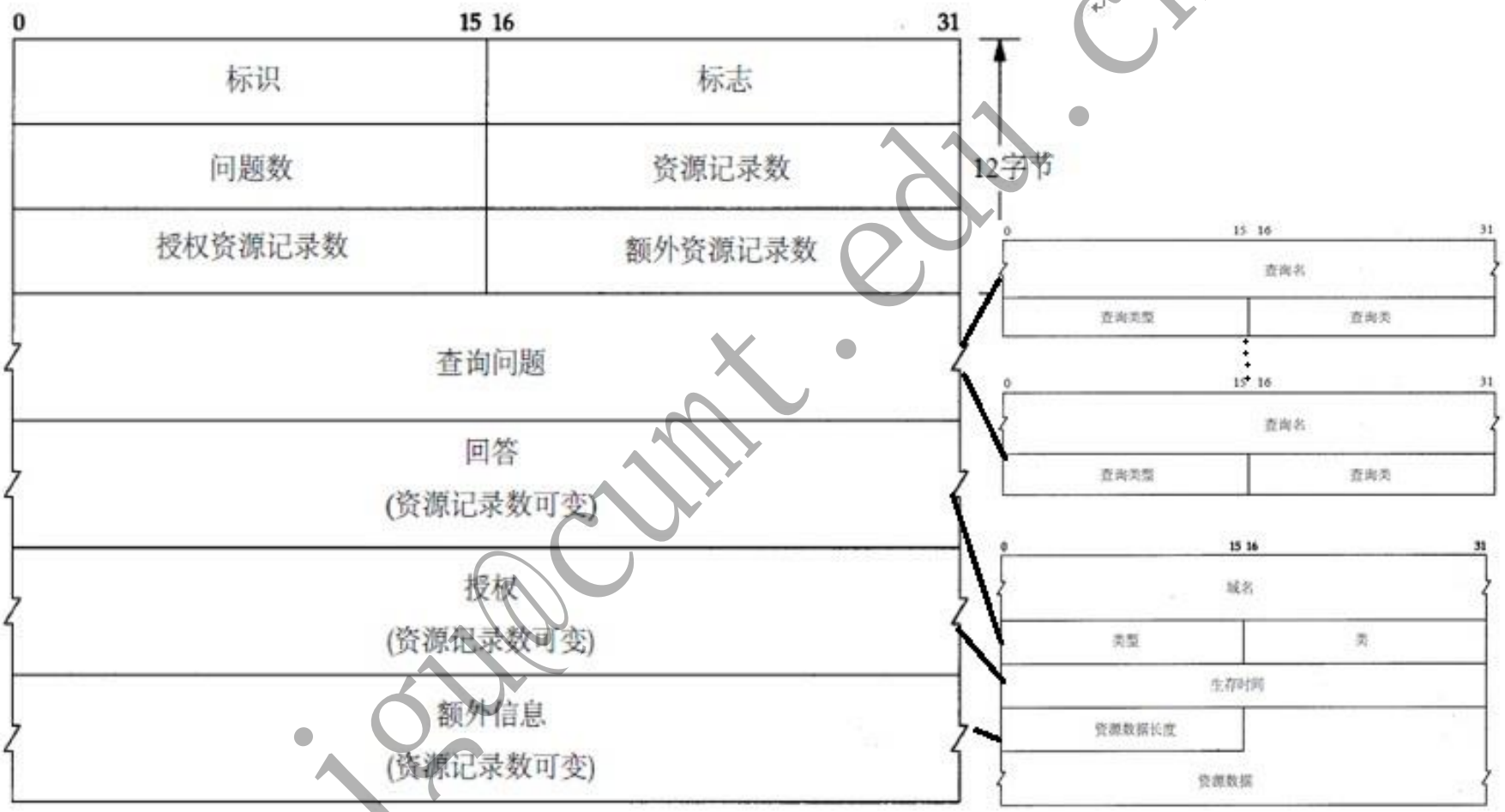
8、本地域名服务器最后把查询结果告诉m.xyz.com。

整个查询过程共用到了8个UDP报文。

本地域名服务器采用递归查询（比较少用）



DNS报文格式



Q5：如何降低域名服务器的负荷？

- 每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。
- 可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少。
- 为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器，并处理超过合理时间的项（例如，每个项目只存放两天）。
- 当权限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存在的时间值。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转换的准确性。

Q6：如何提高域名服务器的可靠性？

- DNS 域名服务器都把数据复制到几个域名服务器来保存，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。
- 主域名服务器定期把数据复制到辅助域名服务器中，而更改数据只能在主域名服务器中进行。这样就保证了数据的一致性。

如果根域名服务器出事了，怎么办？

来自根域名服务器的安全性问题

美国能够用切断根服务器的方式，瘫痪中国网络！

谣言，NO!

- 根域名服务器并不直接把域名转换成 IP 地址。
- 网民查询域名的时候并不直接去访问根域名服务器，而是通过递归域名服务器（在本地网络里设置的DNS域名服务器）来查询域名。
- 递归服务器通常设立在运营商处，根服务器中的记录可以缓存在递归服务器中心，这样递归服务器实际上就起到了根服务器的作用。
- 根域名服务器中的记录很少，记录了1000多个顶级域名的信息，常用的不到10个，所以缓存回来并不难。在使用迭代查询时，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。

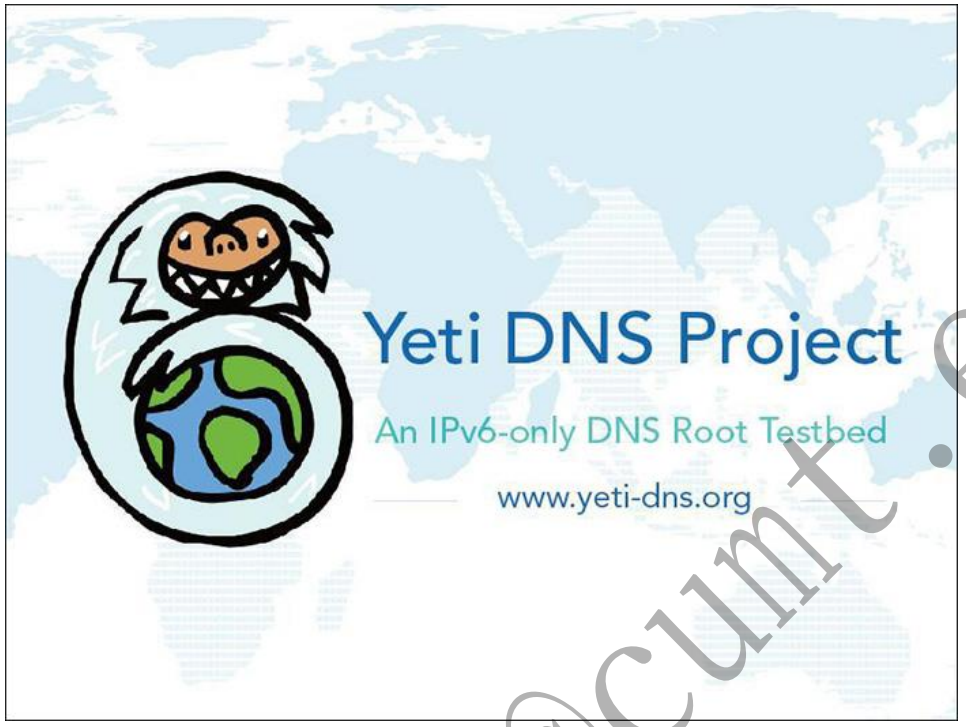
如果美国真的中断根服务器，我们怎么办？

首先，对中国的影响主要在国际互通。
比如说国外的网民要访问中国的一些网站可能访问不到，但是并不影响中国的网民访问中国的网站，网上购物、视频以及聊天、支付等等网络应用都不会有影响。

其次，我们会通过一些应急手段解决突发问题。比如说我们可以在递归服务器里面把根写进去，或者我们自己再建一套根的镜像系统或者应急系统，都能解决这个问题。
镜像根服务器就是原来根服务器的克隆服务器。

- 在中国就建立了很多根服务器镜像，在域名系统北京市工程研究中心就有一个镜像。从此中国解析.cn或.com的域名就不用由国外的根服务器提供服务了，而是由中国自己的镜像服务器来运作。

IPv6的“雪人计划”上马，或彻底重塑国际互联网秩序



"雪人计划"(Yeti DNS Project)——基于全新技术架构的全球下一代互联网（IPv6）根服务器测试和运营实验项目。

2015年6月23日正式发布，2017年11月28日，"雪人计划"已在全球完成25台IPv6根服务器架设，中国部署了其中的4台。

IPv6根服务器全球分布

“雪人计划”IPv6根服务器全球分布情况

国家	主根服务器	辅根服务器	国家	主根服务器	辅根服务器
中国	1	3	西班牙	0	1
美国	1	2	奥地利	0	1
日本	1	0	智利	0	1
印度	0	3	南非	0	1
法国	0	3	澳大利亚	0	1
德国	0	2	瑞士	0	1
俄罗斯	0	1	荷兰	0	1
意大利	0	1			

由于在IPv4报文的限制，使得我们域名根服务器的总数有限制。IPv6出现以后，这个限制被打破，未来我们就能再多写几条根服务器的地址进去，使得这个根就不只是13个了。

Q7：怎么实现文件的远程传送？

- 网络环境中的一项基本应用就是将文件从一台计算机中复制到另一台可能相距很远的计算机中。
- 但是，在两个主机之间传送文件往往非常困难。原因是众多的计算机厂商研制出的文件系统多达数百种，且差别很大。
  - (1) 计算机存储数据的格式不同。
  - (2) 文件的目录结构和文件命名的规定不同。
  - (3) 对于相同的文件存取功能，操作系统使用的命令不同。
  - (4) 访问控制方法不同。

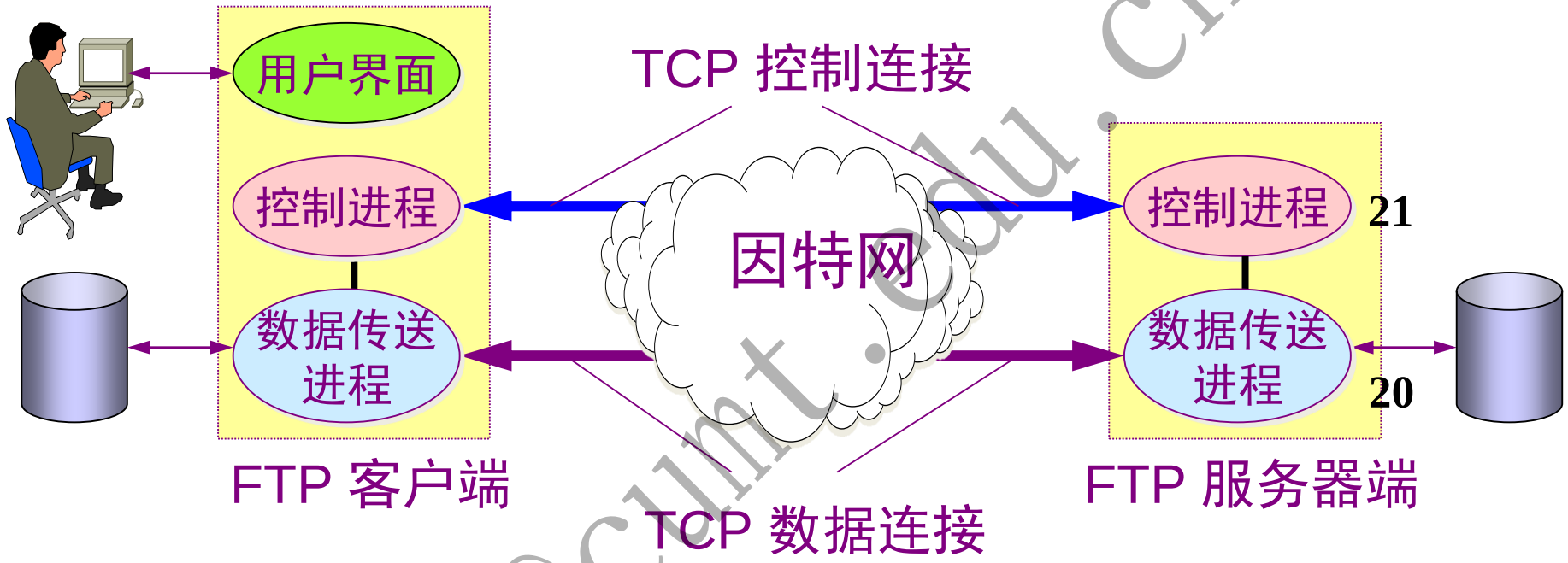
文件传送协议FTP

- 文件传输协议(FTP，File Transfer Proto)在RFC 959中定义，于1985年10月发布。
- 文件传输协议(FTP)被设计成为一个跨平台的、简单且易于实现的协议，屏蔽了各计算机系统的细节，适合于在异构网络中任意计算机之间传送文件，是因特网上使用得最广泛的文件传送协议。
- FTP 的主要功能是减少或消除在不同操作系统下处理文件的不兼容性，FTP 提供交互式的访问，允许客户指明文件的类型与格式，并允许文件具有存取权限。
- FTP 只提供文件传送的一些基本的服务，它使用 TCP 可靠的运输服务。

FTP有两个不同的端口号

- FTP 使用客户服务器方式。一个 FTP 服务器进程可同时为多个客户进程提供服务。
- FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求；另外有若干个从属进程，负责处理单个请求。
  - 当客户进程向服务器进程发出建立连接请求时，要寻找连接服务器进程的熟知端口(21)，同时还要告诉服务器进程自己的另一个端口号码，用于建立数据传送连接。
  - 接着，服务器进程用自己传送数据的熟知端口(20)与客户进程所提供的端口号码建立数据传送连接。
- 由于 FTP 使用了两个不同的端口号，所以数据连接与控制连接不会发生混乱。

FTP 使用的两个 TCP 连接



- 控制连接在整个会话期间一直保持打开，FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。
- 数据连接和数据传送进程实际完成文件的传送，在传送完毕后关闭“数据传送连接”并结束运行。

主进程的工作步骤：

- 打开熟知端口（端口号为 21），使客户进程能够连接上。
- 等待客户进程发出连接请求。
- 启动从属进程来处理客户进程发来的请求。从属进程对客户进程的请求处理完毕后即终止，但从属进程在运行期间根据需要还可能创建其他一些子进程。
- 回到等待状态，继续接受其他客户进程发来的请求。
- 主进程与从属进程的处理是并发地进行。

FTP面临淘汰

- FTP有着极高的延时，这意味着，从开始请求到第一次接收需求数据之间的时间会非常长；并且不时的必须执行一些冗长的登陆进程。
- 互联网中有很大一部分 FTP 服务器被称为“匿名”（Anonymous）FTP 服务器。这类服务器的目的是向公众提供文件拷贝服务，不要求用户事先在该服务器进行登记注册，也不用取得FTP服务器的授权。
- 目前使用WWW环境已取代匿名FTP成为最主要的信息查询方式，但是匿名FTP仍是 Internet上传输分发软件的一种基本方法。如red hat 、autodesk等公司的匿名站点。

网盘和云盘

网盘，又称网络U盘、网络硬盘，是由互联网公司推出的在线存储服务。服务器机房为用户划分一定的磁盘空间，为用户免费或收费提供文件的存储、访问、备份、共享等文件管理等功能，并且拥有高级的世界各地的容灾备份。

百度网盘

云盘

数据中心

虚拟化的存储资源池（storage pool）

Web服务应用程序接口（API）

Q8：怎么实现文件的远程访问？

- FTP提供文件传送，而NFS(Network File System)则提供文件访问，允许应用进程打开一个远地文件，并能在该文件的某一个特定的位置上开始读写数据，就像访问本地文件一样。
- NFS 可使用户只复制一个大文件中的一个很小的片段，而不需要复制整个大文件。
  - 例如，计算机 A 的 NFS 客户软件，把要添加的数据和在文件后面写数据的请求一起发送到远地的计算机 B 的 NFS 服务器。NFS 服务器更新文件后返回应答信息。
  - NFS 在网络上传送的只是少量的修改数据。

Q9：简单文件传送协议 TFTP？

- TFTP(Trivial File Transfer Protocol) 是一个很小且易于实现的文件传送协议。
- TFTP 使用客户服务器方式和使用 UDP 数据报（端口69），因此 TFTP 需要有自己的差错改正措施。
- TFTP 只支持文件传输而不支持交互。
- TFTP 没有一个庞大的命令集，没有列目录的功能，也不能对用户进行身份鉴别。

TFTP 的主要特点：

(1) 每次传送的数据 PDU 中有 512 字节的数据，但最后一次可不足 512 字节。

(2) 数据 PDU 也称为文件块(block)，每个块按序编号，从 1 开始。

(3) 支持 ASCII 码或二进制传送。

(4) 可对文件进行读或写。

(5) 使用很简单的首部。

TFTP文件块需要确认

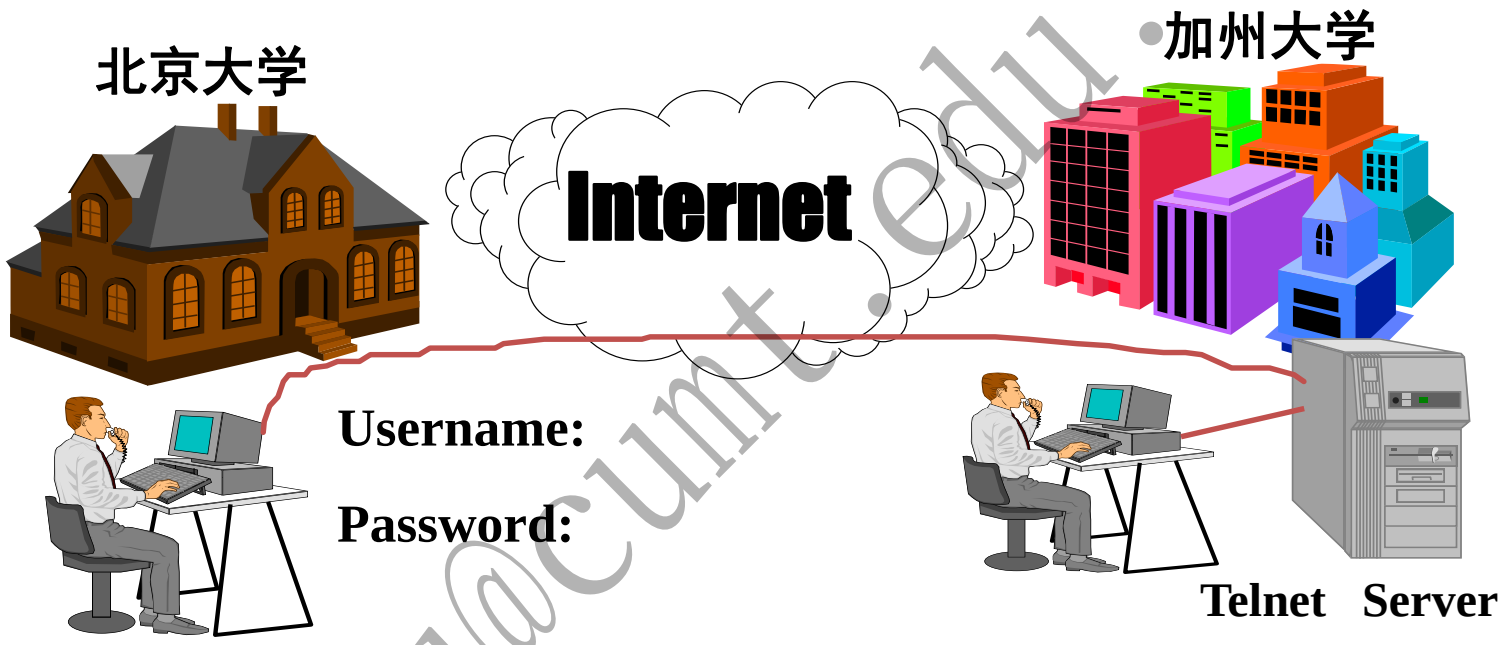
- 发送完一个文件块后就等待对方的确认，确认时应指明所确认的块编号。
- 发完数据后在规定时间内收不到确认就要重发数据 PDU。
- 发送确认 PDU 的一方若在规定时间内收不到下一个文件块，也要重发确认 PDU。这样就可保证文件的传送不致因某一个数据报的丢失而告失败。

Q10：怎么远程登录到另一个主机？

- TELNET 是一个简单的远程终端协议，也是因特网的正式标准。
- 用户用 TELNET 就可在其所在地通过 TCP 连接注册（即登录）到远地的另一个主机上（使用主机名或 IP 地址）。
- TELNET 能将用户的击键传到远地主机，同时也能将远地主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上。

客户–服务器方式

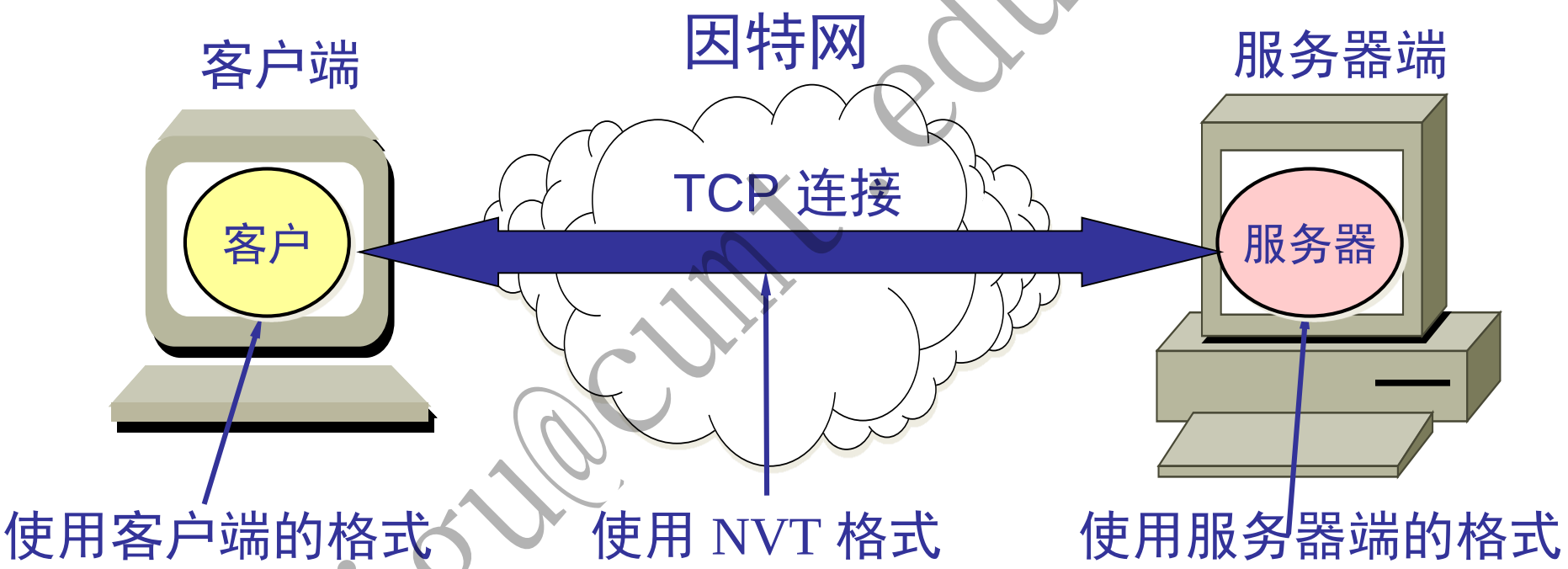
- 现在由于 PC 的功能越来越强，用户已较少使用 TELNET 了。
- TELNET 也使用客户–服务器方式。在本地系统运行 TELNET 客户进程，而在远地主机则运行 TELNET 服务器进程。
- 和 FTP 的情况相似，服务器中的主进程等待新的请求，并产生从属进程来处理每一个连接。



telnet 112.191.39.39

112.191.39.39/ 23

TELNET 使用
网络虚拟终端 NVT 格式

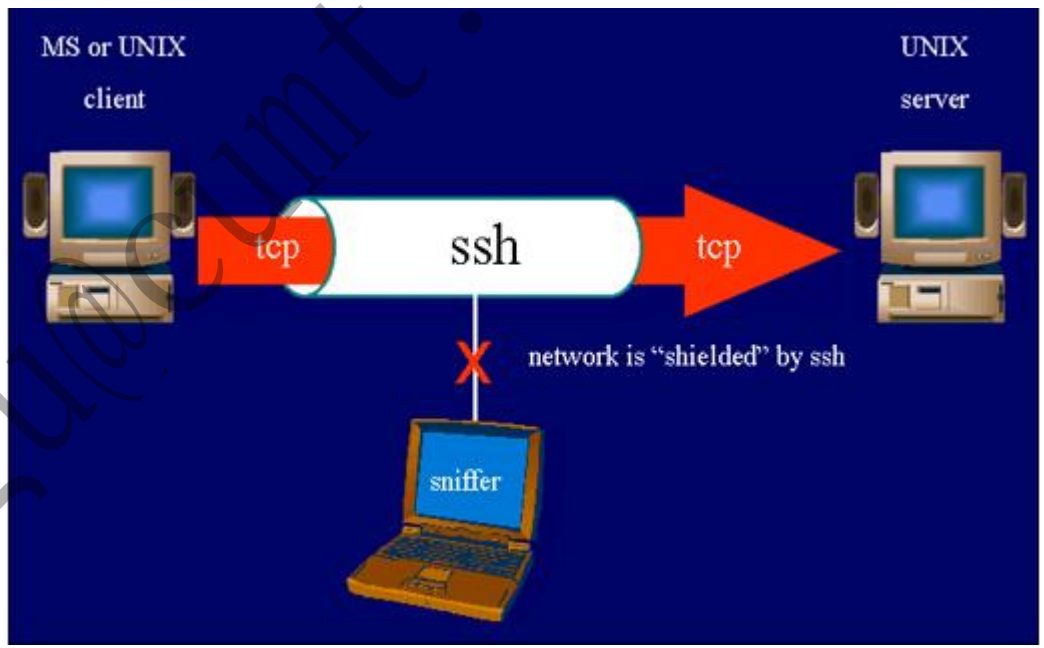


网络虚拟终端 NVT 格式

- 客户软件把用户的击键和命令转换成 NVT 格式，并送交服务器。
- 服务器软件把收到的数据和命令，从 NVT 格式转换成远地系统所需的格式。
- 向用户返回数据时，服务器把远地系统的格式转换为 NVT 格式，本地客户再从 NVT 格式转换到本地系统所需的格式。

安全的远程连接协议

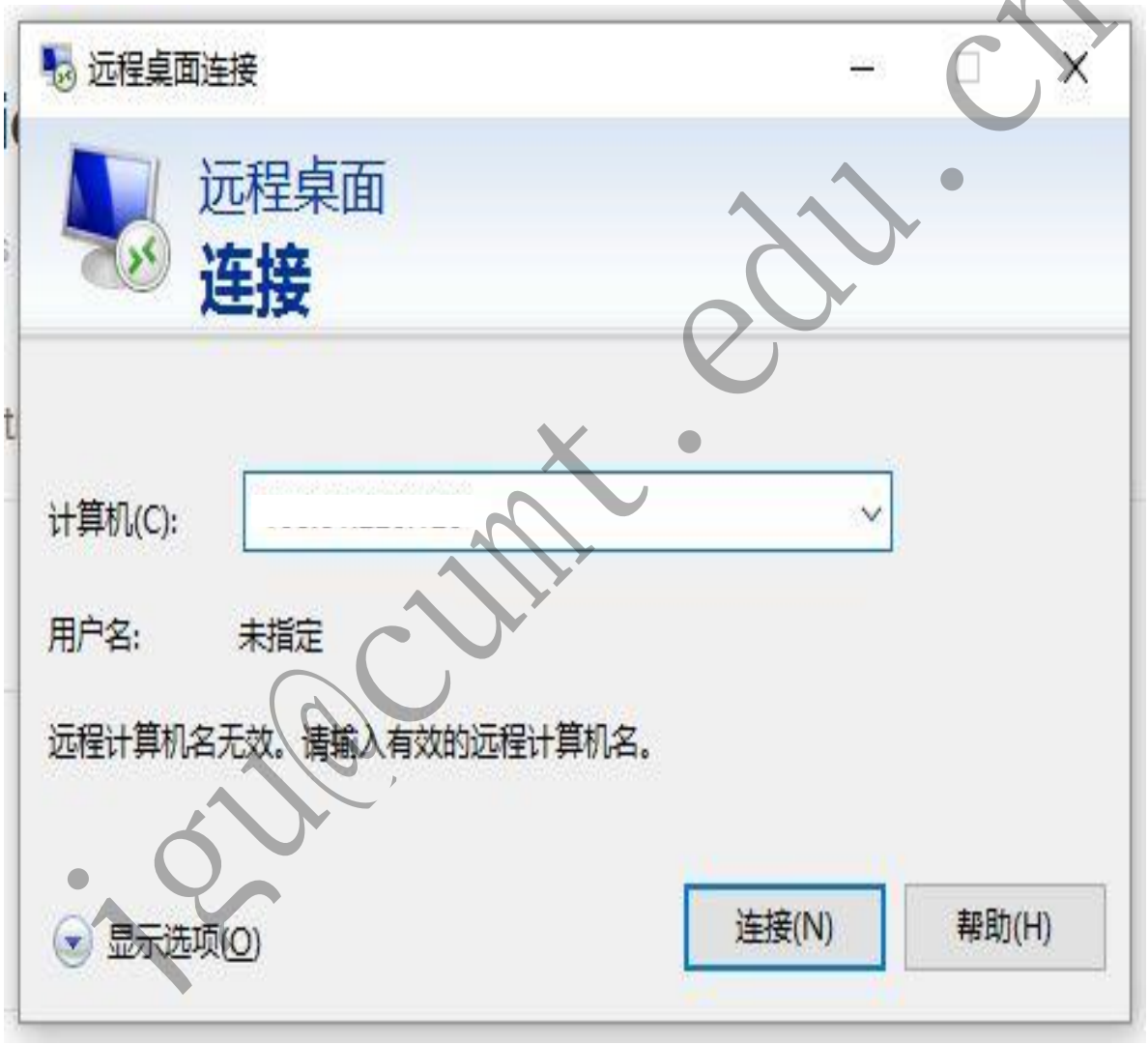
- telnet协议，明文传输数据，包括用户名和密码；
- ssh（Secure Shell）在传输数据之前，客户端与服务器端需要先建立加密通道，才能进行数据传输；
  - SSH最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。

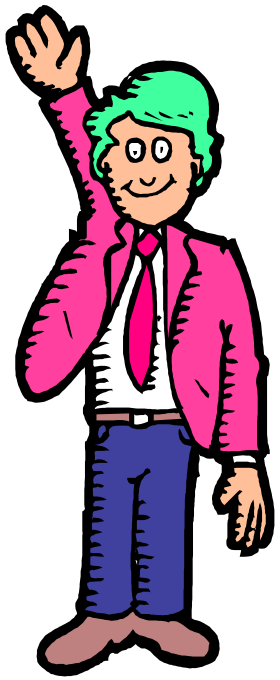


ssh的版本

- ✓ v1：基于CRC-32做MAC校验的方式，不太安全，容易收到中间人攻击，现在使用较少了；
- ✓ v2：双方主机协议选择安全的MAC校验方式；基于DH算法来做密钥交换，基于RSA或者DES算法来实现省份验证的；其中，DH非对称算法可以再不传输密钥的情况下，让对端算出私钥。

Windows的远程桌面链接





THANK YOU!