第6章　　应用层

第 6 章 应用层

6.1 域名系统 DNS

6.1.1 域名系统概述

6.1.2 因特网的域名结构

6.1.3 域名服务器

6.2 文件传送协议

6.2.1 FTP 概述

6.2.2 FTP 的基本工作原理

6.2.3 简单文件传送协议 TFTP

第 6 章 应用层（续）

6.3 远程终端协议 TELNET

6.4 万维网 WWW

- 6.4.1 概述
- 6.4.2 统一资源定位符 URL
- 6.4.3 超文本传送协议 HTTP
- 6.4.4 万维网的文档
- 6.4.5 万维网的信息检索系统

第 6 章 应用层（续）

6.5 电子邮件

6.5.1 电子邮件概述

6.5.2 简单邮件传送协议 SMTP

6.5.3 电子邮件的信息格式

6.5.4 邮件读取协议 POP3 和 IMAP

6.5.5 基于万维网的电子邮件

6.5.6 通用因特网邮件扩充 MIME

第 6 章 应用层（续）

6.6 动态主机配置协议 DHCP

6.7 简单网络管理协议 SNMP

- 6.7.1 网络管理的基本概念
- 6.7.2 管理信息结构 SMI
- 6.7.3 管理信息库 MIB
- 6.7.4 SNMP 的协议数据单元和报文

6.8 应用进程跨越网络的通信

- 6.8.1 系统调用和应用编程接口
- 6.8.2 几种常用的系统调用

引言

- 前面五章讨论了计算机网络提供通信服务的过程，但还没有讨论这些通信服务是如何提供给应用进程来使用。
- 本章讨论各种应用进程通过什么样的应用层协议来使用网络锁提供的通信服务。

应用层协议的特点

- 每个应用层协议都是为了解决某一类应用问题，而问题的解决又往往是通过位于不同主机中的多个应用进程之间的通信和协同工作来完成的。应用层的具体内容就是规定应用进程在通信时所遵循的协议。
- 应用层的许多协议都是基于客户服务器方式。客户(client)和服务器(server)都是指通信中所涉及的两个应用进程。客户服务器方式所描述的是进程之间服务和被服务的关系。客户是服务请求方，服务器是服务提供方。

应用层的协议

- DNS
- FTP
- HTTP
- DHCP

……

6.1 域名系统 DNS

6.1.1　域名系统概述

6.1.1　域名系统概述

（1）DNS的定义

- 域名系统 DNS （Domain Name System）

　　是因特网使用的命名系统，用来把便于用户使用的主机名（域名）转换为适合机器处理的IP地址。

6.1.1　域名系统概述

（2）DNS是分布式的数据库

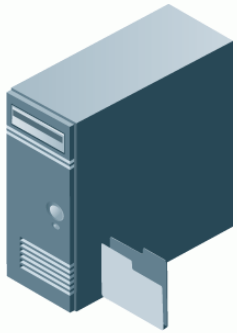
- 因特网的域名系统DNS被设计成为一个联机分布式数据库系统；
- 域名到IP地址的解析是由分布在因特网上的许多域名服务器程序共同完成的。这种程序在专设的节点上运行，所以把**运行域名服务器程序的机器称为域名服务器**。

6.1.1　域名系统概述

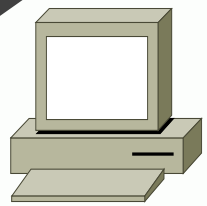
（3）DNS的基本解析过程

- DNS采用客户——服务器方式；

DNS服务器



DNS请求报文

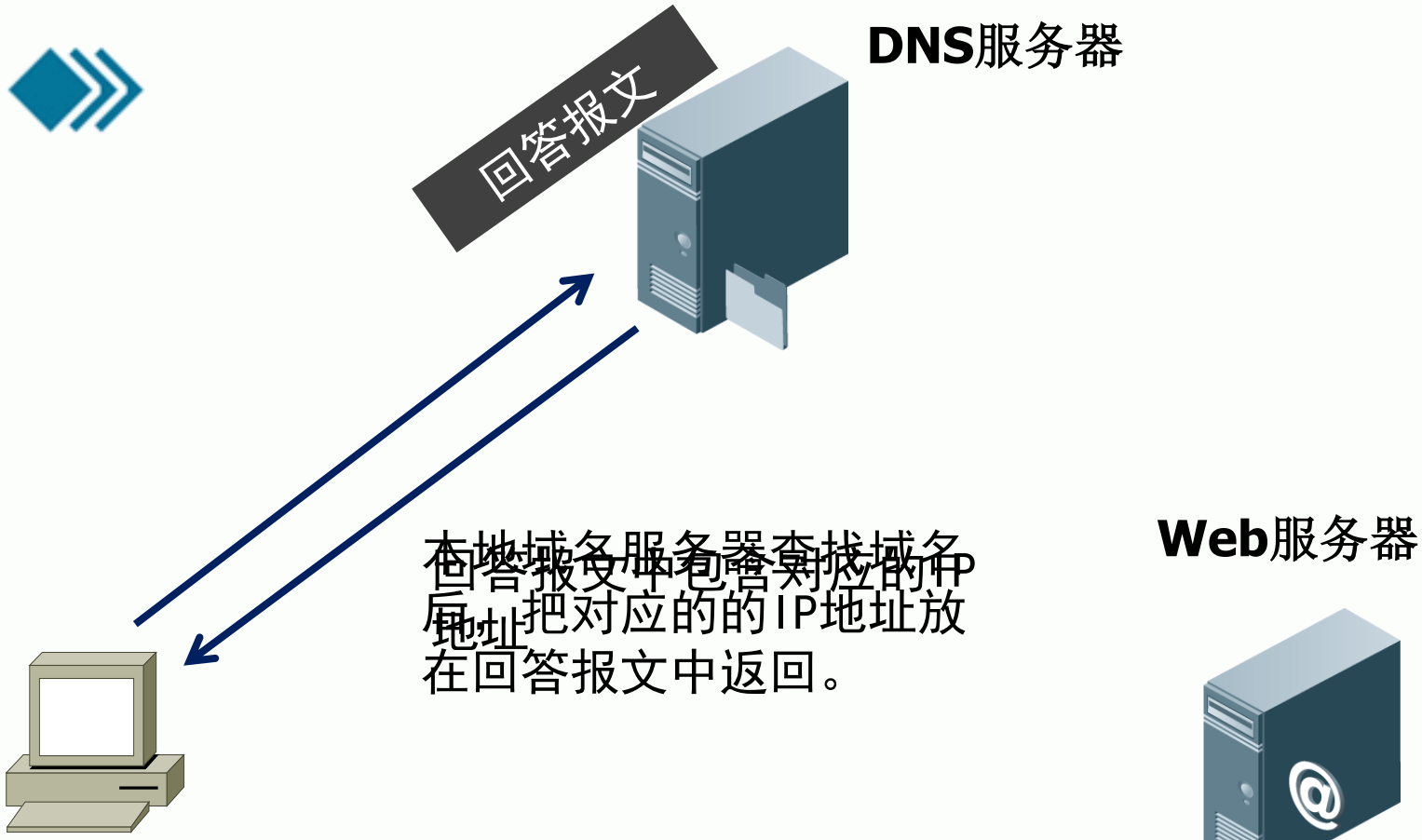


请求报文中包含待解析域名，以UDP用户数据报方式发给本地域名服务器

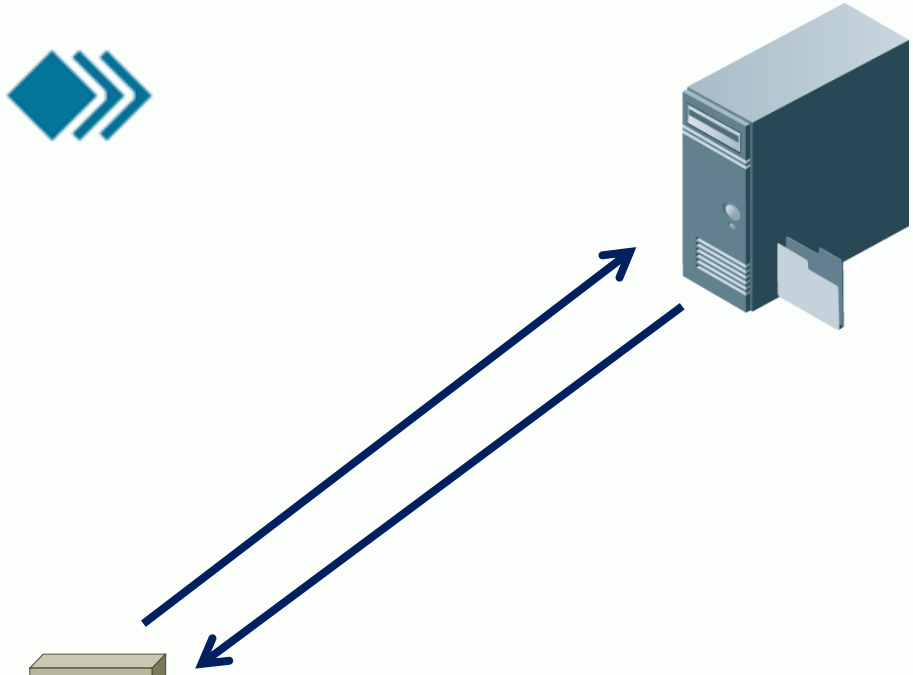
询问DNS服务器发送域名解析请求

Web服务器

访问：**www.sohu.com**

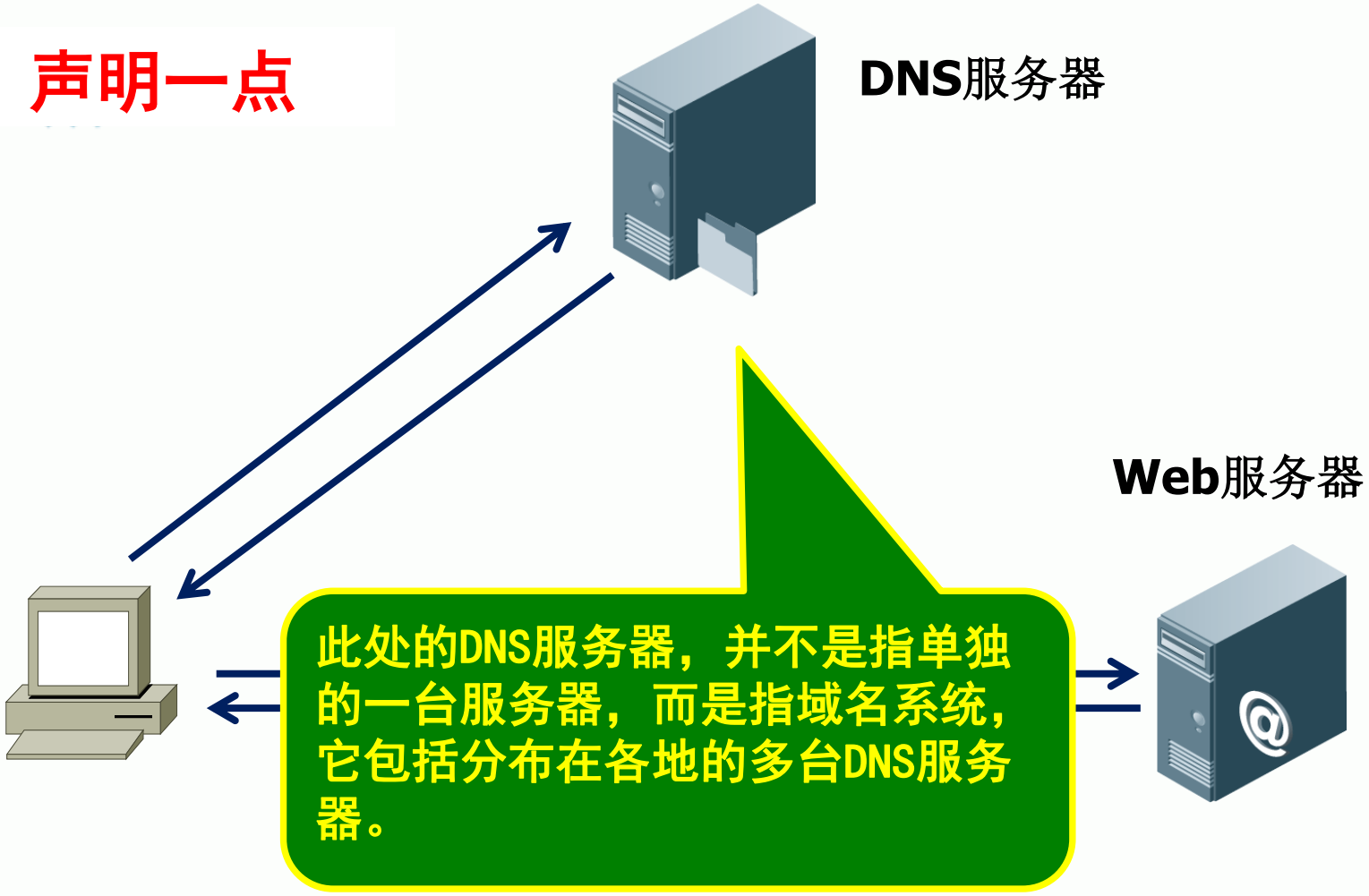


访问：**www.sohu.com**



客户端浏览器将服务器返回的信息组织成网页

➢ 声明一点


DNS服务器
Web服务器
此处的DNS服务器，并不是指单独的一台服务器，而是指域名系统，它包括分布在各地的多台DNS服务器。

6.1.1　域名系统概述

（3）DNS的解析过程分析

① 当某一个应用进程需要把主机名解析为IP地址时，该应用进程就调用解析程序，并成为DNS的一个客户，把待解析的域名放在DNS请求报文中，并以UDP用户数据报文方式发给本地域名服务器。（使用UDP减少开销）

② 本地域名服务器在查找域名后，把对应的IP地址放在回答报文中返回。

③ 应用进程获得目的主机的IP地址后即可进行通信。

（3）DNS的解析过程分析

若本地域名服务器不能回答该请求，则此域名服务器就暂时成为DNS中的另一个客户，并向其他域名服务器发出查询请求。这种过程直至找到能够回答该请求的域名服务器为止。

6.1.1　域名系统概述

（4）对域名系统（DNS）的进一步认识

- DNS为域名系统(Domain Name System)，一种组织成域层次结构的计算机网络服务命名系统，提供了将域名转换为ip地址的一种方法。
- DNS基于UDP协议，工作于应用层
- DNS采用C/S模式工作；
- 用户只能**间接的**使用DNS；
- 客户端由操作系统支持，需要指定DNS服务器；
- 服务器存储域名与ip的对照表，负责进行地址解析.

6.1.2　因特网的域名结构

6.1.2 因特网的域名结构

（1）层次树状结构

- 因特网采用了层次树状结构的命名方法。
- 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。

6.1.2 因特网的域名结构

（2）域名和IP地址的关系

- 域名只是个逻辑概念，并不代表计算机所在的物理地点。
- 变长的域名和使用有助记忆的字符串，是为了便于人来使用。而 IP 地址是定长的 32 位二进制数字则非常便于机器进行处理。
- 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。

6.1.2 因特网的域名结构

（3）顶级域名 TLD（Top Level Domain)

- 国家顶级域名：.cn 表示中国，.us 表示美国，.uk 表示英国，等等。
- 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）

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）

6.1.2 因特网的域名结构

（3）顶级域名 TLD（Top Level Domain)

- 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，即从IP地址解析为域名 ，因此又称为反向域名。

6.1.2 因特网的域名结构

（4）我国的二级域名

- 在国家顶级域名下注册的二级域名均由该国家自行确定。
- 我国在国际互联网络信息中心（Inter NIC）正式注册并运行的顶级域名是CN，这也是我国的一级域名。
- 在顶级域名之下，我国的二级域名又分为**类别域名**和**行政区域名**两类。

6.1.2 因特网的域名结构

（5）我国的二级域名——类别域名

- 类别域名共6个，包括：
  - 用于科研机构的ac；
  - 用于工商金融企业的com；
  - 用于教育机构的edu；
  - 用于政府部门的 gov；
  - 用于互联网络信息中心和运行中心的net；
  - 用于非盈利组织的org。

6.1.2 因特网的域名结构

（6）我国的二级域名——行政区域名

- **行政区域名有34个，分别对应于各省、自治区和直辖市。**
- BJ-北京市； SH-上海市； TJ-天津市； CQ-重庆市；HE-河北省； SX-山西省； NM -内蒙古自治区； LN-辽宁省； JL-吉林省； HL-黑龙江省； JS-江苏省； ZJ-浙江省；AH-安徽省； FJ-福建省； JX-江西省； SD-山东省；**HA-河南省**； HB-湖北省； **HN-湖南省**； GD-广东省；GX-广西壮族自治区； HI-海南省； SC-四川省； GZ-贵州省； YN -云南省； XZ-西藏自治区； SN-陕西省；GS-甘肃省； QH-青海省； NX-宁夏回族自治区； XJ-新疆维吾尔自治区； TW-台湾； HK-香港； MO-澳门。

6.1.2 因特网的域名结构

此外，从2002年12月份开始，CNNIC开放了国内.cn域名下的二级域名注册，可以在.CN下直接注册域名。

www.hactcm.edu.cn

www.hntcm.cn

（7）三级域名

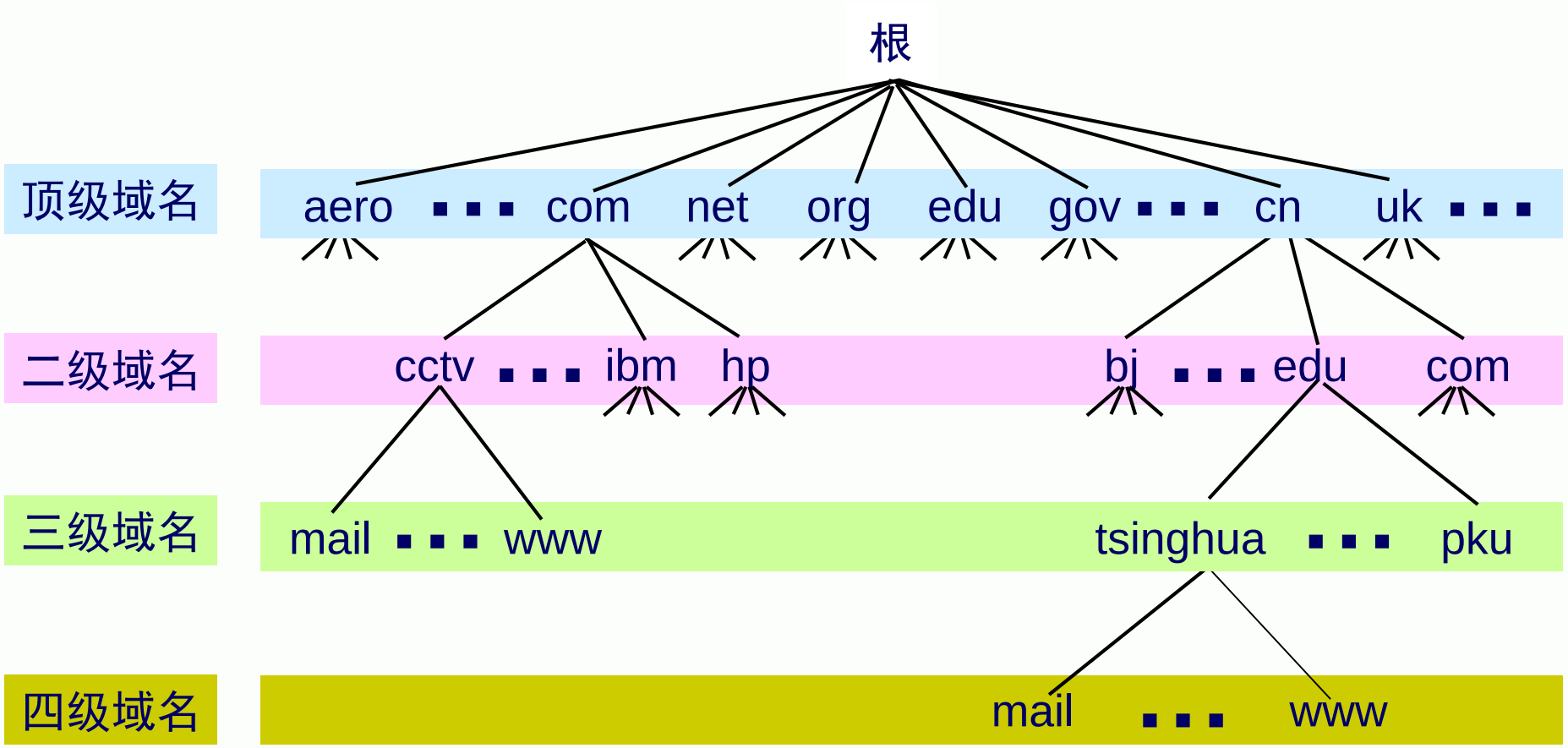
三级域名用字母（ A～Z，a～z，大小写等）、数字（0～9）和连接符（—）组成， 各级域名之间用实点（.）连接，三级域名的长度不能超过20个字符。如无特殊原因，建议采用申请人的英文名（或者缩写）或者汉语拼音名 （或者缩写） 作为三级域名，以保持域名的清晰性和简洁性。

6.1.2　因特网的域名结构

（8）树状域名空间

下图是因特网域名空间的结构，它实际上是一个倒过来的树。

因特网的域名空间

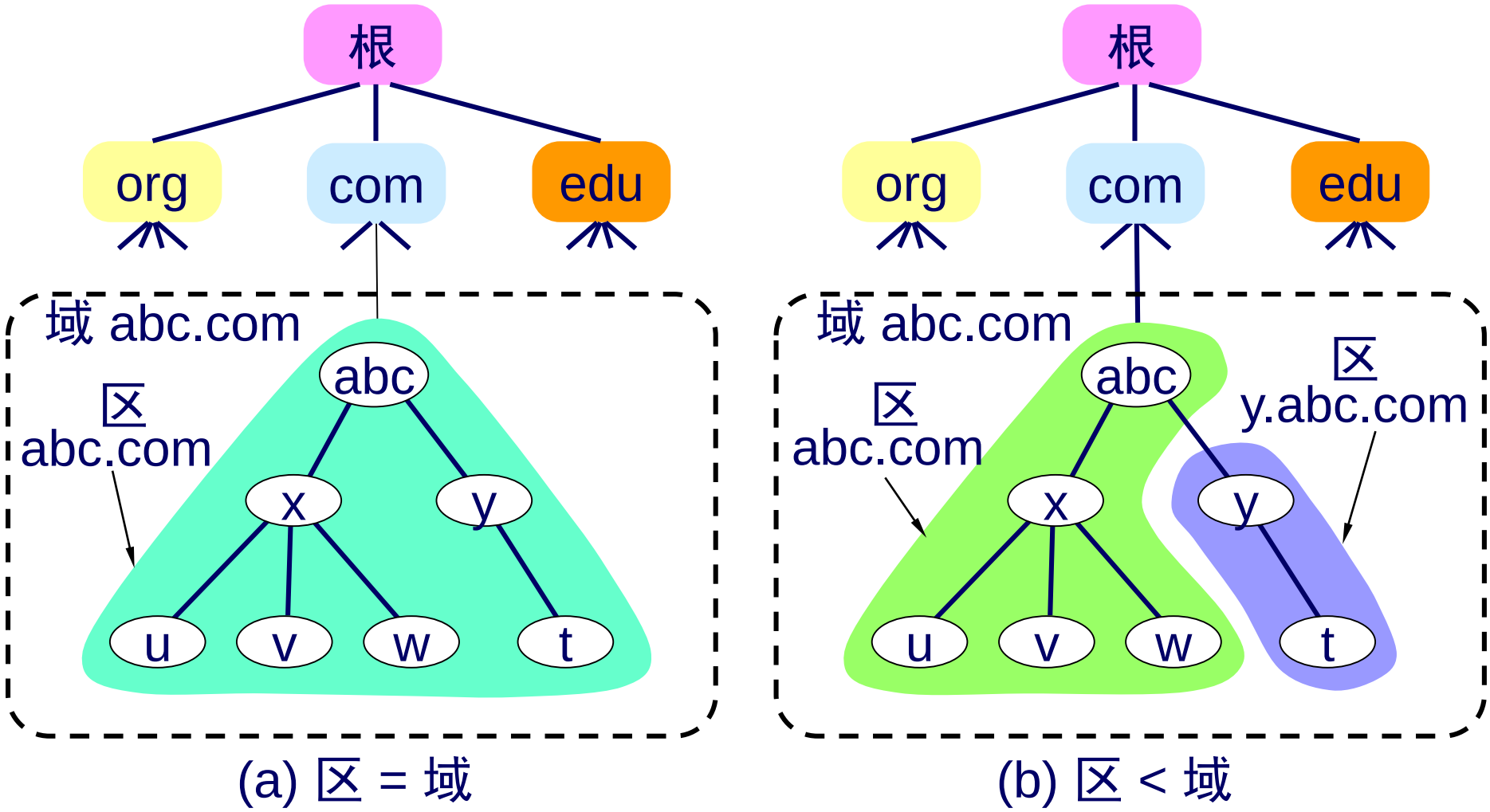

根
顶级域名
aero ▪▪▪ com net org edu gov ▪▪▪ cn uk ▪▪▪
二级域名
cctv ▪▪▪ ibm hp
bj ▪▪▪ edu com
三级域名
mail ▪▪▪ www
tsinghua ▪▪▪ pku
四级域名
mail ▪▪▪ www

6.1.3 域名服务器

6.1.3　域名服务器

- 整个域名系统的服务，是通过分布在各地的域名服务器来实现的。
- DNS 服务器的管辖范围不是以“域”为单位，而是以“区”为单位。
- 一个DNS服务器所负责管辖的（或有权限的）范围叫做区。一个区内设置的DNS服务器通常叫做权限域名服务器，用来保存该区中所有主机的域名到IP地址的映射。

区的不同划分方法举例

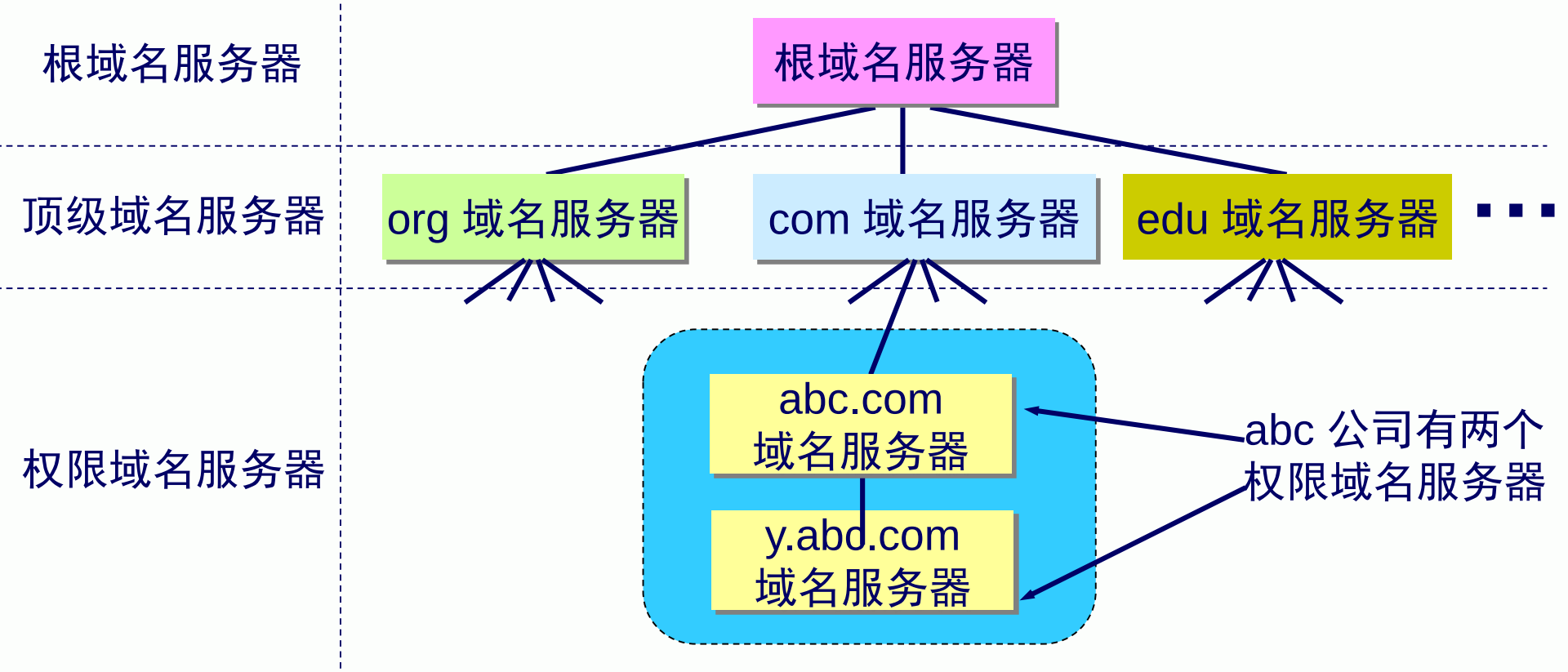

根
org
com
edu
域 abc.com
区
abc.com
abc
x
y
u
v
w
t
(a) 区 = 域
根
org
com
edu
域 abc.com
区
abc.com
区
y.abc.com
abc
x
y
u
v
w
t
(b) 区 < 域

6.1.3　域名服务器

（1）域名服务器的分类

- 因特网上的DNS域名服务器是按照层次安排的；
- 每一个域名服务器都只对域名体系中的一部分进行管辖；
- 根据域名服务器所起的作用，可以把域名服务器划分为以下四种不同的类型：
  - **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



6.1.3 域名服务器

（2）根域名服务器

- 是最高层次的域名服务器；
- 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。】
- 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）。

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

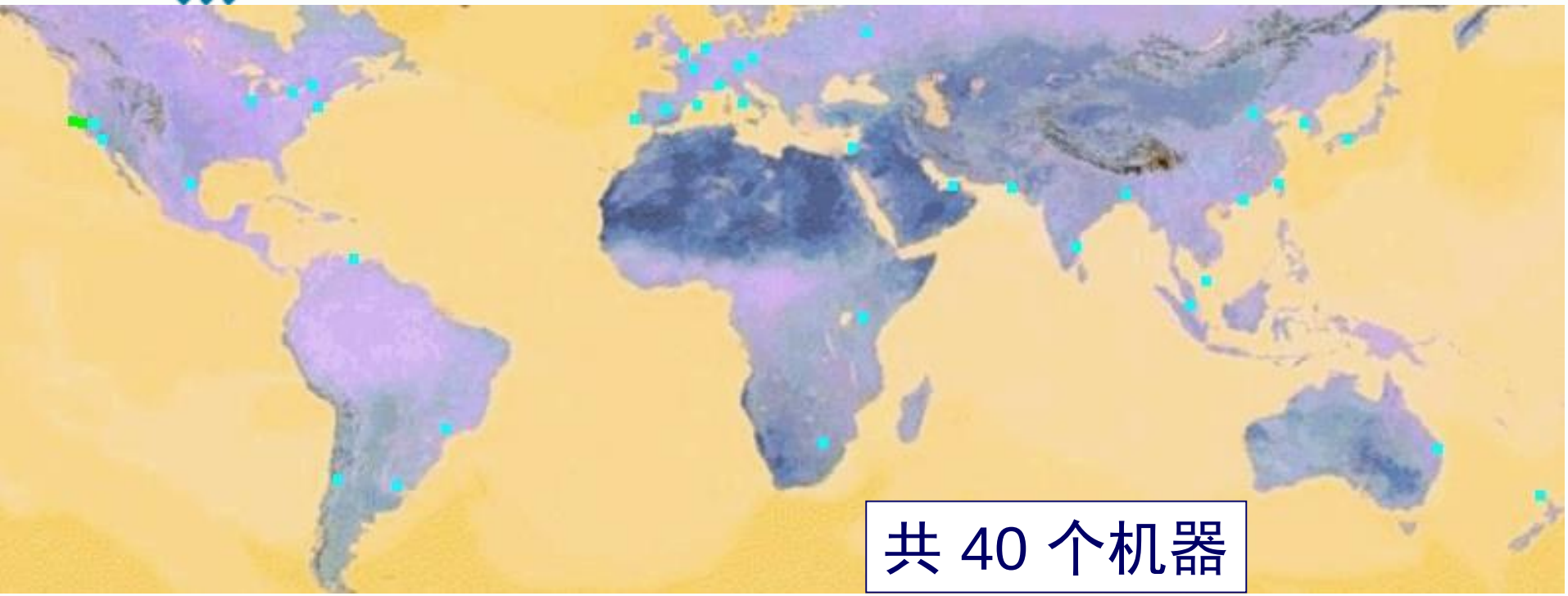
  b.rootservers.net

  …

  m.rootservers.net

- 到 2006 年底全世界已经安装了一百多个根域名服务器机器，分布在世界各地。
- 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 f 的地点分布图



- 通常，根域名服务器并不知道待查域名的 IP 地址，但它知道下一步去哪个顶级域名服务器查询。

6.1.3　域名服务器

（3）顶级域名服务器

- 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（权限域名服务器）的 IP 地址。

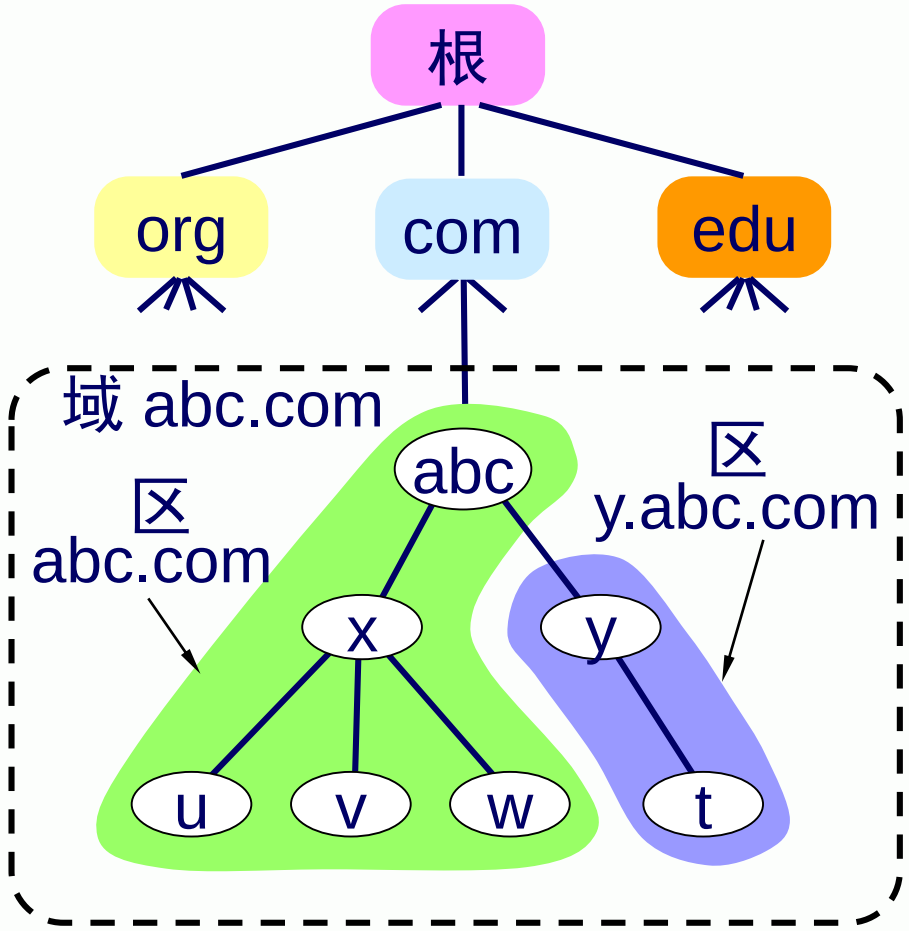
6.1.3 域名服务器

（4）权限域名服务器

- 这就是前面已经讲过的负责一个区的域名服务器。
- 通常权限域名服务器只接受本区域内的主机发出的域名解析请求，即需要权限。
- 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。 （举例）

（4）权限域名服务器

- 右图，区abc.com和区y.abc.com各有一个权限域名服务器。
- 访问t.y.abc.com

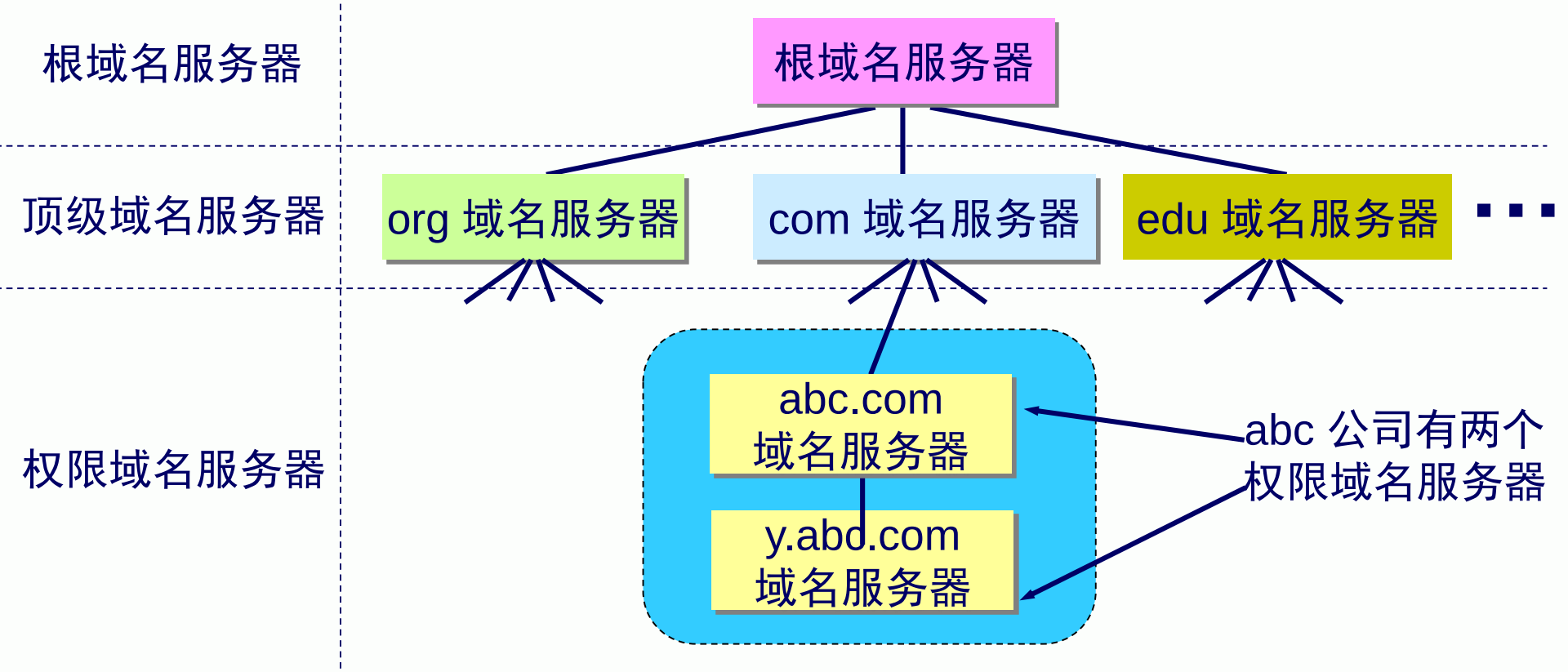


6.1.3　域名服务器

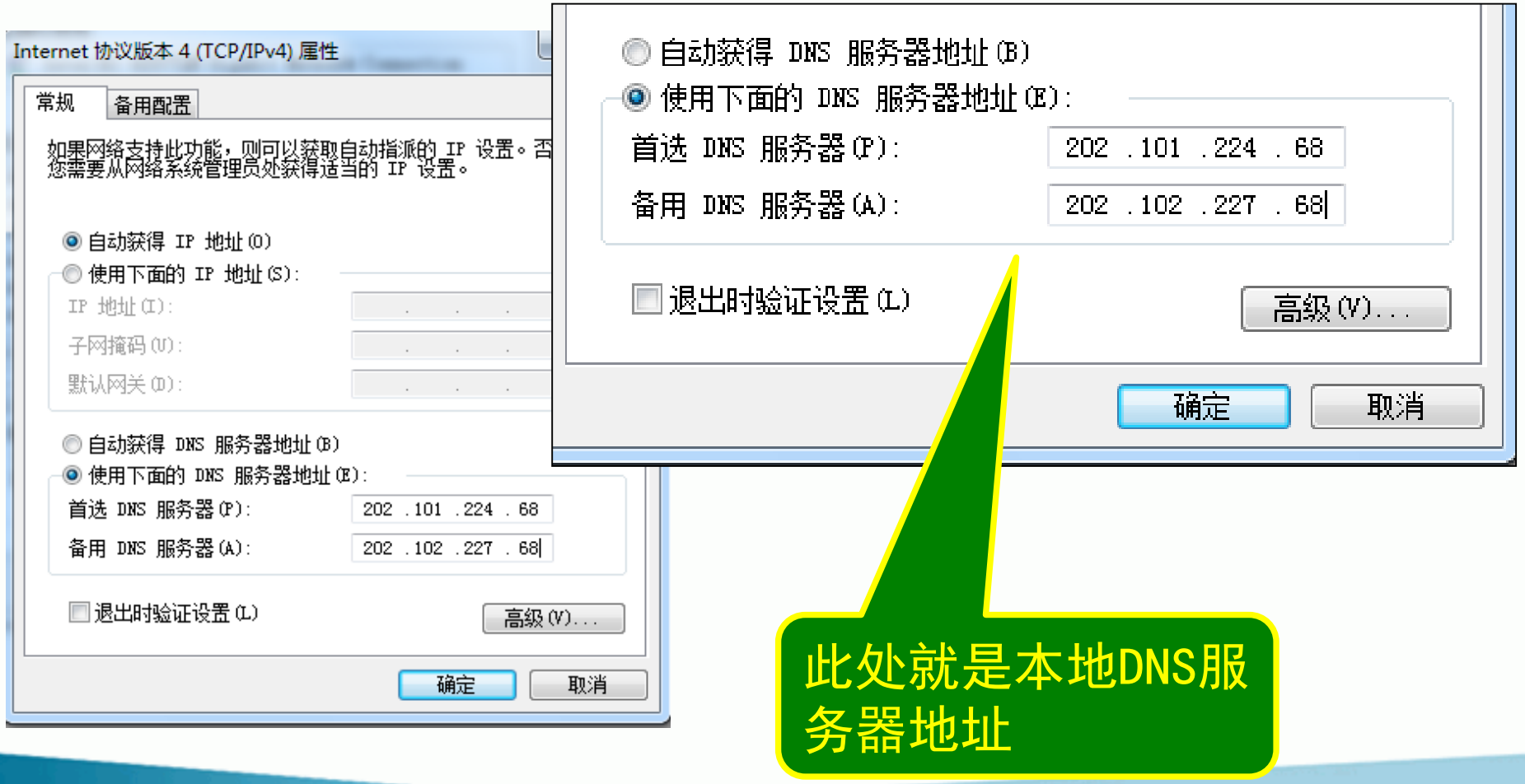
（5）本地域名服务器

- 不属于下页中的域名服务器层次结构；
- 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，

树状结构的 DNS 域名服务器



（5）本地域名服务器


Internet 协议版本 4 (TCP/IPv4) 属性
常规
备用配置
如果网络支持此功能，则可以获取自动指派的 IP 设置。否
您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I):
子网掩码(U):
默认网关(D):
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 202 .101 .224 . 68
备用 DNS 服务器(A): 202 .102 .227 . 68
退出时验证设置(L)
高级(V)...
确定
取消
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 202 .101 .224 . 68
备用 DNS 服务器(A): 202 .102 .227 . 68
退出时验证设置(L)
高级(V)...
确定
取消
此处就是本地DNS服务器地址

6.1.3　域名服务器

（6）主域名服务器与辅助域名服务器

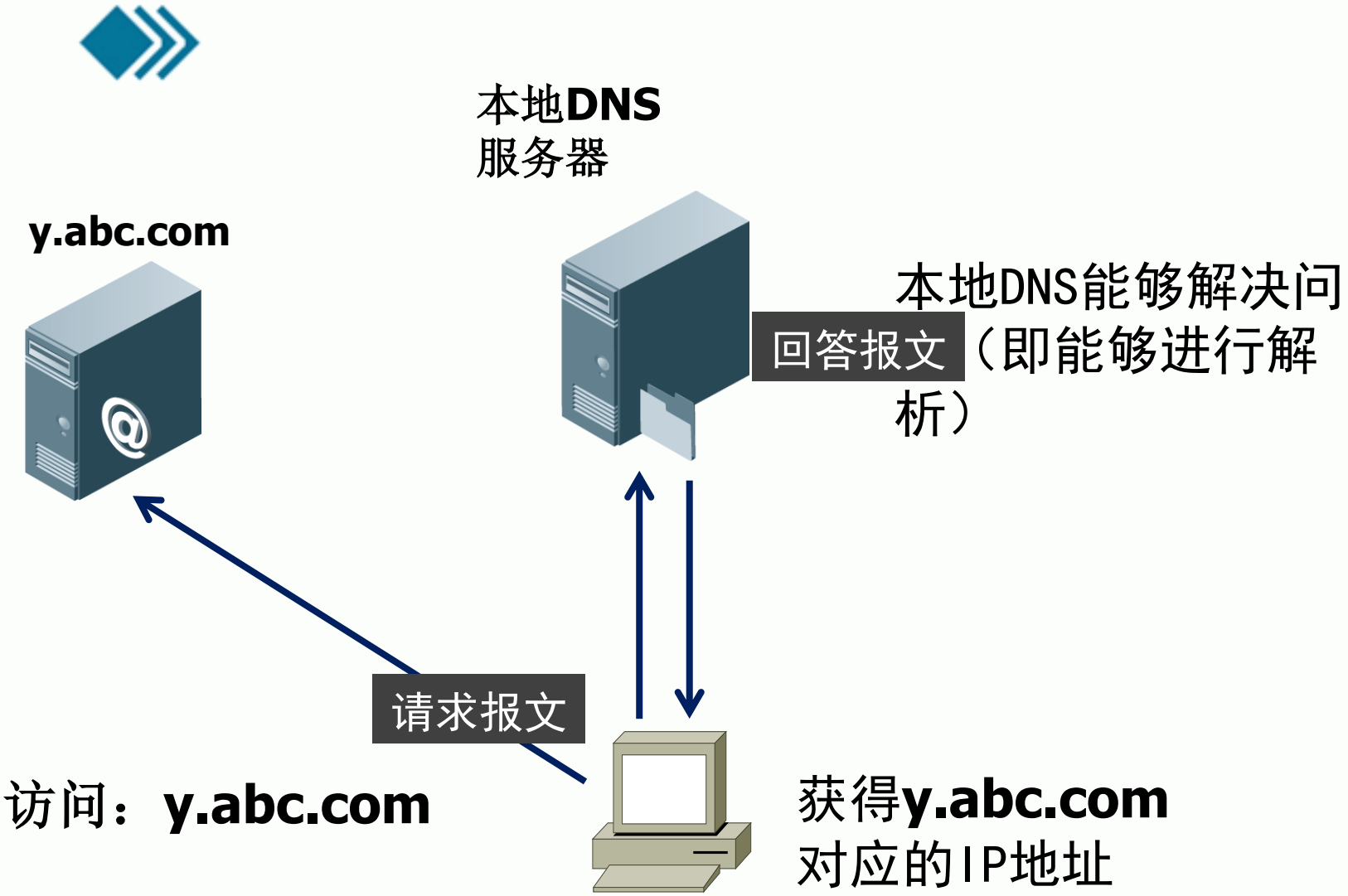
- 为了提高域名服务器的可靠性，DNS 域名服务器都把数据复制到几个域名服务器来保存，其中的一个是主域名服务器，其他的是辅助域名服务器。
- 当主域名服务器出故障时，辅助域名服务器可以保证 DNS 的查询工作不会中断。
- 主域名服务器定期把数据复制到辅助域名服务器中，而更改数据只能在主域名服务器中进行。这样就保证了数据的一致性。

6.1.4　域名的解析过程

6.1.4　域名的解析过程

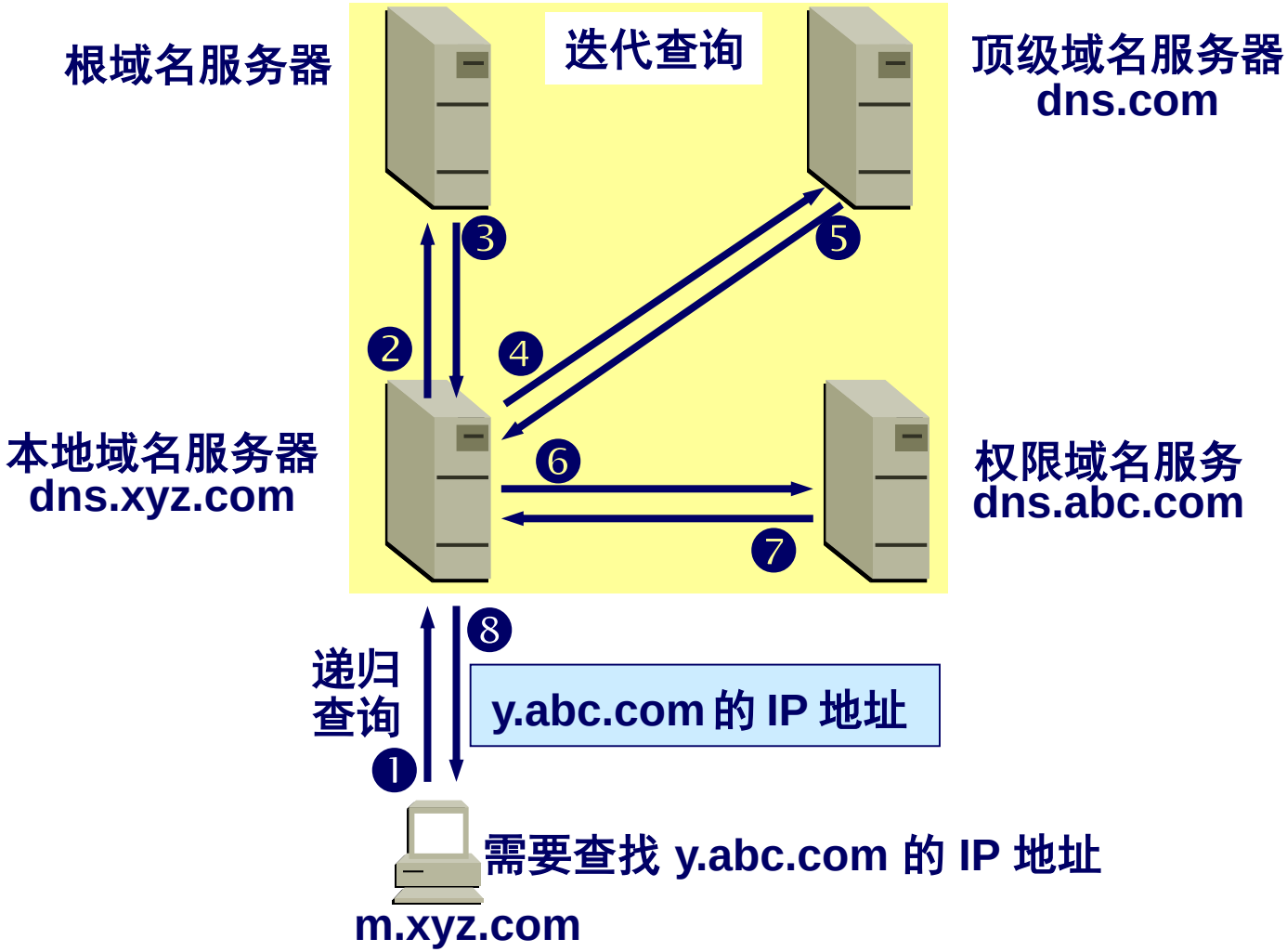
（1）从客户机到本地DNS服务器

- 第一步：客户机提出域名解析请求,并将该请求发送给本地的域名服务器。
- 　第二步：当本地的域名服务器收到请求后,就先查询本地的缓存,如果有该纪录项,则本地的域名服务器就直接把查询的结果返回。
- 　第三步：如果本地的缓存中没有该纪录,则本地域名服务器就直接把请求发给根域名服务器,然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域)的主域名服务器的地址。

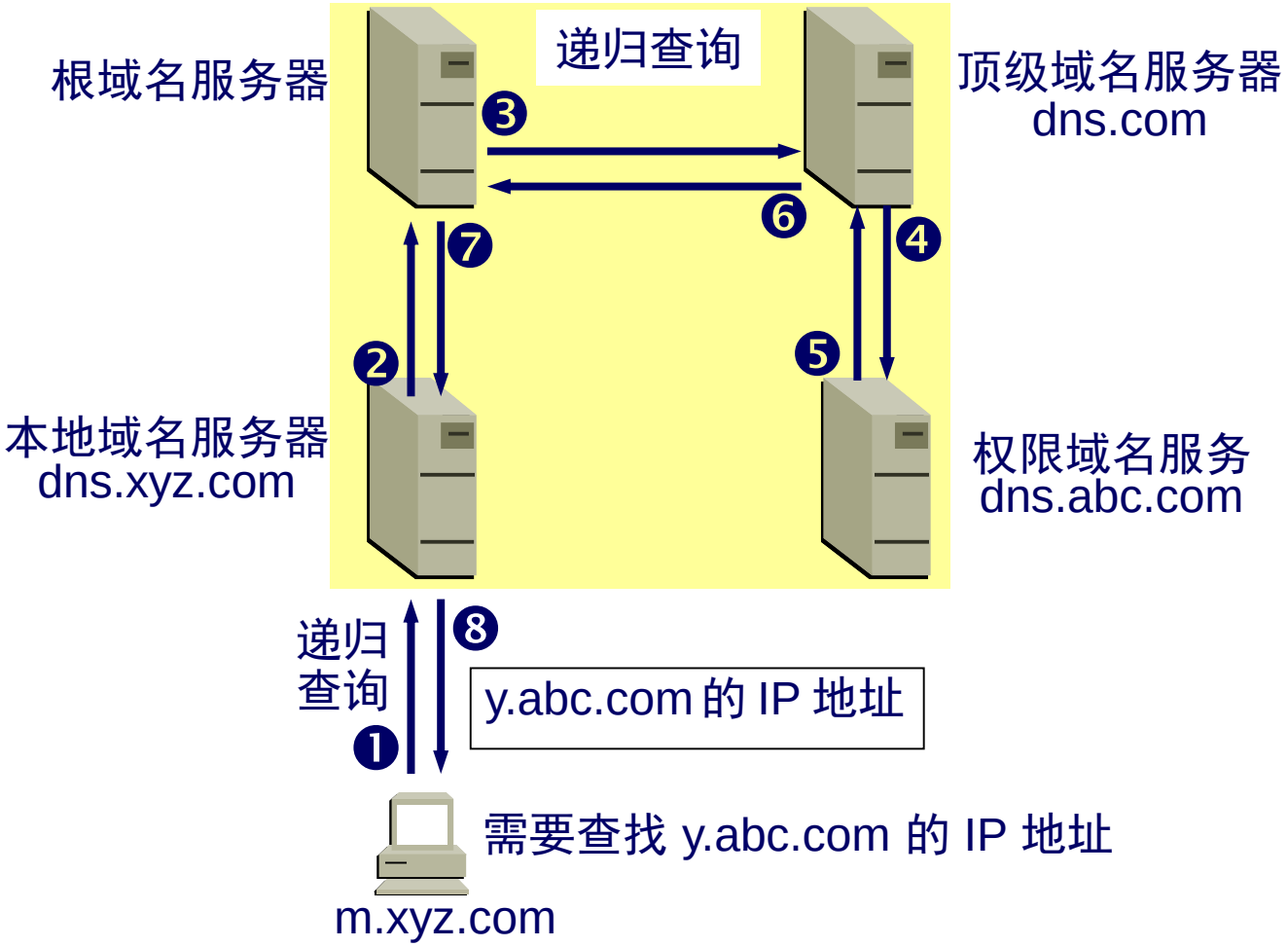

本地DNS
服务器
y.abc.com
回答报文
本地DNS能够解决问
（即能够进行解
析）
请求报文
访问：y.abc.com
获得y.abc.com
对应的IP地址

如果本地DNS服务器不能解决问题，怎么办？

（2）方式1：本地域名服务器采用迭代查询



（3）方式2：本地域名服务器采用递归查询



6.1.4　域名的解析过程

- 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。

6.1.4　域名的解析过程

（4）DNS服务器的高速缓存

- 为了提高查询效率，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）。

6.1.4　域名的解析过程

（6）解析过程总结

① 客户端提出域名解析请求，并将该请求发或转发给本地的DNS服务器。

② 接着，本地DNS服务器收到请求后就去查询自己的缓存，如果有该条记录，则会将查询的结果返回给客户端。

③ 反之，如果本地DNS服务器没有搜索到相应的记录，则会把请求转发到根DNS（13台根DNS服务器的IP信息默认均存储在DNS服务器中，当需要时就会去有选择性的连接）。

6.1.4　域名的解析过程

（6）解析过程总结

④ 然后，根DNS服务器收到请求后会判断这个域名是谁来授权管理，并会返回一个负责该域名子域的DNS服务器地址。比如，查询www.163.com的 IP，根DNS服务器就会在负责.com顶级域名的DNS服务器中选一个（并非随机，而是根据空间、地址、管辖区域等条件进行筛选），返回给本地DNS服务器。可以说根域对顶级域名有绝对管理权，自然也知道他们的全部信息，因为在DNS系统中，上一级对下一级有管理权限，毫无疑问，根DNS是最高一级了。

6.1.4　域名的解析过程

（6）解析过程总结

⑤　本地DNS服务器收到这个地址后，就开始联系对方并将此请求发给他。负责.com域名的某台服务器收到此请求后，如果自己无法解析，就会返回一个管理.com的下一级的DNS服务器地址给本地DNS服务器，也就是负责管理163.com的DNS。

⑥ 当本地DNS服务器收到这个地址后，就会重复上面的动作，继续往下联系。

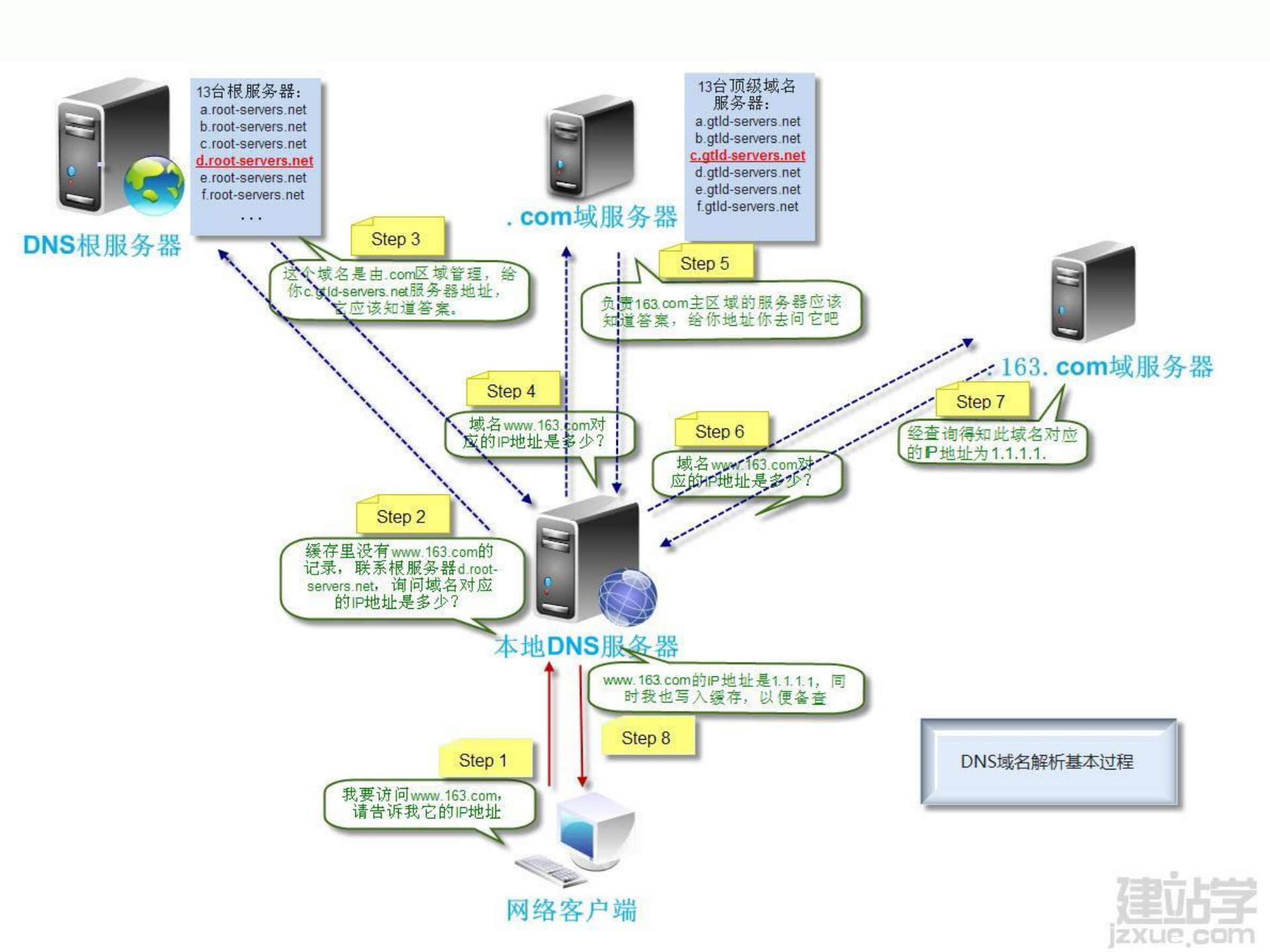
6.1.4　域名的解析过程

（6）解析过程总结

⑦ 不断重复这样的轮回过程，直到有一台DNS服务器可以顺利解析出这个地址为止。在这个过程中，客户端一直处理等待状态，他不需要做任何事，也做不了什么。

⑧ 直到本地DNS服务器获得IP时，才会把这个IP返回给客户端，到此在本地的DNS服务器取得IP地址后，查询就算完成了。本地DNS服务器同时会将这条记录写入自己的缓存，以备后用。

⑨ 到此，整个解析过程完成。



DNS的故事……

暴风影音断网事件

—— 2009年

暴风影音断网事件

2009年5月19日22时，工业和信息化部接到电信运营企业报告，自21时起，江苏、河北、山西、广西、浙江等省陆续出现互联网网络故障，部分互联网用户的服务受到影响。工业和信息化部对此高度重视，要求电信运营企业查明故障原因，及时采取有效措施，尽快恢复正常服务。

2009年 5月20日，工信部发布《情况通报》确认，此次故障原因是由于暴风网站的域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞，造成用户不能正常上网。 工信部确认原因是暴风影音网站受攻击。

暴风影音断网事件

20日，工业和信息化部组织相关单位和专家召开了研判会，分析故障原因。会议认为，由于baofeng.com网站的域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞，造成用户不能正常上网。

中国电信也已表示，由于暴风影音网站自身域名解析故障，导致中国电信DNS服务器访问量突增，网络处理性能下降。

暴风影音网站则表示，经过调查事故原因是DNS域名解析故障，网络故障造成多家网站受到影响，暴风也是受害者之一。

暴风影音断网事件

2009年5月19日21时起，中国互联网遭遇了 “多米诺骨牌”连锁反应，出现了大范围的网络故障。 关于网络故障的原因及技术原理，众说纷纭，莫衷一是。 对此，中国互联网络信息中心(CNNIC)副主任兼总工程师李晓东博士认为，引发本次网络故障的第一张骨牌是DNSPOD遭遇网络攻击，而安装有暴风影音的千万台电脑则成为引发整个网络故障连锁反应的重要推力。

解密中国网络故障“第一张骨牌”

暴风影音断网事件

BAOFENG.COM是北京暴风科技公司拥有的域名，用于其公司的各项互联网业务，该域名由北京暴风科技委托另外一家公司(DNSPOD.COM)代为运维管理，日常查询量比较大。

李晓东博士表示，此次故障的起源点在于DNSPOD.COM被人恶意大流量攻击，承担DNSPOD.COM网络接入的电信运营商断掉了其网络服务。 这是导致本次网络瘫痪的第一个骨牌。

暴风影音断网事件

李晓东表示，事实上，第一轮的网络故障早在当晚21时前就已开始。 当时，由于DNSPOD网络服务被中断，致使其无法为包括BAOFENG.COM在内的域名提供域名解析服务，诸多采用DNSPOD服务的网站无法访问。 这些采用DNSPOD服务的网站或者网络服务(包括暴风影音在内)同时成为此次网络故障的第二张骨牌。

本来DNSPOD的故障不一定会对互联网造成大面积的扩散影响，但是由于暴风影音的安装量巨大和网络服务的特性，使得暴风影音成为此次网络故障的焦点，被推向舆论的风头浪尖。

暴风影音断网事件

据了解，暴风影音软件的部分在线服务功能必须基于BAOFENG.COM域名的正常解析，DNSPOD网络服务被中断后，暴风影音的网络服务因此受到影响

暴风影音断网事件

李晓东表示，第三张骨牌就是电信运营商的本地域名服务器。 因软件网络服务的需要，使得安装有暴风影音的电脑不断发起域名解析请求，成为推倒第三张骨牌的重要推力。

根据域名系统的解析原理，由于本地域名服务器(专业上称为“递归服务器”)有地址缓存，超千万的暴风影音安装用户，仅需在本地网络接入服务商处就可查找到BAOFENG.COM的解析地址，找到暴风影音的网站。

暴风影音断网事件

安装了暴风影音软件的用户电脑产生的巨量域名请求拥塞了为这些用户提供服务的各地电信运营商的本地域名服务器，导致多个省份的本地域名服务器出现故障甚至无法提供正常服务，第三个骨牌就此岌岌可危乃至最终倒掉。

李晓东告诉记者，第三张骨牌是互联网服务的关键环节。电信运营商的本地域名服务器出现拥塞甚至无法服务后，使用这些本地域名服务器的其他互联网用户也无法上网，进而导致更大范围内的用户申报网络故障。

暴风影音断网事件

域名系统安全“牵一发而动全身”

域名作为广大民众访问互联网的起点和入口，是全球互联网通信的基础。 而域名系统作为承载全球亿万域名正常使用的系统，是互联网的基础设施，其作用相当于互联网的中枢神经系统，域名系统的故障会导致互联网陷入瘫痪。

暴风影音断网事件

完整的域名系统由递归域名服务系统(即本地域名服务器)、根域名服务系统、顶级域名服务系统以及各级域名服务系统等四个层级构成。 简单的说，广大民众访问一个网站或其他互联网服务时，需要在全球网络中完成对应四个层次的查询。 因此，任何一层出现故障，都会导致相应范围的网络应用瘫痪，大到一个国家和地区的网将络全面瘫痪，小到某个网站将无法访问。

李晓东表示，域名系统是一种公开服务，历来是被攻击的对象，从本次网络故障发生的过程来看，相关机构对域名系统的重要性认识不足，重视程度显然不够，安全保障能力比较低。

暴风影音断网事件

李晓东建议，一方面，提供公共域名服务的机构应提高自身安全防御和抗攻击能力；另一方面，拥有大量用户的互联网软件也应审慎考虑，优化软件安全性，避免一不小心成了分布式拒绝服务攻击(DDOS)的帮凶。

此次网络故障所涉的三张骨牌都是攻击受害者，估计黑客攻击DNSPOD时也没预料到攻击会产生如此恶劣的后果，最终酿成大范围的网络瘫痪。 域名系统就像是“空气”，平时我们感觉不到它的存在，但是一旦出现问题，其影响可能是“致命”的。 因此，李晓东呼吁：希望大家携手共同努力，重视并加大各个层级域名系统保护力度，为亿万网民营造一个“安全、可靠”的互联网环境。

暴风影音断网事件

附：BAOFENG.COM域名解析过程

在有本地缓存的情况下，本地域名服务器直接指向BAOFENG.COM域名服务器，无需再往上一级查询了。

说明：本次网络瘫痪的重要原因是，DNSPOD遭遇网络攻击，遭到电信运营商断网处理，致使其托管数十万域名无法正常解析。 通常情况下，如果是网民在地址栏输入“BAOFENG.COM”等托管域名，因为无法访问，网民就不会再次输入相关域名请求解析。

暴风影音断网事件

附：BAOFENG.COM域名解析过程

但是，本次网络瘫痪中，发起请求的不仅是网民，更多的是安装网民电脑中的暴风影音软件，它不像人是有智慧的，在访问不成功后会自动放弃，程序的设计导致其无法访问时会持续不断发起访问请求，而且这些请求全部拥塞在本地域名服务器中，无法转送到DNSPOD完成BAOFENG.COM解析，大量拥塞的请求占用了大量的服务器处理性能，进而导致本地域名服务器无法对其他的正常请求进行解析，并最终酿成大规模的网络故障

总结一下

本事件中涉及的对象

- PC: 网络中的主机（装有暴风影音）
- 公共DNS：电信、联通运营商DNS，（为广大用户提供DNS查询服务）；
- DNSPod：为暴风影音等网站提供DNS解析服务的域名解析服务提供商 ；
- 暴风影音网站服务器

关于DNSPod

域名被申请以后，有些网站维护者不愿意使用域名注册服务商提供的收费域名解析服务，于是大量的免费域名解析服务提供商成为了他们的选择，此次断网事件的主角之一——DNSPOD就是其中之一。

DNSPOD是国内著名的免费域名解析服务提供商，它拥有6台服务器，为全国13万网站提供域名解析服务，而此次断网事件的另一主角--国内著名视频播放软件暴风影音，就是其用户之一。

关于暴风影音

- 国内著名视频播放软件,暴风影音软件的装机量号称达到2亿以上，在中国普及率仅次于腾讯QQ,据称暴风用户同时在线人数达到上千万。

关于暴风影音

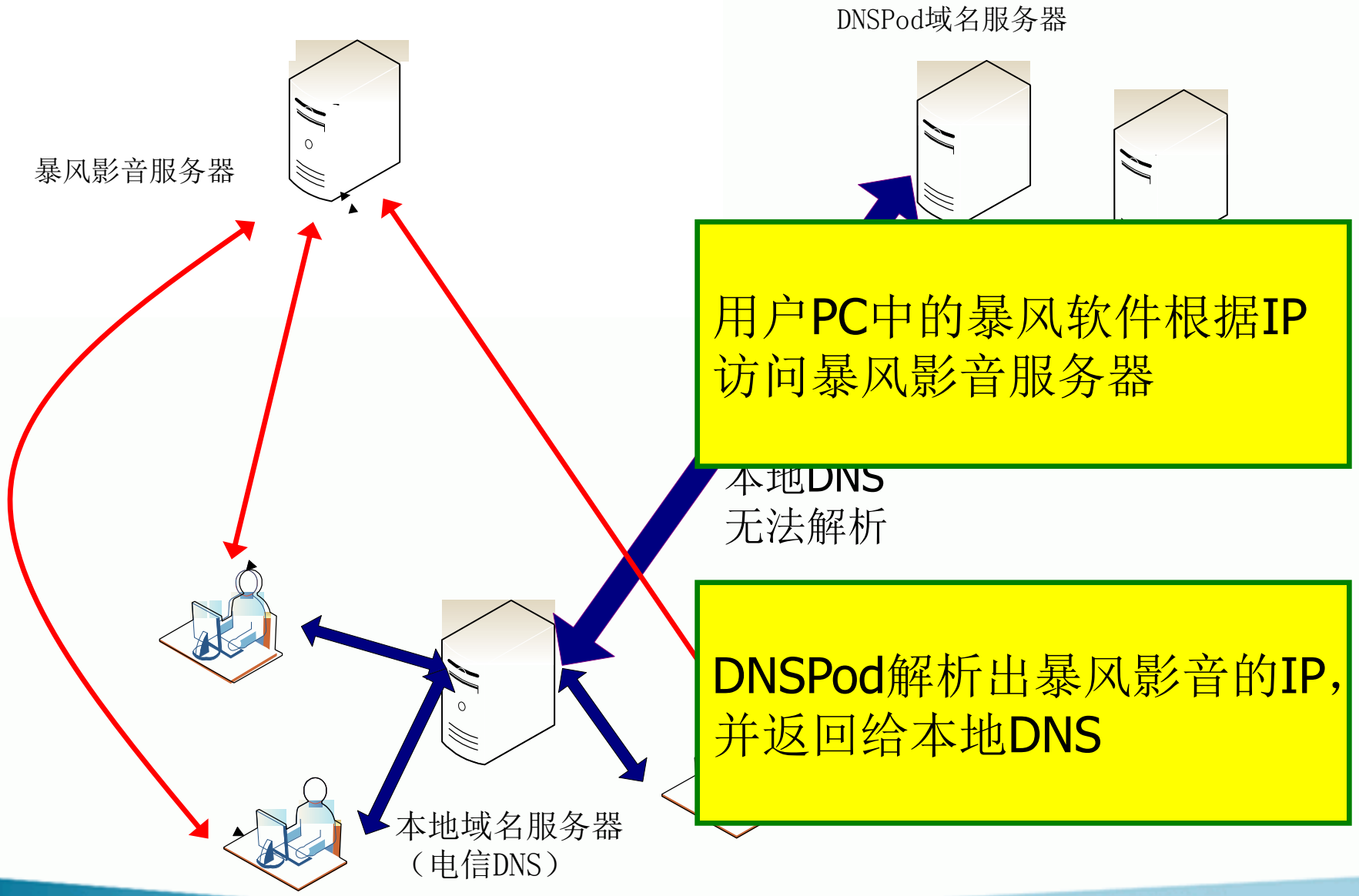
- 暴风影音含有一个名为stormliv的后台程序，只要用户安装了暴风影音，开机后就会自动运行，该自动运行程序为了躲避用户删除，使用“服务”的方式自动启动，在“管理工具”-“服务”中，找到一个名为“Contrl Center of Storm Media”的项目，将其禁用，才能停止其自动启动。

关于暴风影音

只要一开机，不管是否启动暴风影音主程序，该后台程序都会自动联网，并且访问暴风影音服务器（baofeng.com），进行更新程序，下载广告，报告无法播放文件类型等操作。

不仅如此，当遇到无法连接暴风服务器的情况时，该后台程序会不停的重试连接服务器，毫无意义的消耗本地和网络资源。

正常情况下的访问……


DNSPod域名服务器
暴风影音服务器
用户PC中的暴风软件根据IP访问暴风影音服务器
本地DNS
无法解析
DNSPod解析出暴风影音的IP，并返回给本地DNS
本地域名服务器
（电信DNS）

出现了什么问题？

DNSPOD被攻击

事件的起点是因为一家游戏私服为了商业利益，利用DDOS攻击另一家游戏私服，未能成功，于是前者转而攻击后者所使用的域名服务器DNSPOD，希望通过此举使对手的域名无法被解析，从而用户无法访问。DDOS造成的巨大流量马上就使DNSPOD的服务器全部瘫痪。

起初的状况

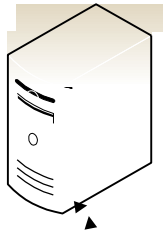
- 此时，尽管暴风影音的DNSPOD域名服务器无法访问，但之前访问过暴风影音的用户电脑里会暂时缓存暴风影音网站的ip地址，暂存时间从几秒到几分钟不等。
- 等这段时间过了以后，用户电脑缓存的ip过期，于是要访问暴风影音的用户向默认的域名服务器发送域名解析请求服务，比如北京的电信用户会向北京的DNS服务器发送请求。而默认的域名服务器也会缓存暴风影音的ip，一般会设置成3600秒，即一个小时，在这一个小时内，一切照旧，没有发生问题，用户照样可以顺利访问暴风影音。

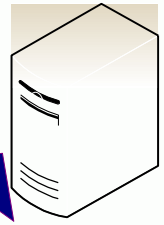
接下来的状况

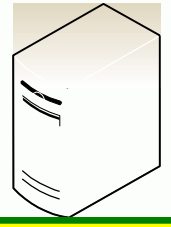
- 但一个小时后问题出现了，默认DNS服务器的缓存也过期了。
- 这个时候，DNS服务器内还会有一项或若干项称之为“NS”的纪录，该纪录记载了暴风影音的域名解析服务器即DNSPOD服务器的ip地址，这个记录一般会维持24小时。
- 但问题是这个ip地址的服务器已经被DDOS攻击以致瘫痪。于是，从这以后，用户要访问暴风影音，会向默认的DNS服务器发送域名解析请求，而该DNS服务器也没有暴风的ip纪录，于是会向DNSPOD的服务器发送域名解析请求，但是肯定没有反应。

DNSPod域名服务器

暴风影音服务器

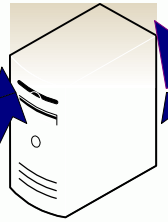


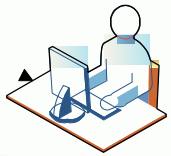




用户PC中的暴风软件不停的向本地DNS（电信DNS)发送查询请求。

DNSPod死了，无法解析出暴风影音的IP，返回失败报文

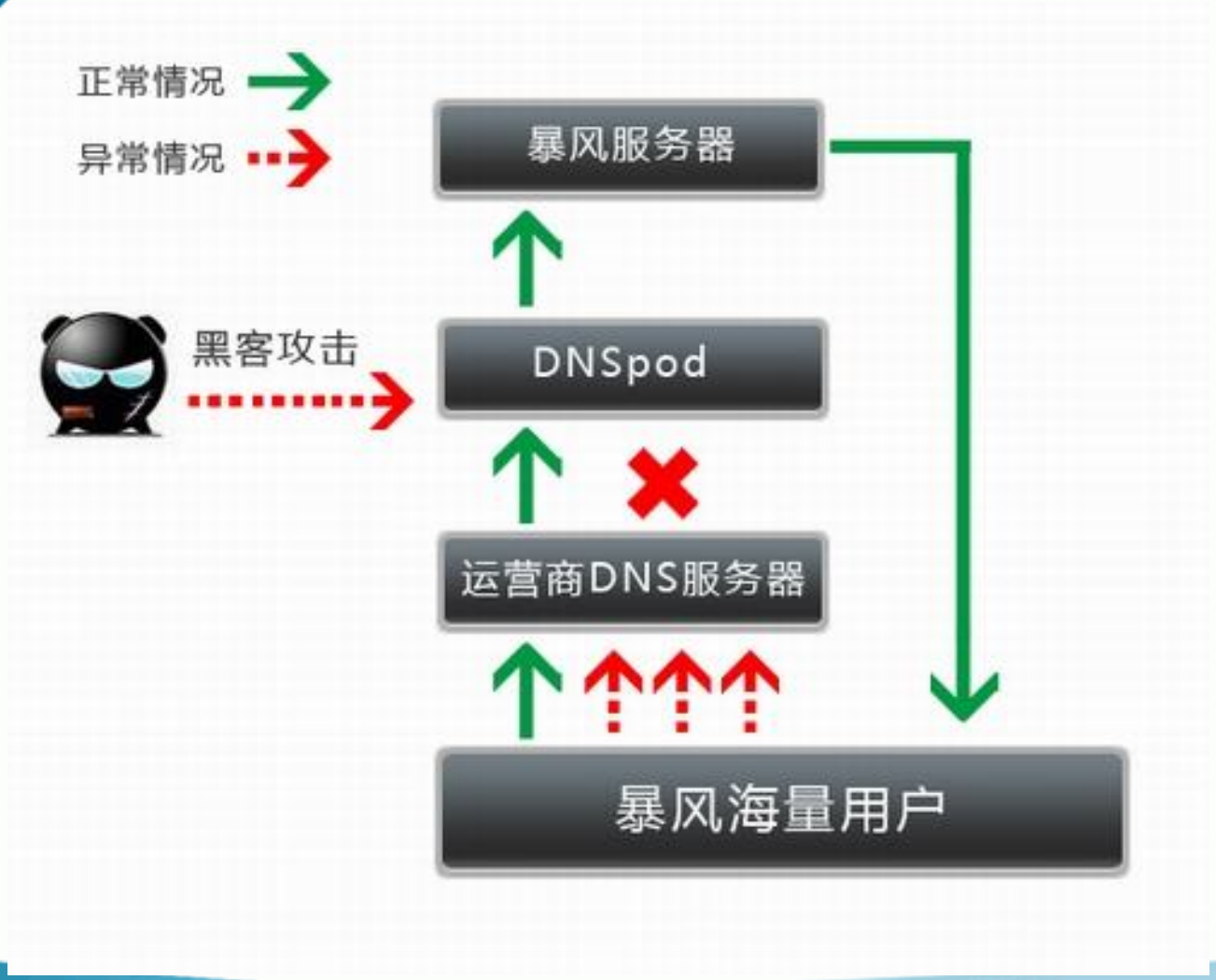




本地域名服务器
（电信DNS）

大麻烦来了！

- 在这种情况下应该停止继续联网查询，而暴风影音的stormliv后台进程却继续不断的发送请求，不断的失败又不断的发送。
- 由于默认域名服务器返回查询失败的报文要经过一到两秒，然后才能结束这次会话，处理速度跟不上暴风影音庞大用户群的大量查询请求，于是最后由于内存不足或连接数超过一定限额而最后拒绝服务。（电信的DNS死了！）
- 其他对于另外网站的域名解析请求也得不到相应，造成的结果就是不管访问哪个网站都无法得到域名解析的结果，所以无法访问。（大家都上不了网了！）


正常情况
异常情况
暴风服务器
黑客攻击
DNSpod
运营商DNS服务器
暴风海量用户

6.2　文件传送协议 FTP

6.2.1 FTP概述

6.2.1 FTP概述

- 文件传送协议 FTP（File Transfer Protocol）是因特网上使用得最广泛的文件传送协议,[RFC 959]。
- 因特网早期，用FTP传送文件约占整个因特网的通信量的三分之一，大于电子邮件的通信量，直到1995年，WWW通信量首次超过FTP
- 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 屏蔽了各计算机系统的细节，因而适合于在异构网络中任意计算机之间传送文件。

6.2.2　FTP 的基本工作原理

6.2.2 FTP 的基本工作原理

- 文件传送协议 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 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，负责启动FTP服务，并接受新的请求；另外有若干个从属进程，负责处理单个客户的具体请求。

6.2.2 FTP 的基本工作原理

（1）主进程的工作步骤如下

① 启动服务，打开熟知端口（端口号为 21），使客户进程能够连接上。

② 等待客户进程发出连接请求。

③ 当客户发出请求时，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。

④ 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。

6.2.2 FTP 的基本工作原理

（2）从属进程的工作

① 下图中的服务器中有两个从属进程：控制进程和数据传送进程。用来负责具体客户与服务器之间的文件传输。

② 在进行文件传输时，FTP的客户与服务器之间要建立两个并行的TCP连接：控制连接和数据连接。

③ 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。

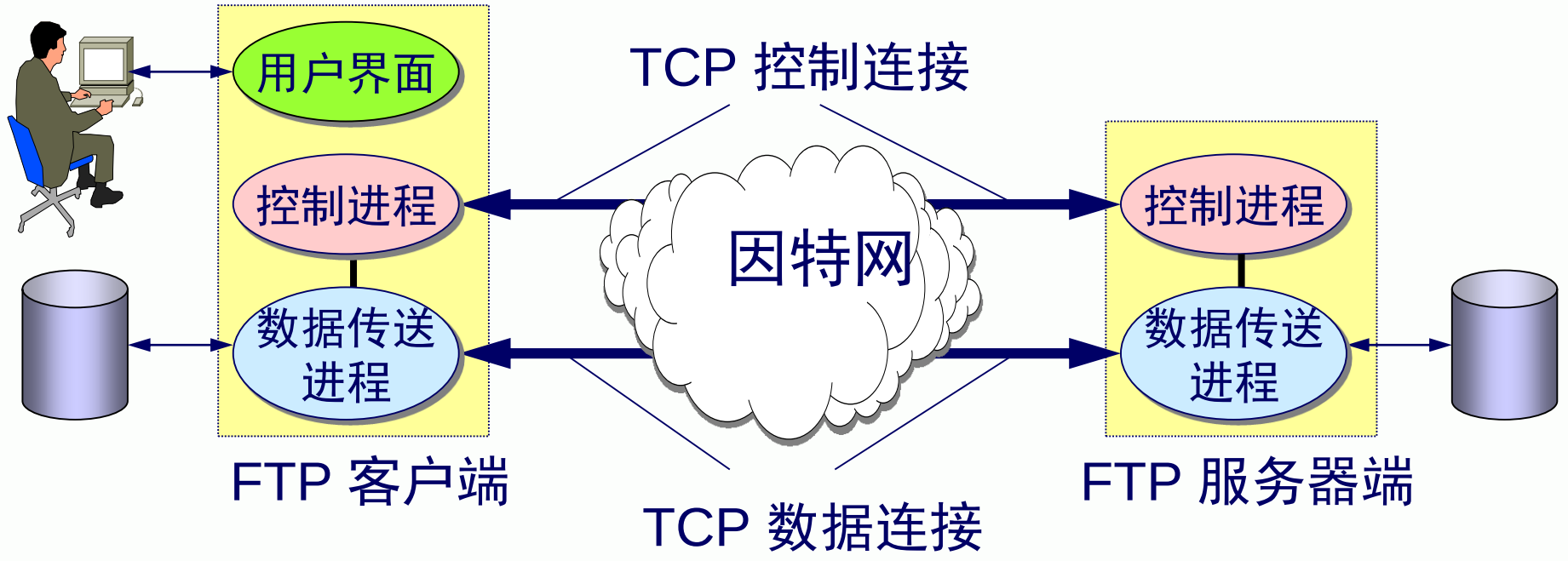
6.2.2 FTP 的基本工作原理

（2）从属进程的工作

④ 实际用于传输文件的是“数据连接”。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建“数据传送进程”和“数据连接”，用来连接客户端和服务器端的数据传送进程。

⑤ 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

6.2.2 FTP 的基本工作原理



6.2.2 FTP 的基本工作原理

（3）FTP服务中使用两个不同的端口号

- 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。

6.2.3 简单文件传送协议 TFTP (Trivial File Transfer Protocol)

6.2.3 简单文件传送协议 TFTP

（1）TFTP 的基本概念

- TFTP 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，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。

6.2.3 简单文件传送协议 TFTP

（2）TFTP 的主要特点是

- 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。
- 数据 PDU 也称为文件块(block)，每个块按序编号，从 1 开始。
- 支持 ASCII 码或二进制传送。
- 可对文件进行读或写。
- 使用很简单的首部。

6.2.3 简单文件传送协议 TFTP

（3）TFTP 的工作很像停止等待协议

- 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。

6.2.3 简单文件传送协议 TFTP

（3）TFTP 的工作很像停止等待协议

- 在一开始工作时。TFTP 客户进程发送一个读请求 PDU 或写请求 PDU 给 TFTP 服务器进程，其熟知端口号码为 69。
- TFTP 服务器进程要选择一个新的端口和 TFTP 客户进程进行通信。
- 若文件长度恰好为 512 字节的整数倍，则在文件传送完毕后，还必须在最后发送一个只含首部而无数据的数据 PDU。
- 若文件长度不是 512 字节的整数倍，则最后传送数据 PDU 的数据字段一定不满512字节，这正好可作为文件结束的标志。

6.3 远程终端协议 TELNET

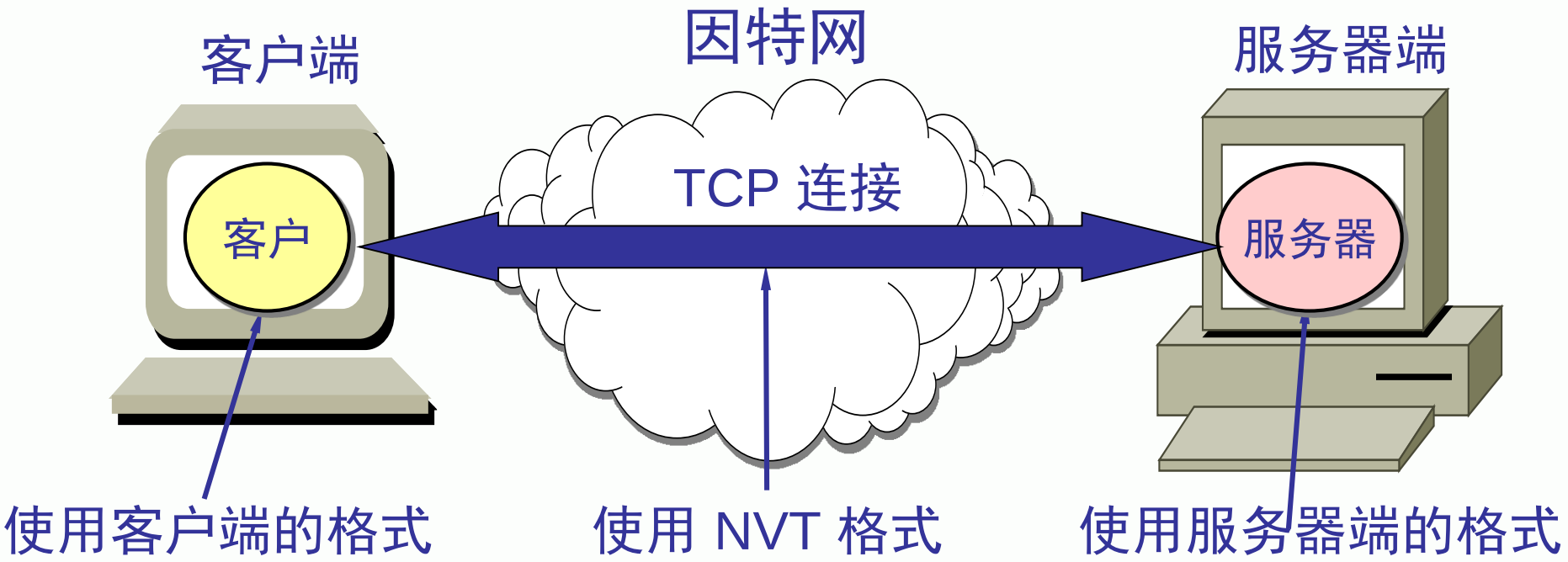
6.3 远程终端协议 TELNET

- 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。

6.3 远程终端协议 TELNET

- 现在由于 PC 机的功能越来越强，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 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。

6.6　动态主机配置协议 DHCP

6.6　动态主机配置协议 DHCP

6.6.1　DHCP应用背景

6.6.2　DHCP的基本工作原理

6.6.3　几个问题

6.6.4　关于DHCP relay

6.6.1 DHCP应用背景

（1）为什么需要DHCP

- 在协议软件中给这些参数赋值的动作叫做协议配置。
- 一个软件协议在使用之前必须是已正确配置的。
- 具体的配置信息有哪些则取决于协议栈。

6.6.1 DHCP应用背景

（1）为什么需要DHCP

例如，连接到因特网的计算机的协议软件需要配置的项目包括：

① IP 地址

② 子网掩码

③ 默认路由器的 IP 地址

④ 域名服务器的 IP 地址

- 这些信息通常存储在一个配置文件中，计算机在引导过程中可以对这个文件进行存取。

6.6.1 DHCP应用背景

（1）为什么需要DHCP

两种情况：

- 无盘工作站的上网
- 网络中的计算机经常改变位置

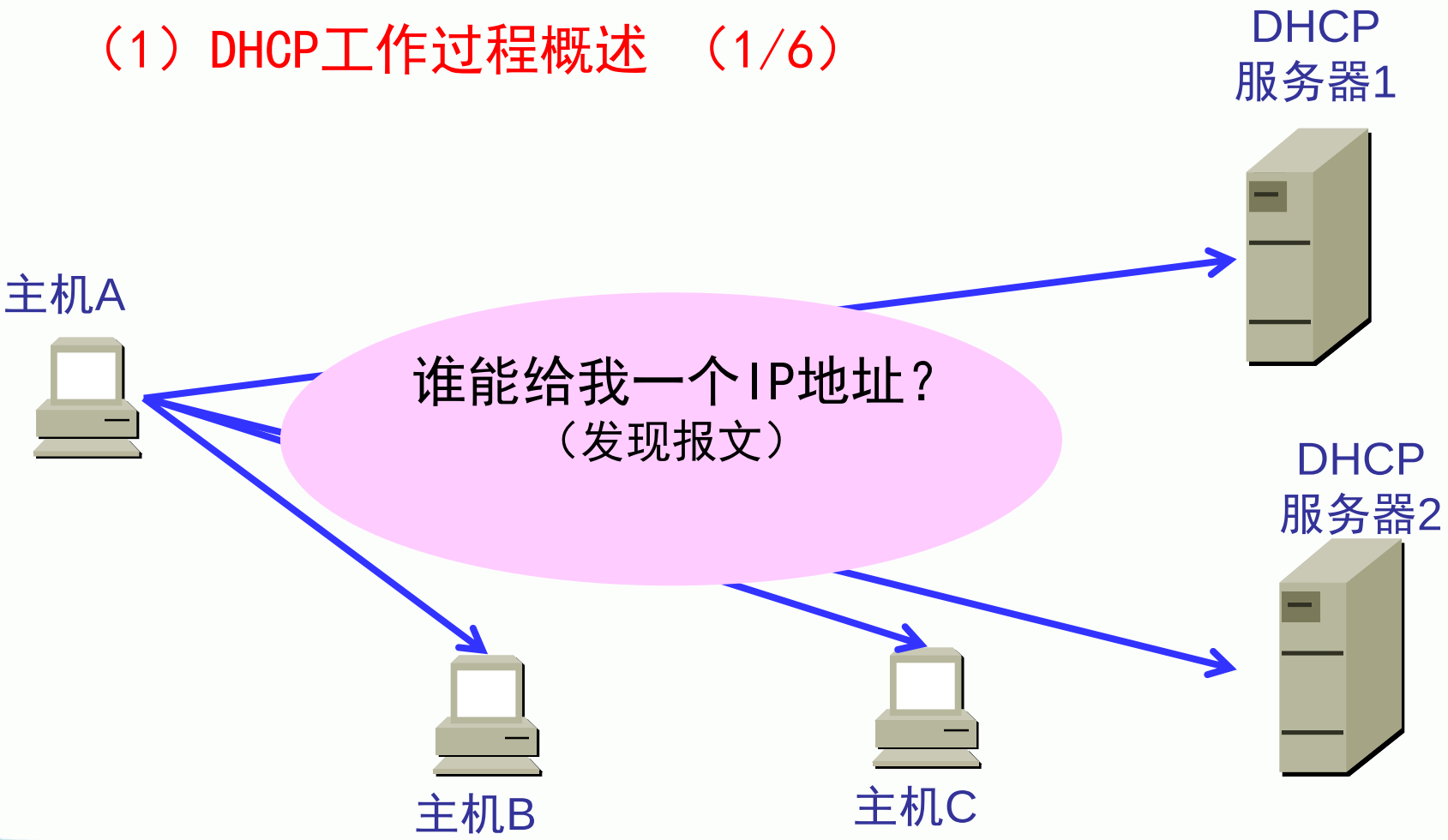
6.6.1 DHCP应用背景

（2）什么是DHCP？

- 动态主机配置协议 （Dynamic Host Configuration Protocol）
- DHCP 提供了一种即插即用连网的机制。
- 这种机制允许一台计算机加入新的网络和获取IP地址而不用手工参与。

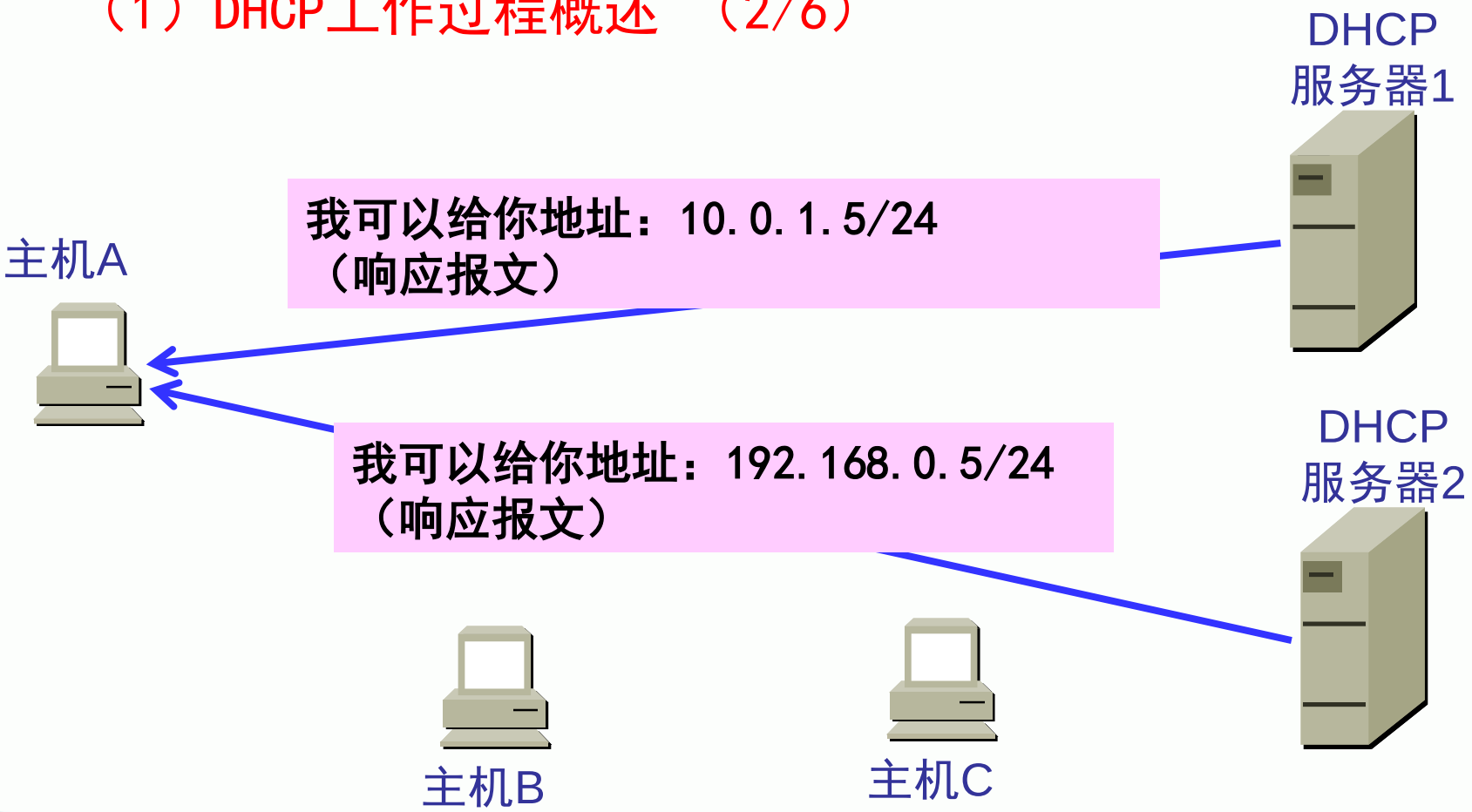
6.6.2 DHCP基本工作原理

（1）DHCP工作过程概述 （1/6）



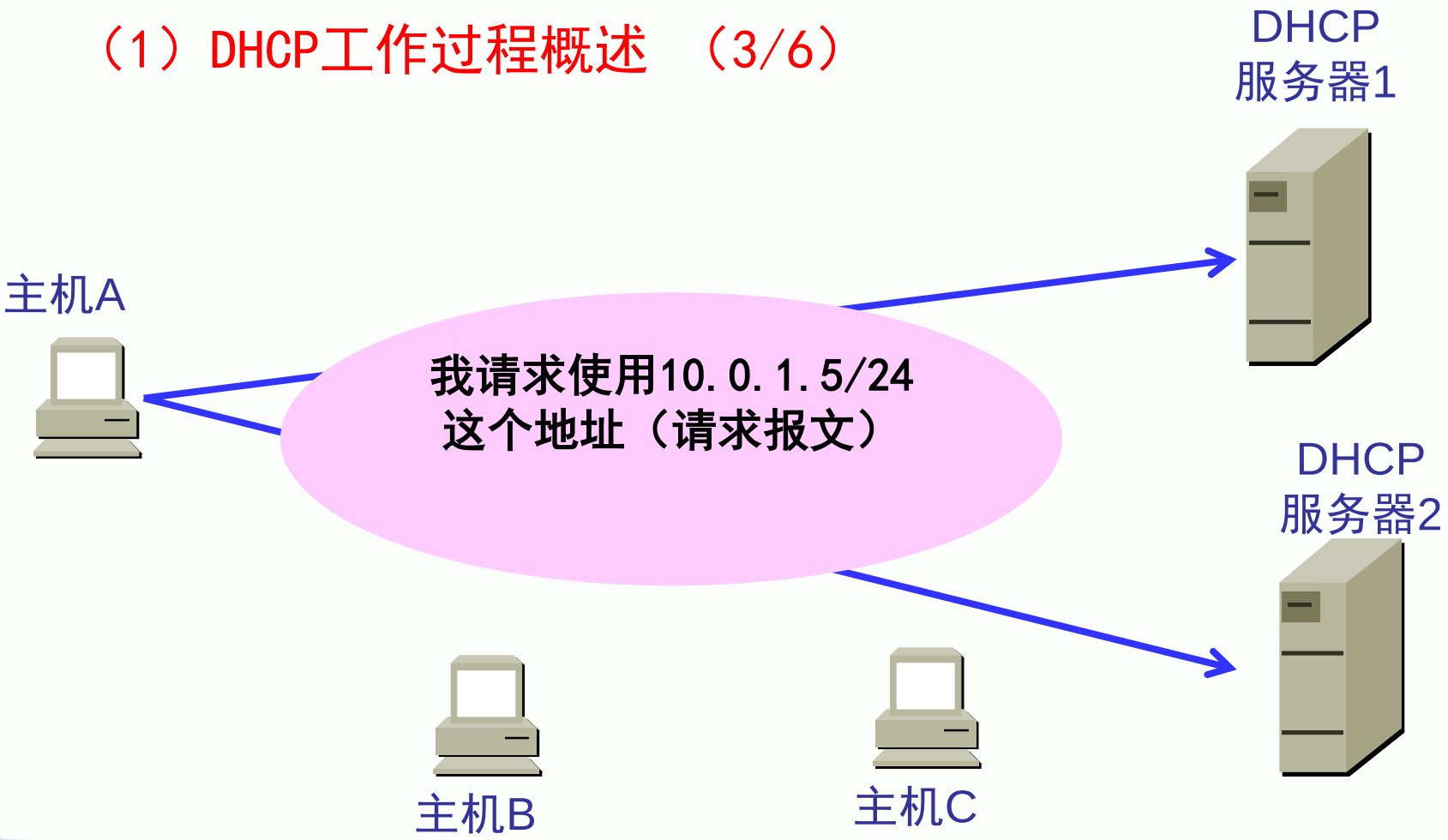
6.6.2 DHCP基本工作原理

（1）DHCP工作过程概述 （2/6）



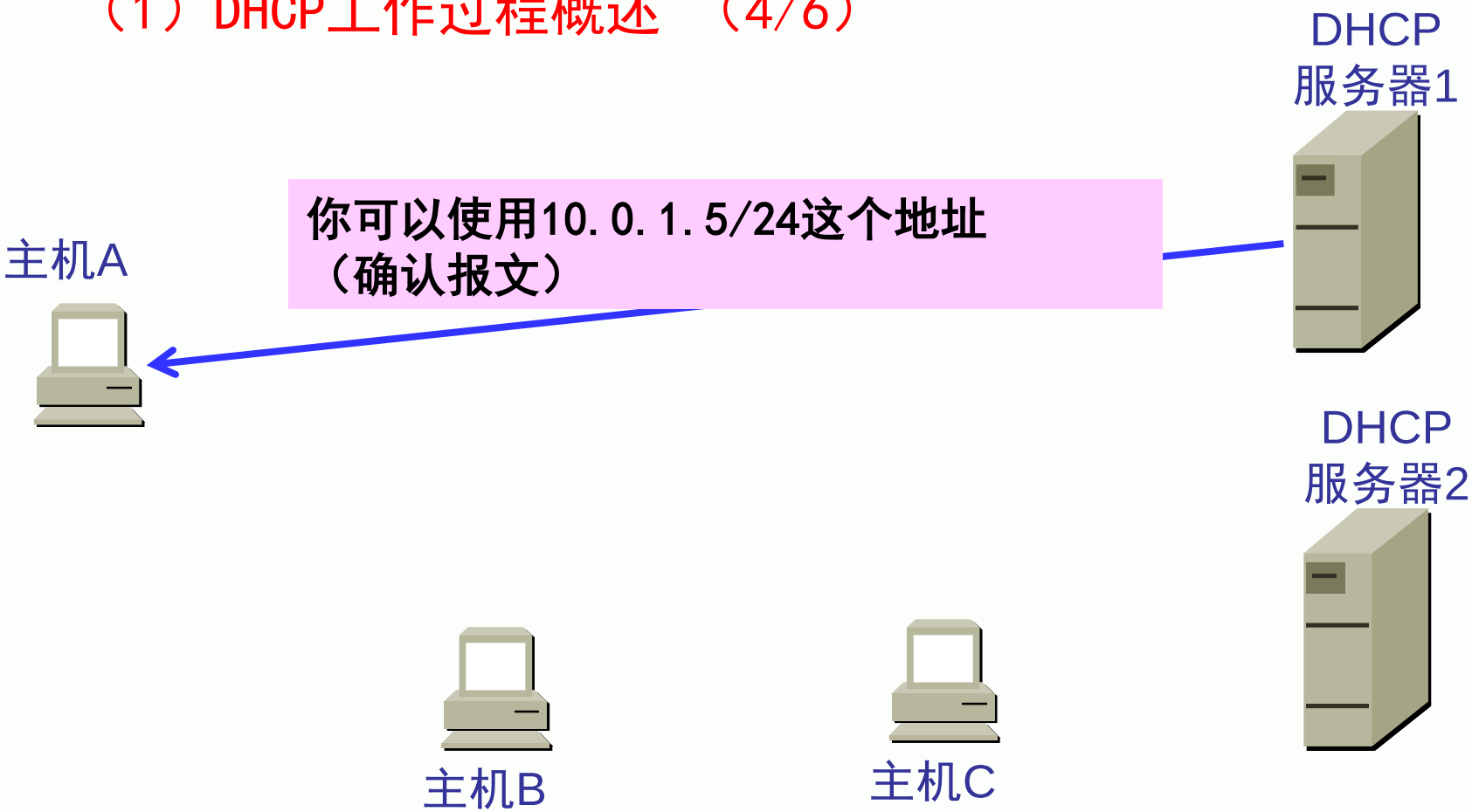
6.6.2 DHCP基本工作原理

（1）DHCP工作过程概述 （3/6）



6.6.2 DHCP基本工作原理

（1）DHCP工作过程概述 （4/6）



6.6.2 DHCP基本工作原理

（1）DHCP工作过程概述 （5/6）

① 需要 IP 地址的主机在启动时就向 DHCP 服务器广播发送发现报文（DHCPDISCOVER），这时该主机就成为 DHCP 客户。

② 本地网络上所有主机都能收到此广播报文，但只有 DHCP 服务器才回答此广播报文。

③ DHCP 服务器从服务器的 IP 地址池(address pool)中取一个地址分配给该计算机。DHCP 服务器的回答报文叫做提供报文（DHCPOFFER）。

6.6.2 DHCP基本工作原理

（1）DHCP工作过程概述 （6/6）

④ 客户机可能会收到多个DHCP提供报文，它选择第1个，然后向所选择的DHCP服务器发送DHCP请求报文，告诉该服务器，自己准备使用该服务器提供的地址信息。

⑤ 被选择的DHCP服务器发送确认报文DHCPACK，从这时起，DHCP客户机就可以使用这个IP地址了。

⑥ 被选择的DHCP服务器将该IP地址保留，不再让其他客户使用。

6.6.2 DHCP基本工作原理

（2）DHCP租用期（1/2）

- DHCP 服务器分配给 DHCP 客户的 IP 地址的临时的，因此 DHCP 客户只能在一段有限的时间内使用这个分配到的 IP 地址。DHCP 协议称这段时间为租用期。
- 租用期的数值应由 DHCP 服务器自己决定。
- DHCP 客户也可在自己发送的报文中（例如，发现报文）提出对租用期的要求。

6.6.2 DHCP基本工作原理

（2）DHCP租用期（2/2）

- 更新租约：
- DHCP服务器向DHCP客户机出租的IP地址一般都有一个租借期限，期满后DHCP服务器便会收回出租的IP地址。
- 如果DHCP客户机要延长其IP租约，则必须更新其IP租约。DHCP客户机启动时和IP租约期限过一半时，DHCP客户机都会自动向DHCP服务器发送更新其IP租约的信息。

6.6.3 几个问题

6.6.3 几个问题

（1）问题1：

客户机第1次启动时，是如何进行自我配置？

例如：客户机发出的发现报文中，

源MAC？ / 目的MAC？

源IP？ / 目的IP ？

源端口？/ 目的端口？

6.6.3 几个问题

- 问题1解答：（1/5）

由于客户机采用动态获得IP地址的方式，因此客户机在启动时会自动找DHCP服务器，即发出发现报文（DHCP Discover）报文；

下面分析一下客户机的数据包内容。

6.6.3 几个问题

- 问题1解答：（2/5）

运输层的首部：

发现报文（DHCP Discover）报文，在运输层进行封装，使用UDP协议，使用UDP68端口作为源端口，使用UDP67端口作为目的端口源端口。（注：DHCP客户使用的UDP端口是68，而DHCP服务器使用的UDP端口是67）

6.6.3 几个问题

- 问题1解答：（3/5）

网际层的首部：

发现报文在网际层进行封装，由于自身没有配置有效的IP地址，它会自动将自己的IP地址配置成0.0.0.0，并使用0.0.0.0的地址作为源地址，使用255.255.255.255作为目标地址来广播请求IP地址信息。

6.6.3 几个问题

- 问题1解答：（4/5）

网络接口层的首部：

发现报文在网络接口层进行封装，使用DHCP客户机的MAC地址作为源地址，使用ff:ff:ff:ff:ff:ff作为目的MAC地址，进行广播。

6.6.3 几个问题

- 问题1解答：（5/5）

归纳一下，在discover报文中，使用：

- UDP68端口作为源端口，使用UDP67端口作为目的端口；
- 0.0.0.0作为源地址，255.255.255.255作为目标地址；
- DHCP客户机的MAC地址为源MAC（以便使DHCP服务器能确定是哪个客户机发送的请求），全f为目的MAC；

抓包分析

从上图可看出：

- 以太网帧中的源MAC和目的MAC；
- IP协议中的源IP和目的IP；
- UDP报文中的源端口和目的端口；
- 客户端的IP和MAC
- 报文类型（DHCP Discover）；
- 客户端想申请的IP：192.168.1.34，因为DHCP客户机总是试图重新租用它接收过的最后一个IP地址，估计图一中的客户机的上一个IP是192.168.1.34。

6.6.3 几个问题

（2）问题2：

服务器的响应报文中，又该如何配置相应的地址参数？

6.6.3 几个问题

问题2解答：（1/3）

- **服务器响应也称为DHCPOFFER。**
- 当DHCP服务器接收到客户机请求IP地址的信息时，它就在自己的IP地址池中查找是否有合法的IP地址提供给客户机。如果有，DHCP服务器就将此IP地址做上标记，加入到DHCPOFFER的消息中，然后DHCP服务器就广播一则包括下列信息的DHCPOFFER消息：
- DHCP客户机的MAC地址；DHCP服务器提供的合法IP地址；子网掩码；默认网关（路由）；租约的期限；DHCP服务器的IP地址。

6.6.3 几个问题

- 问题2解答：（2/3）

归纳一下，**DHCP服务器的offer报文中：**

- 使用**UDP67端口作为源端口，使用UDP68端口作为目的端口；**
- 因为DHCP客户机还没有IP地址，所以服务器**使用自己的IP地址作为源地址，使用255.255.255.255作为目标地址；**
- **服务器MAC地址为源MAC，全f为目的MAC；**
- 广播**DHCPOFFER信息。**

以上信息用于通信

6.6.3 几个问题

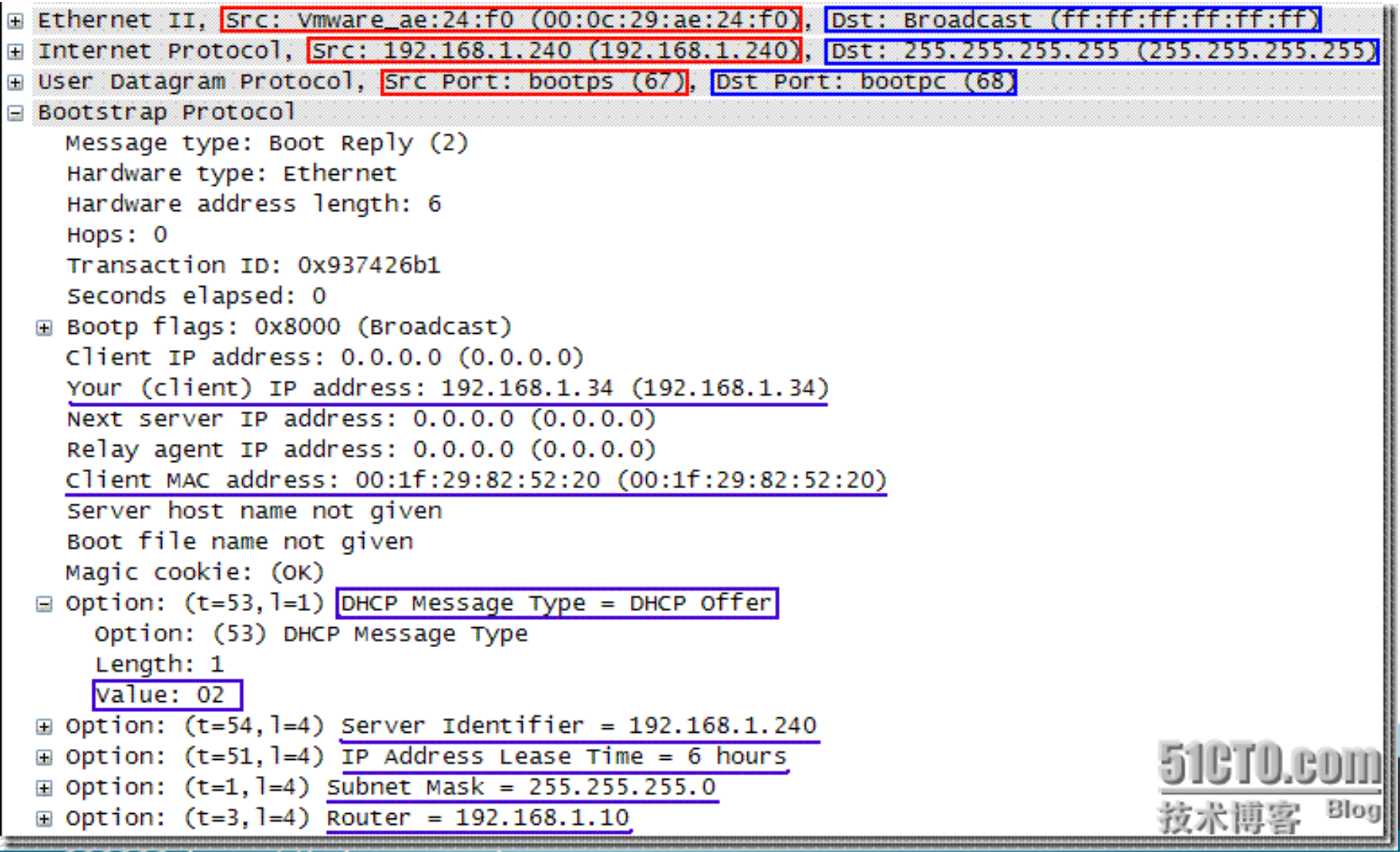
- 问题2解答：（3/3）

DHCP服务器的offer报文中，除了前面所提到的通信信息外，还包括：

- DHCP客户机的MAC地址；
- DHCP服务器提供的合法IP地址；子网掩码；默认网关；
- 租约的期限；

- 上述信息是提供给客户机的配置信息

抓包分析：DHCP offer报文



6.6.3 几个问题

（3）问题3：

DHCP服务器如何知道客户机选择了自己所提供的地址参数？

6.6.3 几个问题

- 问题3解答：（1/3）

- 当客户机从第一个DHCP服务器接收DHCPOFFER并选择IP地址后，客户机将DHCPREQUEST消息广播到所有的DHCP服务器，表明它接受提供的内容。
- DHCPREQUEST消息包括为该客户机提供IP配置的服务器的服务标识符（IP地址）。
- DHCP服务器收到请求报文后，查看服务器标识符字段，以确定它自己是否被选中为指定的客户机提供IP地址，如果那些DHCPOFFER被拒绝，则DHCP服务器会取消提供并保留其IP地址以用于下一个IP租约请求。

6.6.3 几个问题

- 问题3解答：（2/3）

- 在客户机选择IP的过程中，虽然客户机选择了IP地址，但是还没有配置IP地址，而在一个网络中可能有几个DHCP服务器，所以**客户机仍然使用0.0.0.0的地址作为源地址，使用UDP68端口作为源端口，使用255.255.255.255作为目标地址，使用UDP67端口作为目的端口来广播DHCPREQUEST信息**

6.6.3 几个问题

- 问题3解答：（3/3）

- 在DHCP Requset报文中，包含了客户机想申请的IP地址，以及客户机选择的DHCP服务器的IP地址。
- 当DHCP服务器收到Request报文时，就知道客户机是否选择了自己所提供的IP地址。

抓包分析：DHCP Request报文

```
⊞ Ethernet II, Src: 00:1f:29:82:52:20 (00:1f:29:82:52:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x937426b1
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1f:29:82:52:20 (00:1f:29:82:52:20)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊟ Option: (t=53,l=1) DHCP Message Type = DHCP Request
      Option: (53) DHCP Message Type
      Length: 1
      Value: 03
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=50,l=4) Requested IP Address = 192.168.1.34
  ⊞ Option: (t=54,l=4) Server Identifier = 192.168.1.240
  ⊞ Option: (t=12,l=10) Host Name = "BOBYUAN-PC"
  ⊞ Option: (t=81,l=13) Client Fully Qualified Domain Name
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=12) Parameter Request List
```

6.6.3 几个问题

（4）问题4：

客户机到底什么时候开始使用DHCP服务器提供的IP地址？

6.6.3 几个问题

- 问题4解答：（1/2）

➢ DHCP服务器接收到DHCP Request消息后，发出确认租约的报文（DHCPACK消息），该报文以广播形式发到网络中，该报文中指明了某客户机的MAC以及服务器所分配给他的IP；

6.6.3 几个问题

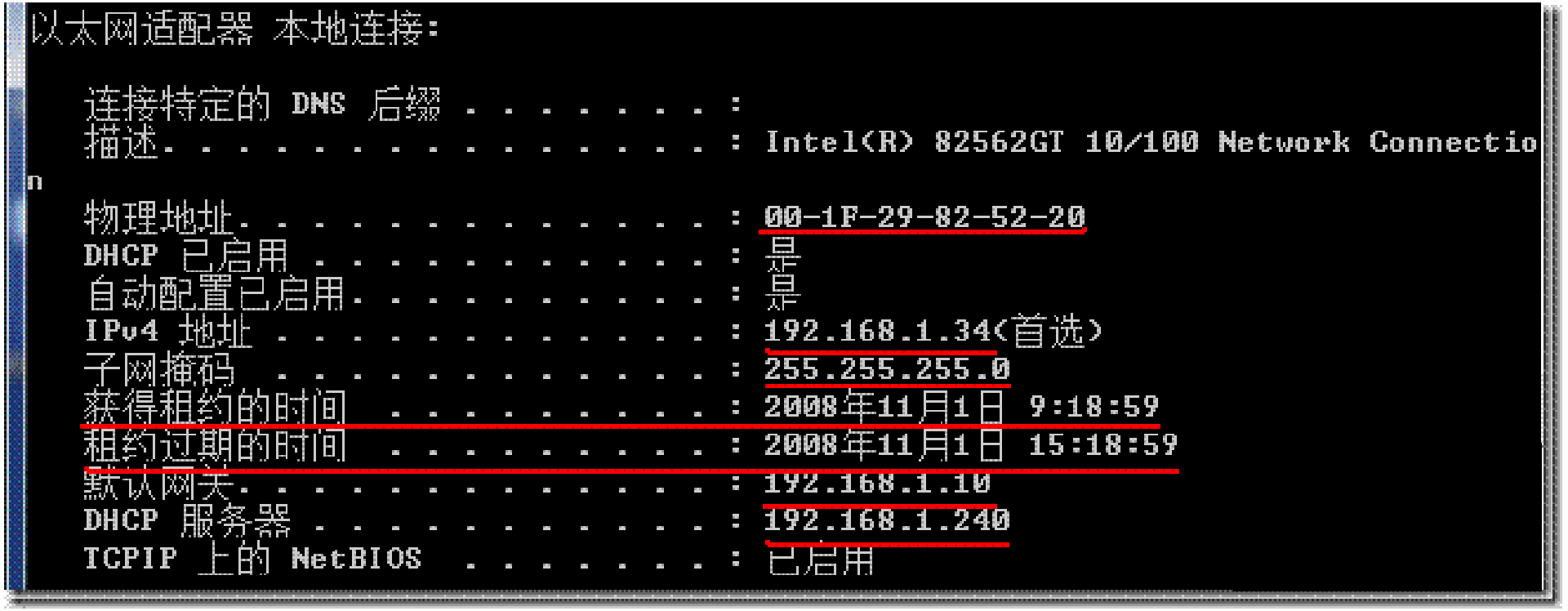
- 问题4解答：（2/2）

- 虽然服务器确认了客户机的租约请求，但是客户机此时还没有收到服务器的DHCPACK消息，所以客户机还没有配置自己的IP地址，所以**服务器仍然使用自己的IP地址作为源地址，使用UDP67端口作为源端口，使用255.255.255.255作为目标地址，使用UDP68端口作为目的端口来广播DHCPACK信息。**
- 客户机收到报文后，查看里面的MAC是否是自己的，是自己的，就配置自己的IP，完成TCP/IP初始化，否则就丢弃该报文。

抓包分析：DHCP ACK 报文

```
⊞ Ethernet II, Src: Vmware_ae:24:f0 (00:0c:29:ae:24:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 192.168.1.240 (192.168.1.240), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x937426b1
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.34 (192.168.1.34)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1f:29:82:52:20 (00:1f:29:82:52:20)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊟ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
      Option: (53) DHCP Message Type
      Length: 1
      Value: 05
  ⊞ Option: (t=54,l=4) Server Identifier = 192.168.1.240
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 6 hours
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=3,l=4) Router = 192.168.1.10
```

可以看到客户端获取的IP地址是192.168.1.34；默认网关是192.168.1.10；DHCP服务器IP是192.168.1.240；租约时间是6个小时



6.6.3 几个问题

（5）问题5：

DHCP客户机获得IP后，以后DHCP客户机每次重新登录网络时，如何与DHCP服务器联系？

6.6.3 几个问题

- 问题5解答：（1/2）

  - DHCP客户机总是试图重新租用它接收过的最后一个IP地址，这给网络带来一定的稳定性。
  - 以后DHCP客户机每次重新登录网络时，就不需要再发送DHCP discover发现信息了，而是直接发送包含前一次所分配的IP地址的DHCP request请求信息。
  - 当DHCP服务器收到这一信息后，它会尝试让DHCP客户机继续使用原来的IP地址，并回答一个DHCP ack确认信息。

6.6.3 几个问题

- 问题5解答：（2/2）

  - 如果此IP地址已无法再分配给原来的DHCP客户机使用时（比如此IP地址已分配给其它DHCP客户机使用，或者因为客户机移到其他子网 ），则DHCP服务器给DHCP客户机回答一个DHCP nack否认信息。
  - 当原来的DHCP客户机收到此DHCP nack否认信息后，它就必须重新发送DHCP discover发现信息来请求新的IP地址。

6.6.3 几个问题

（6）问题6：

DHCP客户机启动后，找不到DHCP服务器，会出现什么情况？

6.6.3 几个问题

- 问题6解答：

如果DHCP客户机无法找到DHCP服务器，它将从TCP/IP的B类网段169.254.0.0中挑选一个IP地址作为自己的IP地址，继续每隔5分钟尝试与DHCP服务器进行通讯，一旦与DHCP服务器取得联系，则客户机放弃自动配置的IP地址，而使用DHCP服务器分配的IP地址。

6.6.3 几个问题

（7）问题7：

DHCP客户机获得的IP地址是有租期的……

6.6.3 几个问题

- 问题7解答 ：（1/4）

自动续订

- DHCP服务器向DHCP客户机出租的IP地址一般都有一个租借期限，期满后DHCP服务器便会收回出租的IP地址。如果DHCP客户机要延长其IP租约，则必须更新其IP租约。
- DHCP客户机启动时和IP租约期限过一半时，DHCP客户机都会自动向DHCP服务器发送更新其IP租约的信息。

6.6.3 几个问题

- 问题7解答 ： （2/4）

  - DHCP 客户端除了在开机的时候发出 DHCP request 请求之外，在租约期限一半的时候也会发出 DHCP request ，如果此时得不到 DHCP 服务器的确认的话，客户端还可以继续使用该 IP ；
  - 当租约期过了87.5%时，如果客户端仍然无法与当初的DHCP服务器联系上，它将与其它DHCP服务器通信。如果网络上再没有任何DHCP服务器在运行时，该客户端必须停止使用该IP地址，并重新发送一个Dhcpdiscover数据包开始，再一次重复整个过程。

6.6.3 几个问题

- 问题7解答 ：（3/4）

  - 如果租约到期了（指在前面所提及的自动续约失败的情况下），那么客户端必须立即释放当前使用的IP地址。然后，DHCP客户端重新开始DHCP租约过程，尝试租用一个新的IP地址。
  - DHCP客户机在开机状态下，关闭DHCP服务器，租约期一到，客户机的IP变成0.0.0.0。

6.6.3 几个问题

- 问题7解答 ：（4/4）

手动续订

- 如果需要立即更新DHCP配置消息，用户可以手动续订IP租约。例如，如果用户希望DHCP客户端立即从DHCP服务器获取新安装的路由器的地址，那么需要用户从客户端续订租约来更改这些配置。
- 要手动续订租约，使用ipconfig命令，并带/renew开关参数。这条命令向DHCP服务器发送一条DHCPREQUEST消息请求更新配置选项和续订租约时间。

6.6.4　DHCP 中继代理

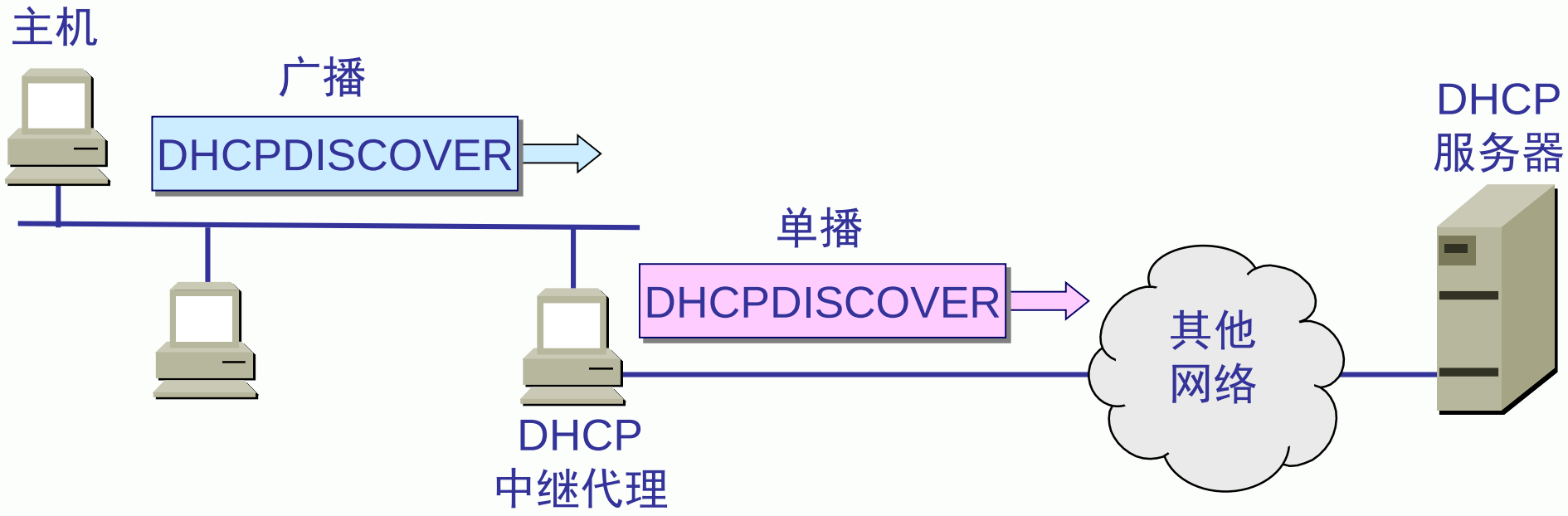
6.6.4 DHCP 中继代理

- **DHCP Relay**（DHCPR）DHCP中继 也叫做DHCP中继代理
- 如果DHCP客户机与DHCP服务器在同一个物理网段，则客户机可以正确地获得动态分配的ip地址。如果不在同一个物理网段，则需要DCHP Relay Agent(中继代理)。

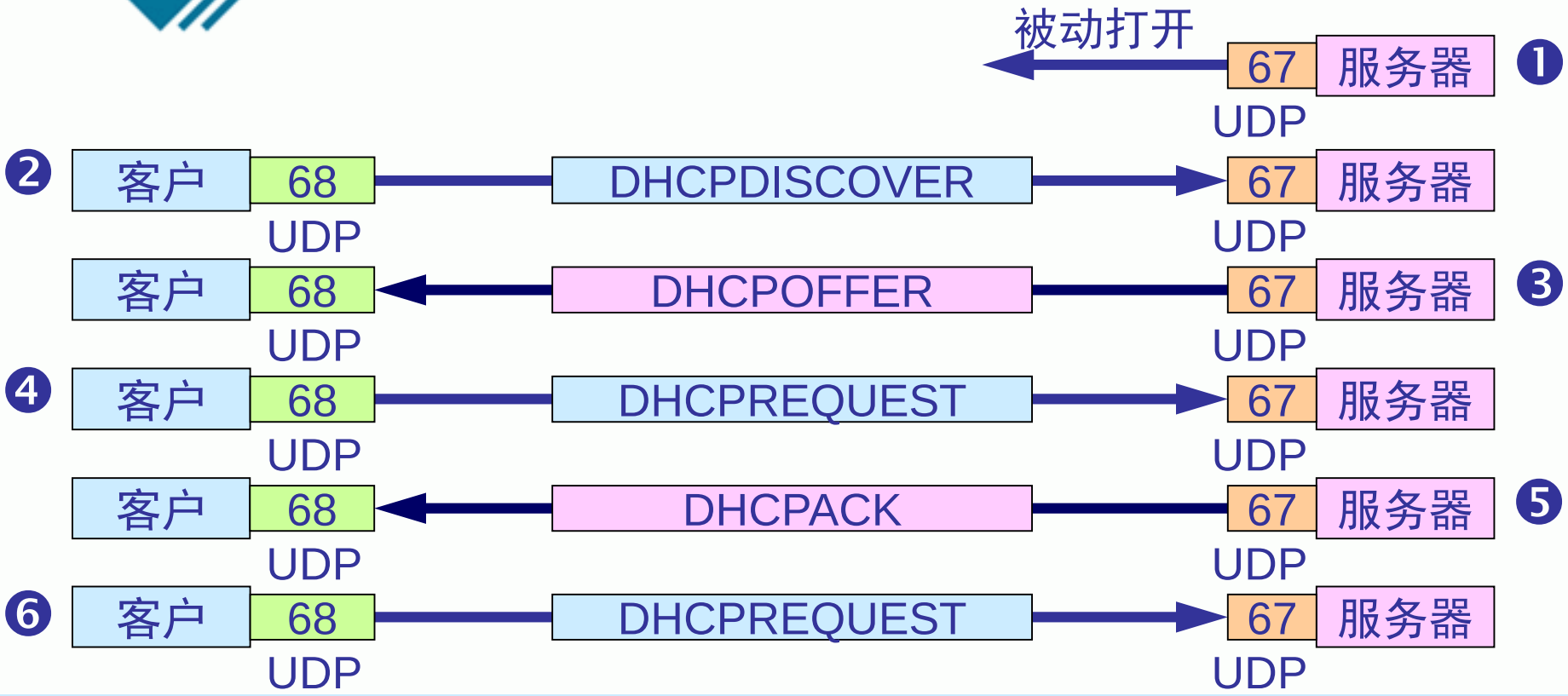
6.6.4 DHCP 中继代理

- 用DHCP Relay代理可以去掉在每个物理的网段都要有DHCP服务器的必要,它可以传递消息到不在同一个物理子网的DHCP服务器，也可以将服务器的消息传回给不在同一个物理子网的DHCP客户机。
- 当 DHCP 中继代理收到主机发送的发现报文后，就以单播方式向 DHCP 服务器转发此报文，并等待其回答。收到 DHCP 服务器回答的提供报文后，DHCP 中继代理再将此提供报文发回给主机。

DHCP 中继代理
以单播方式转发发现报文

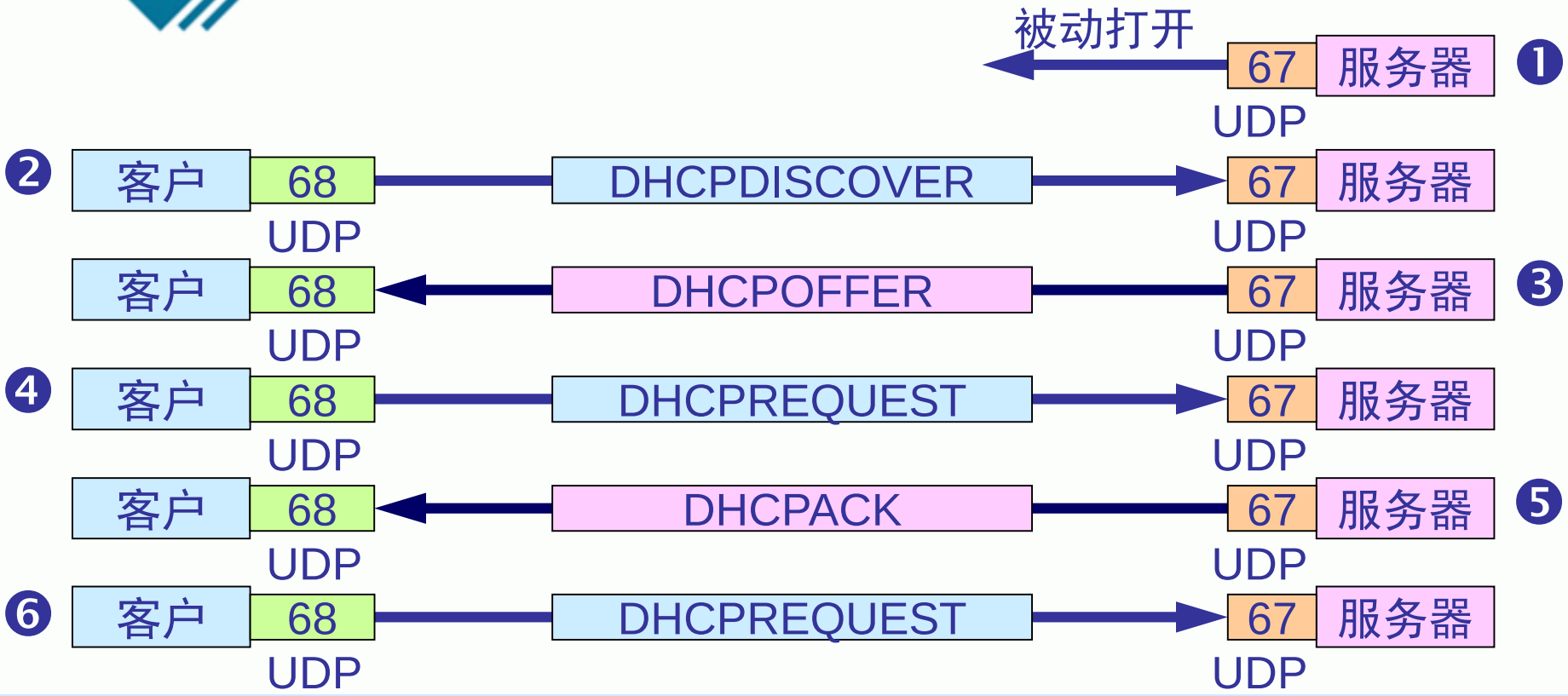


DHCP 协议的工作过程



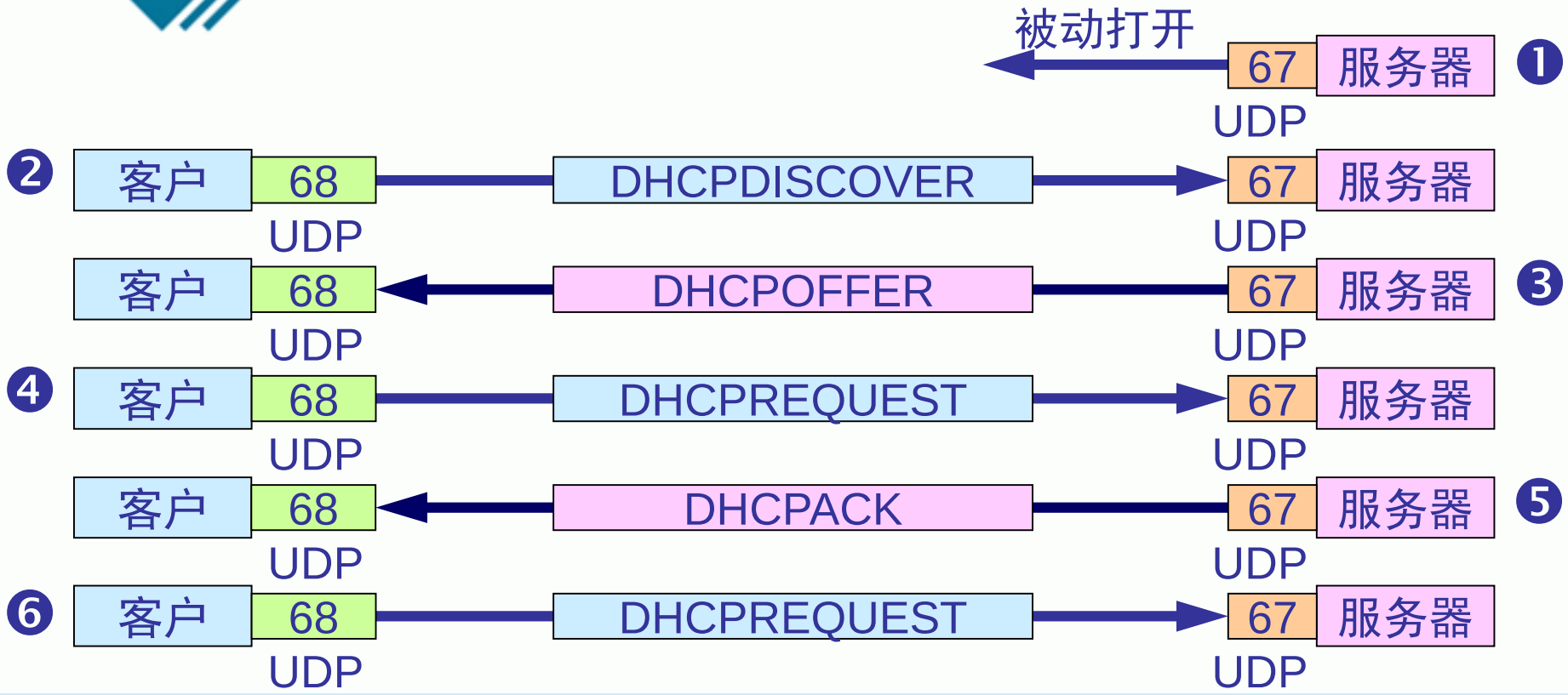
❶：DHCP 服务器被动打开 UDP 端口 67，等待客户端发来的报文。

DHCP 协议的工作过程



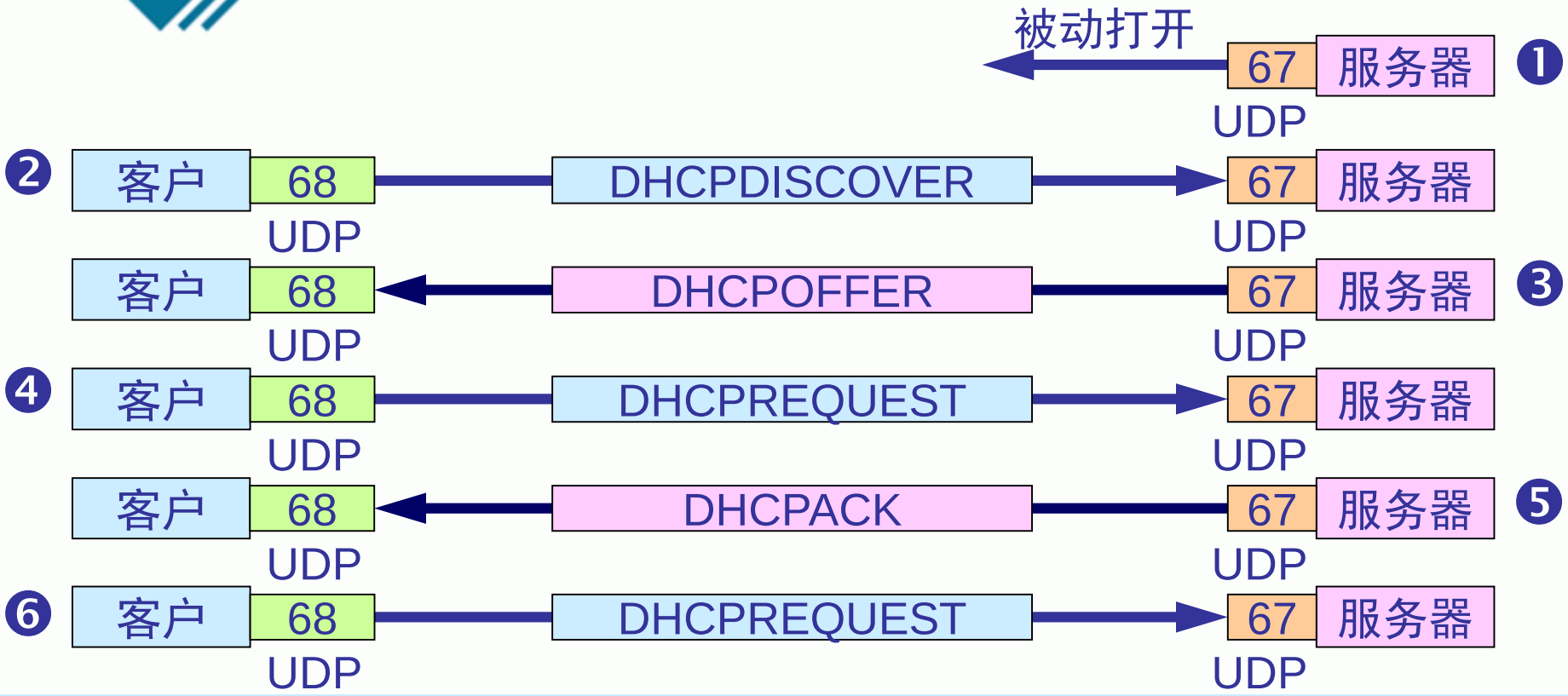
❷：DHCP 客户从 UDP 端口 68 发送 DHCP 发现报文。

DHCP 协议的工作过程



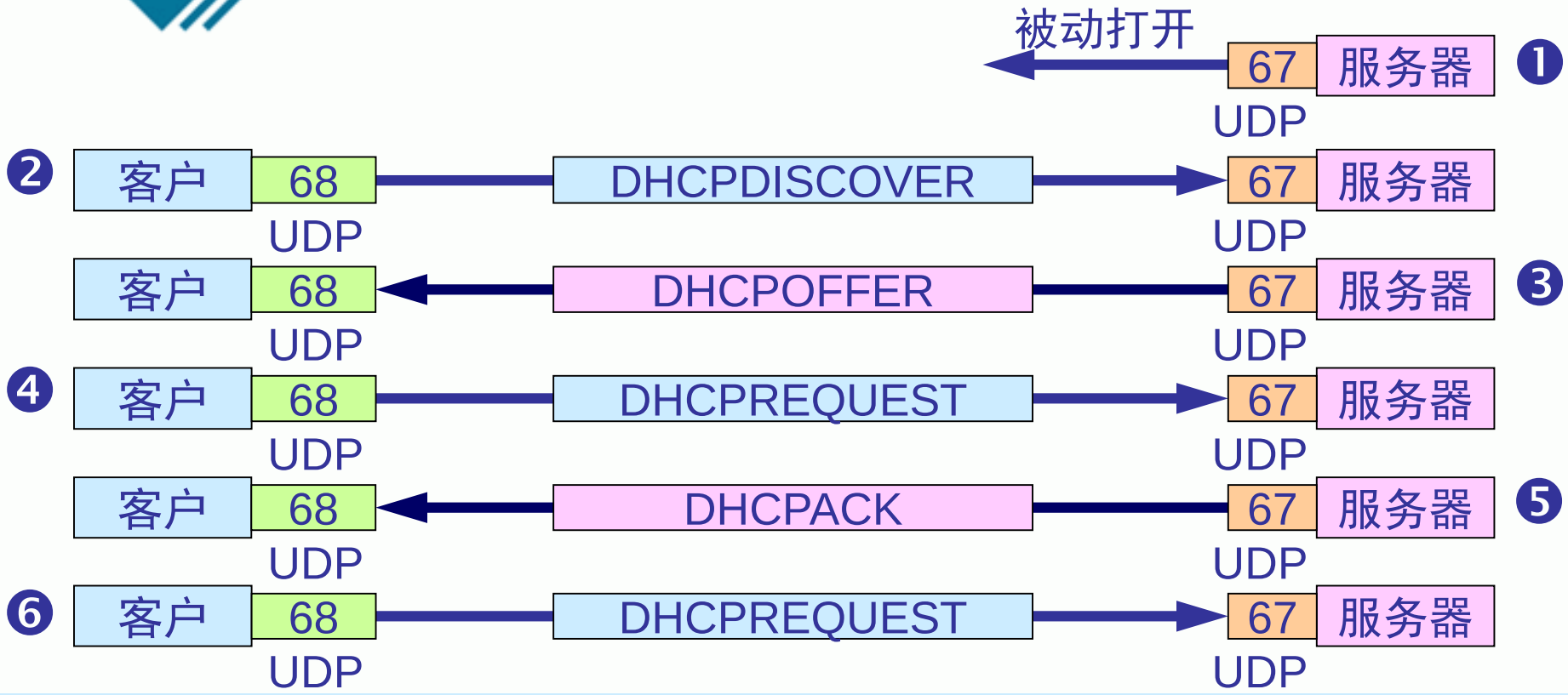
❸：凡收到 DHCP 发现报文的 DHCP 服务器都发出 DHCP 提供报文，因此 DHCP 客户可能收到多个 DHCP 提供报文。

DHCP 协议的工作过程



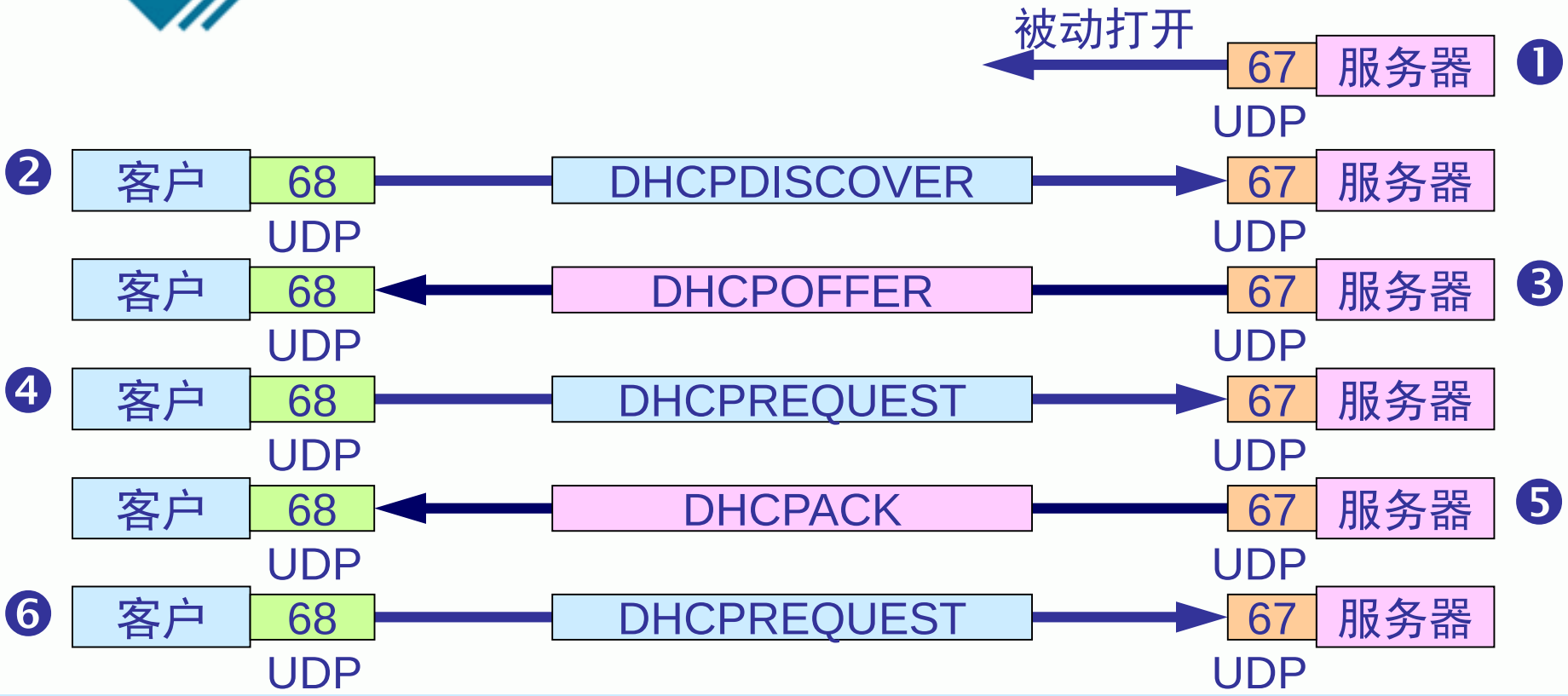
❹：DHCP 客户从几个 DHCP 服务器中选择其中的一个，并向所选择的 DHCP 服务器发送 DHCP 请求报文。

DHCP 协议的工作过程



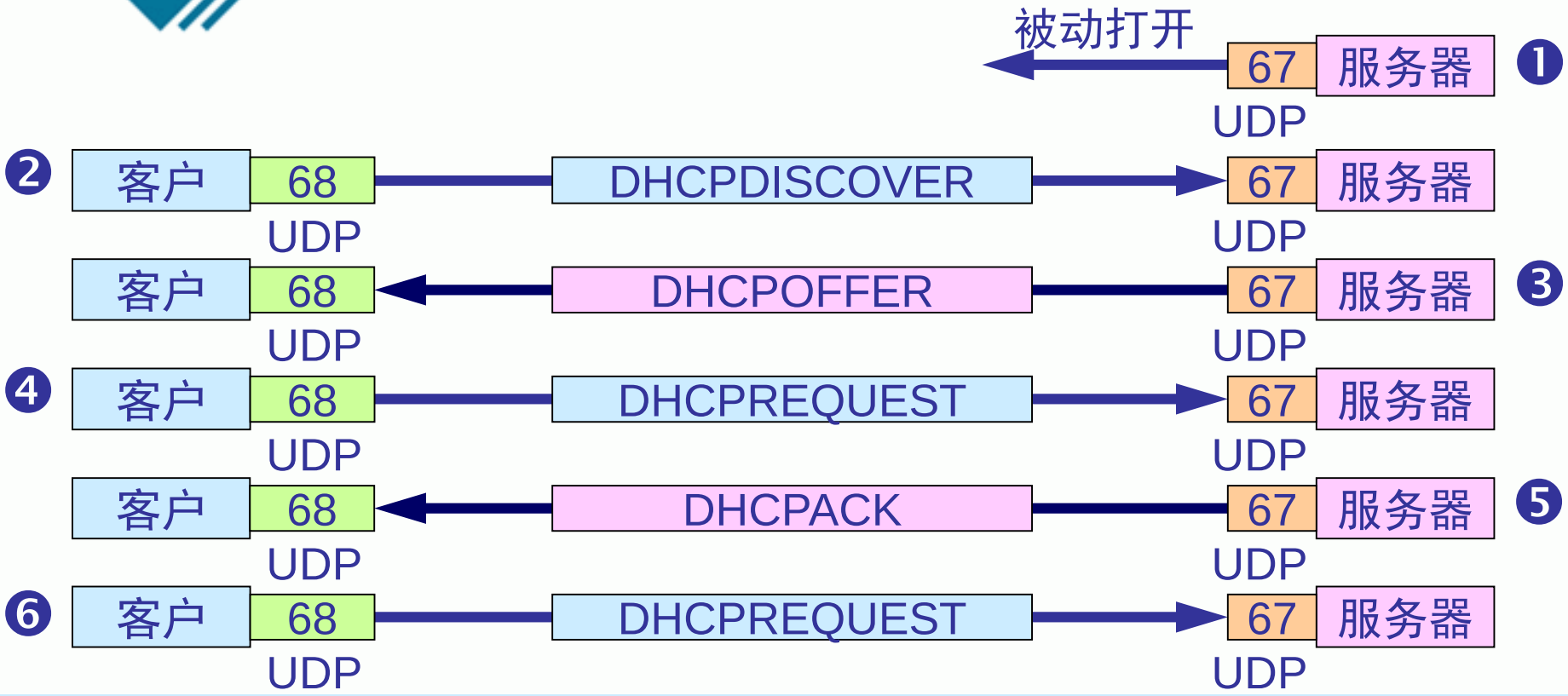
❺：被选择的 DHCP 服务器发送确认报文 DHCPACK，进入已绑定状态，并可开始使用得到的临时 IP 地址了。

DHCP 协议的工作过程



DHCP 客户现在要根据服务器提供的租用期 T 设置两个计时器 T_1 和 T_2，它们的超时时间分别是 0.5T 和 0.875T。当超时时间到就要请求更新租用期。

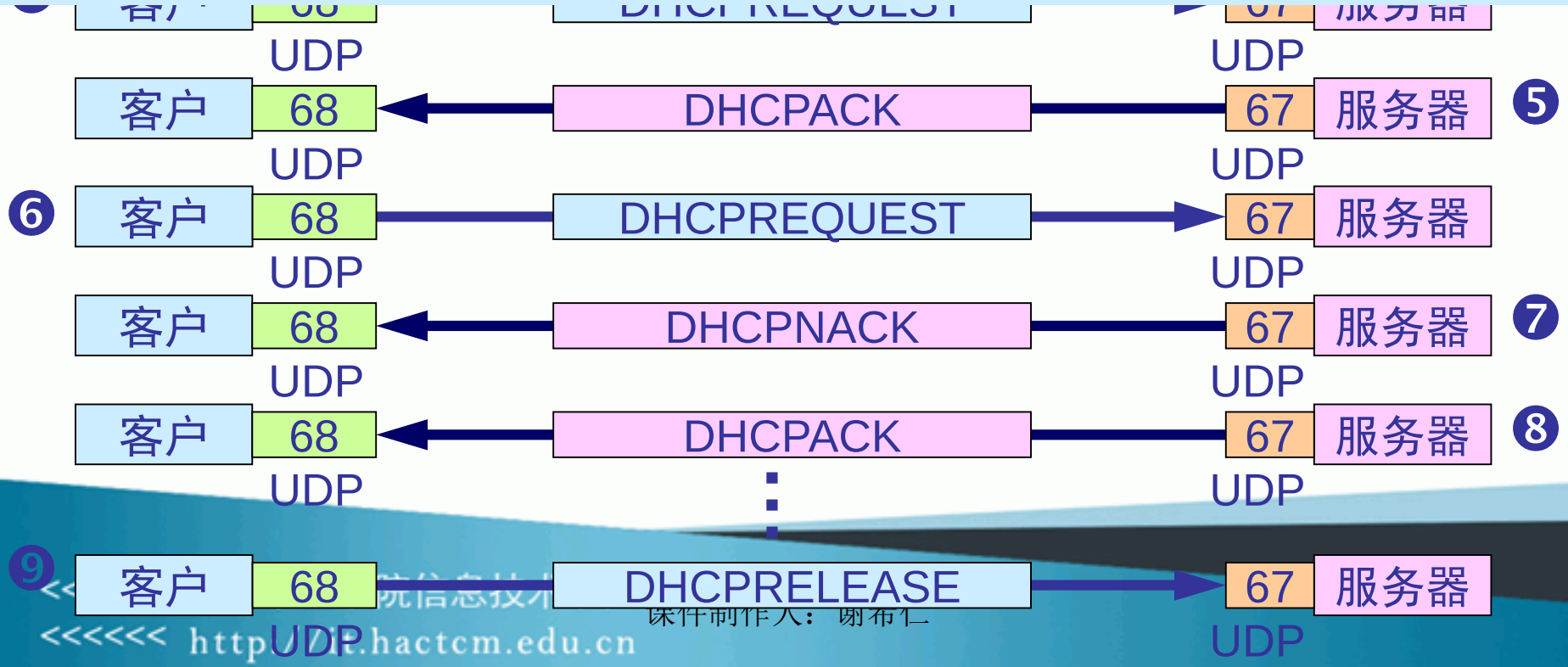
DHCP 协议的工作过程



❻：租用期过了一半（T1 时间到），DHCP 发送请求报文 DHCPREQUEST 要求更新租用期。

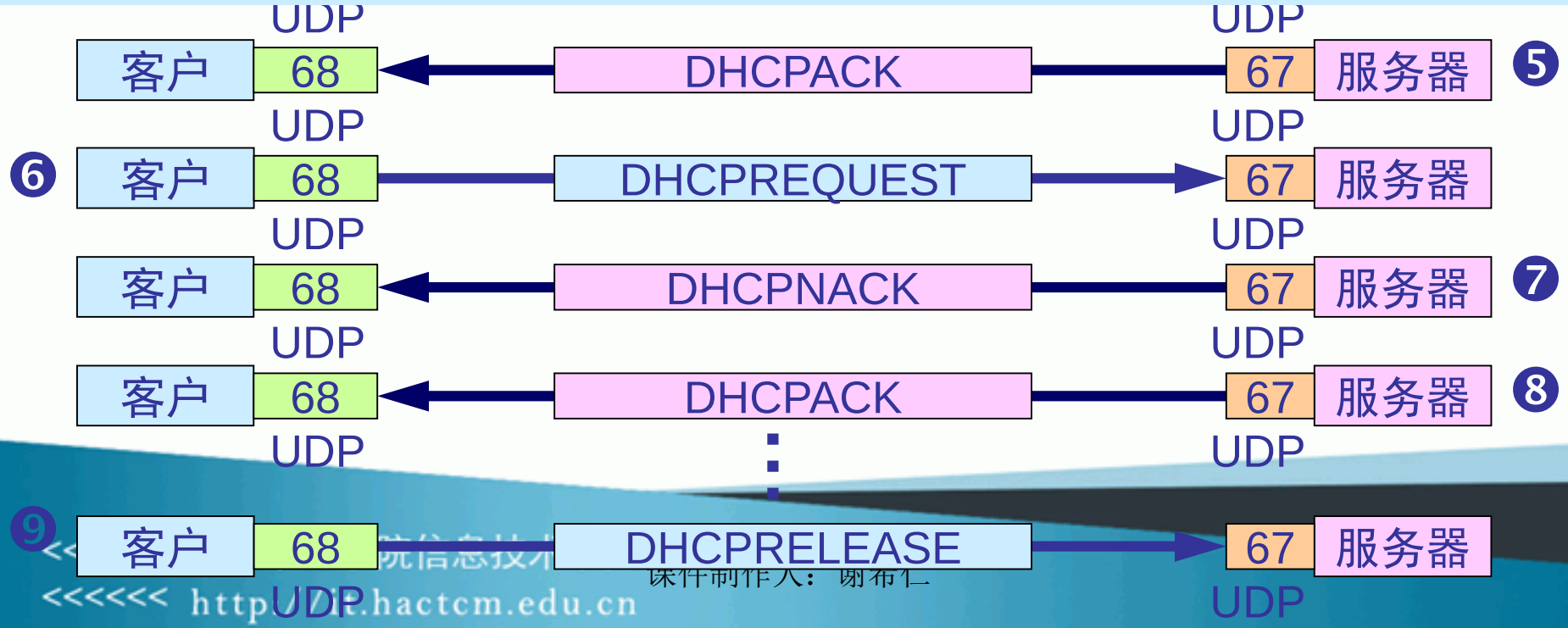
DHCP 协议的工作过程

❼：DHCP 服务器若同意，则发回确认报文 DHCPACK。DHCP 客户得到了新的租用期，重新设置计时器。



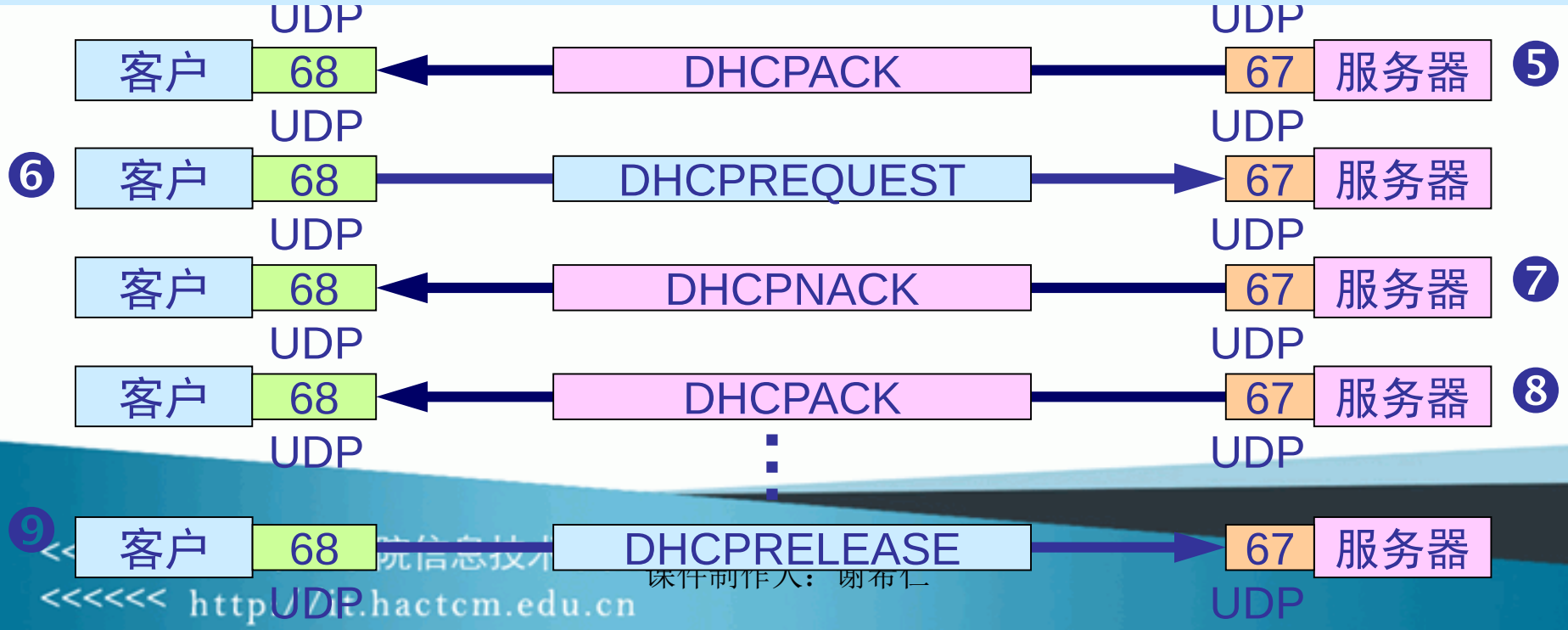
DHCP 协议的工作过程

❽：DHCP 服务器若不同意，则发回否认报文 DHCPNACK。这时 DHCP 客户必须立即停止使用原来的 IP 地址，而必须重新申请 IP 地址（回到步骤❷）。



DHCP 协议的工作过程

若 DHCP 服务器不响应步骤❻的请求报文 DHCPREQUEST，则在租用期过了 87.5% 时，DHCP 客户必须重新发送请求报文 DHCPREQUEST（重复步骤❻），然后又继续后面的步骤。



DHCP 协议的工作过程

❾：DHCP 客户可随时提前终止服务器所提供的租用期，这时只需向 DHCP 服务器发送释放报文 DHCPRELEASE 即可。