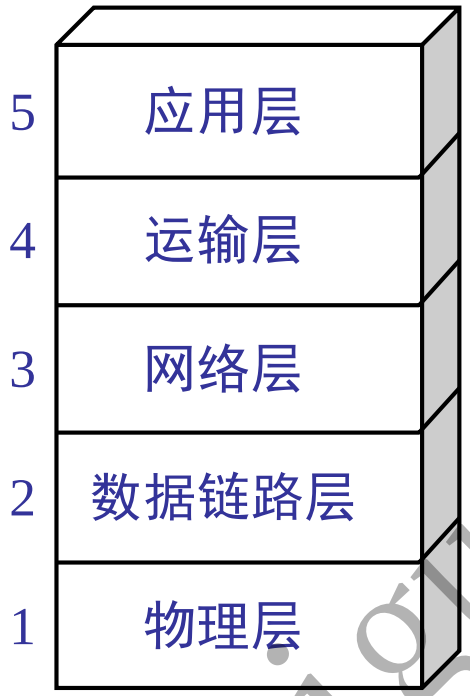
计算机网络

顾 军

计算机学院

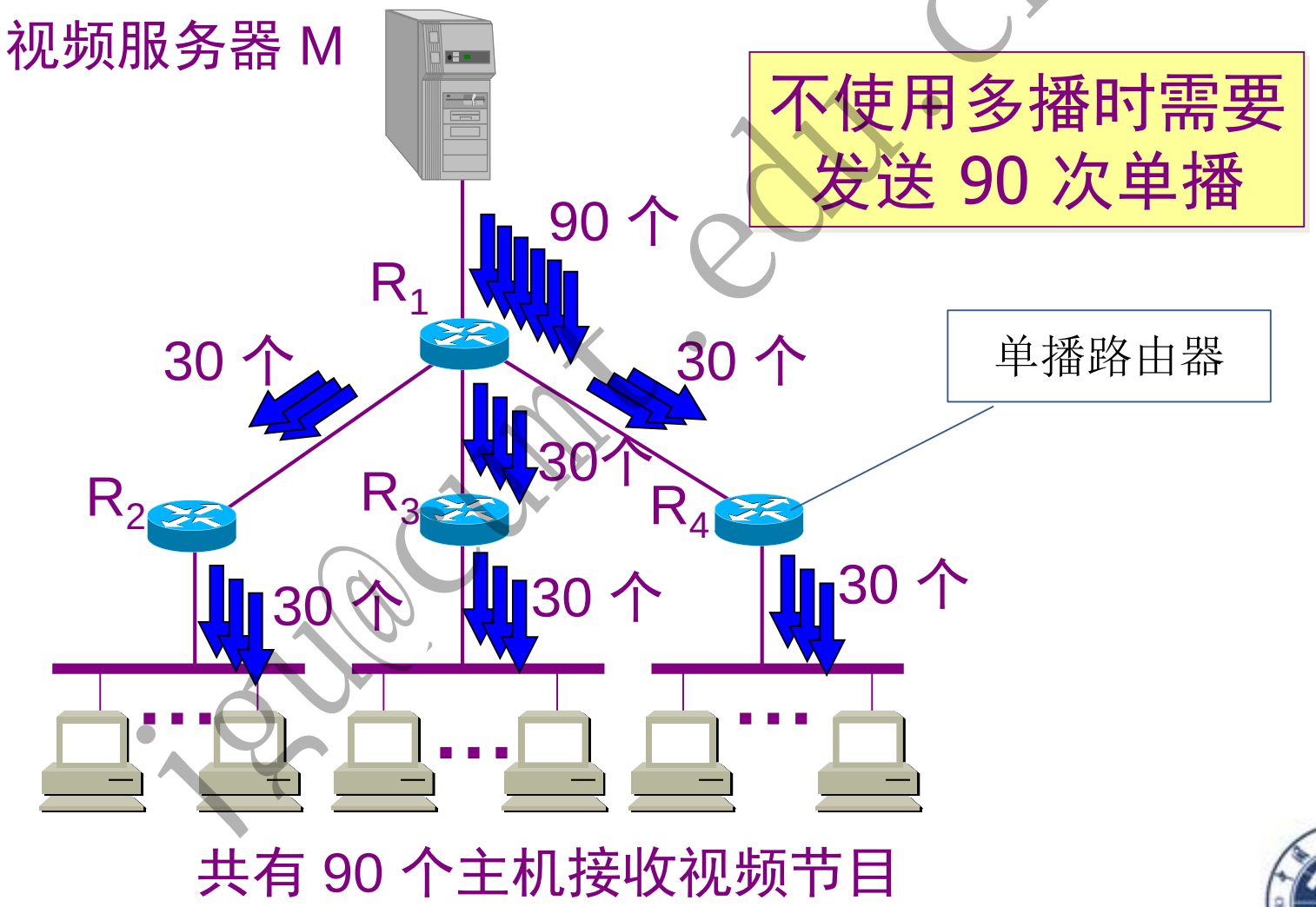
jgu@cumt.edu.cn

专题4：数据包怎么在互联网中寻路和转发？

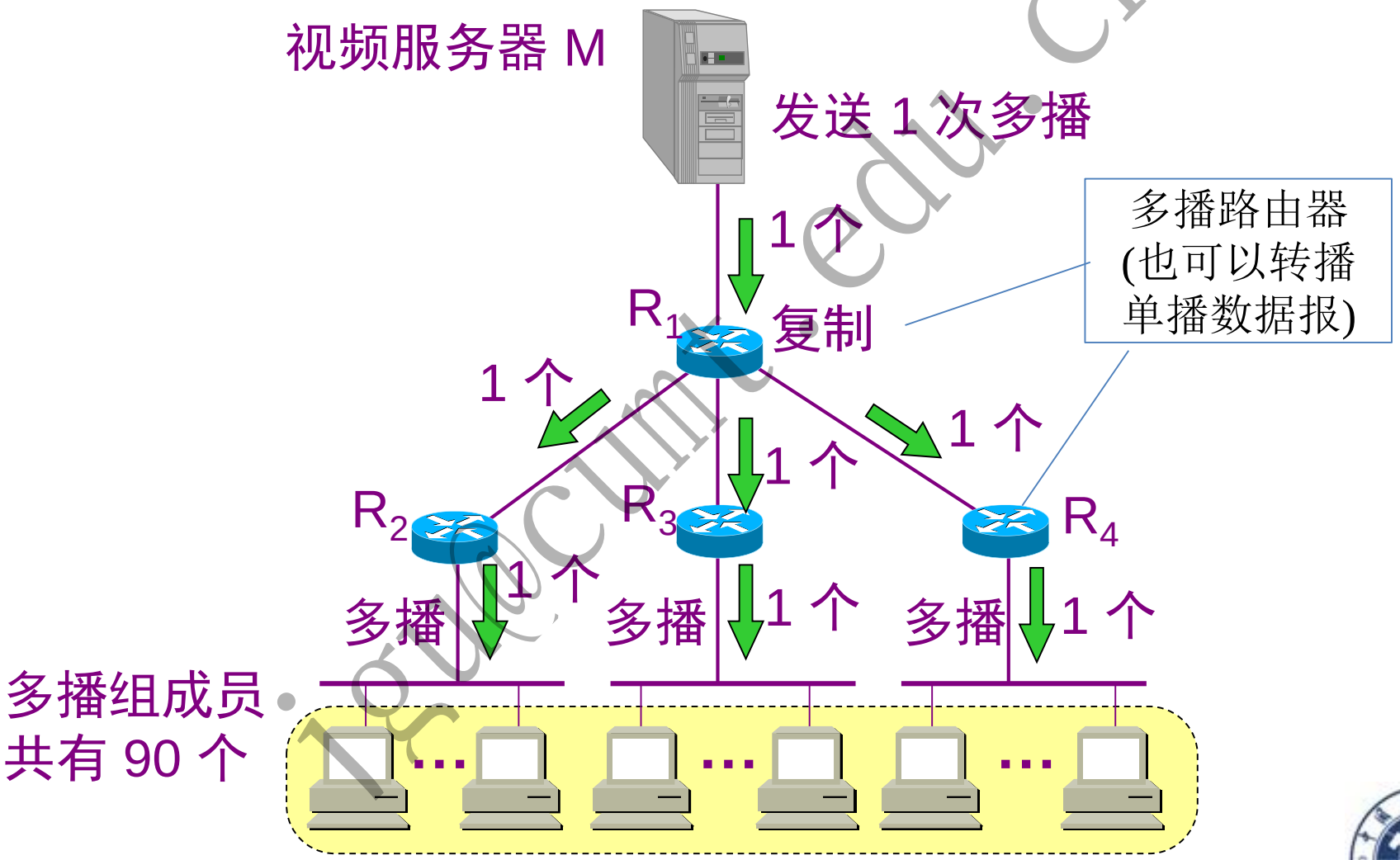


- 应用层(application layer)
- 运输层(transport layer)
- 网络层(network layer)
- 数据链路层(data link layer)
- 物理层(physical layer)

Q31：什么是多播？



多播可明显地减少网络中资源的消耗



IP多播的概念

- 在互联网上进行多播就叫做IP多播。
- IP多播（也称多址广播或组播）是一种允许一台或多台主机（多播源）发送单一数据包到多台主机（一次的，同时的）的TCP/IP网络技术。多播作为一点对多点的通信，是节省网络带宽的有效方法之一。
- IP多播被广泛应用在网络音频/视频广播、网络视频会议、多媒体远程教育、AOD/VOD、媒体推送“push”技术（如比赛得分、天气预报、新闻标题等）、状态监视（如股票行情、传感设备、安全系统、生产信息等）和虚拟现实游戏等方面。

Q32：IP多播的地址标识？

多播使用组地址—— IP 使用 D 类地址支持多播。

- 224.0.0.0 到 239.255.255.255
- 每一个D类地址标志一个多播组，可以标志2^{28}个多播组
- 多播地址只能用于目的地址，不能用于源地址
- IP多播数据报是“尽最大努力交付”，并且不产生ICMP差错报文

永久组播地址

D类地址中有些地址已经被因特网号码指派管理局IANA指派为永久组地址，不能随便使用

- 224.0.0.0 基地址（保留）
- 224.0.0.1 本子网上的所有参加多播的主机和路由器
- 224.0.0.2 本子网上的所有参加多播的路由器
- 224.0.0.3 未指定
- 224.0.0.4 DVMRP(距离矢量组播路由选择协议)路由器
- ……
- 224.0.1.0 至 238.255.255.255 全球范围都可使用的多播地址

IP多播的种类

(1) 只在本局域网上进行硬件多播

- 虽然比较简单，但很重要，因为现在大部分主机都是通过局域网接入到因特网的

(2) 在因特网的范围进行多播

- 在因特网网上进行多播的最后阶段，还是要把多播数据报在局域网上用硬件多播交付多播组的所有成员

Q33：如何在因特网上实现IP多播？

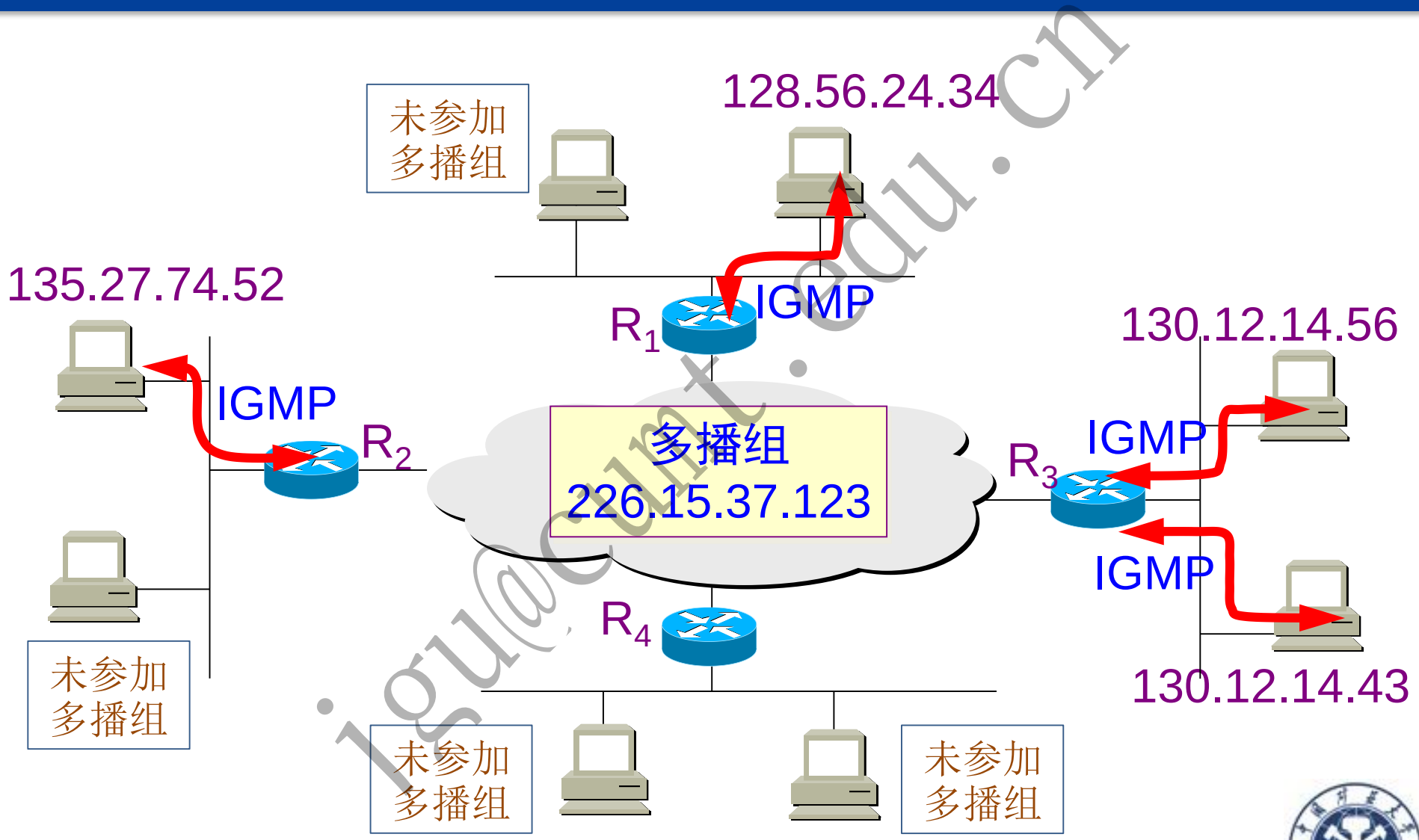
IP多播需要两种协议

- 为了使路由器知道多播组成员的信息，需要利用网际组管理协议 IGMP (Internet Group Management Protocol)。

多播组成员的管理

- 一个多播会话的多播源并不一定要成为接收其发送的流量的多播组中的成员。
  - 一般情况下，源并不知道哪些主机是组员，接收者任何时候都可以自由加入和离开组。
  - 如果源和所有的组员共享一个LAN，那么就不需要其它协议。
  - 如果发送的多播流量需要经过大型的网络，则路由器必须通过某种方法获知连接的网络中是否有组员，如果有，是哪个组的成员。

IGMP使多播路由器知道多播组成员信息



IGMP 的使用范围

- IGMP 并非在因特网范围内对所有多播组成员进行管理的协议。
- IGMP 不知道 IP 多播组包含的成员数，也不知道这些成员都分布在哪些网络上。
- IGMP 协议是让连接在本地局域网上的多播路由器知道本局域网上是否有主机（严格讲，是主机上的某个进程）参加或退出了某个多播组。

仅有IGMP协议是不够的

- 连接在局域网上的多播路由器还必须和因特网上的其他多播路由器协同工作，以便把多播数据报用最小代价传送给所有的组成员。这就需要使用多播路由选择协议。

Q34：IGMP协议如何工作？

- 1989 年公布的 RFC 1112（IGMPv1）早已成为了因特网的标准协议。
- 1997 年公布的 RFC 2236（IGMPv2，建议标准）对 IGMPv1 进行了更新。
- 2002 年 10 月公布了 RFC 3376（IGMPv3，建议标准），宣布 RFC 2236（IGMPv2）是陈旧的。

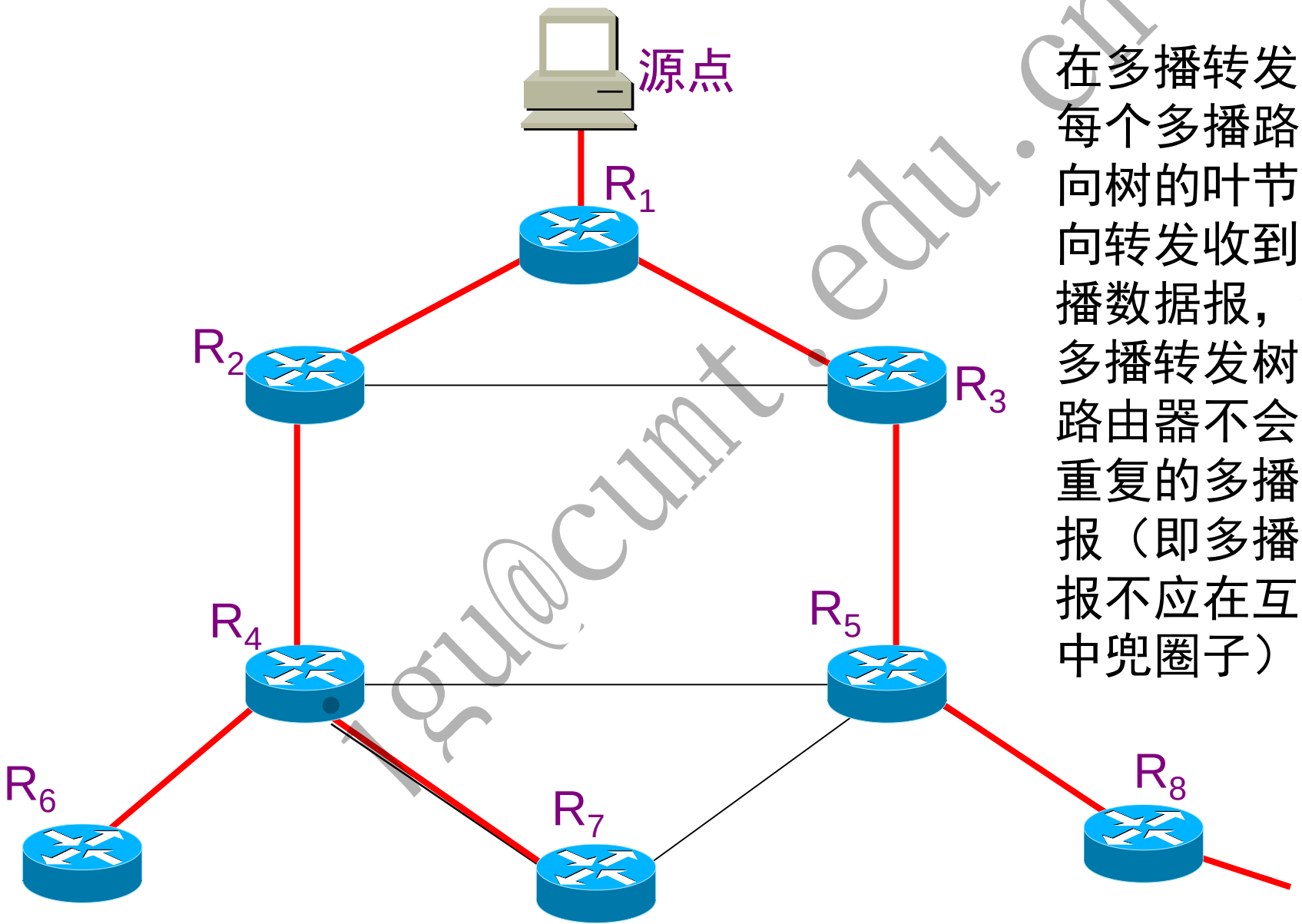
IGMP 可分为两个阶段

- 第一阶段：当某个主机加入新的多播组时，该主机应向多播组的多播地址发送IGMP 报文，声明自己要成为该组的成员。本地的多播路由器收到 IGMP 报文后，将组成员关系转发给因特网上的其他多播路由器。
- 第二阶段：因为组成员关系是动态的，因此本地多播路由器要周期性地探询本地局域网上的主机，以便知道这些主机是否还继续是组的成员。
  - 只要某个组中有一个主机响应，那么多播路由器就认为这个组是活跃的，但一个组在经过几次的探询后仍然没有一个主机响应，则不再将该组的成员关系转发给其他的多播路由器。

Q35：如何实现IP多播路由选择？

- 虽然在TCP/IP中IP多播协议已成为建议标准，但多播路由选择协议（用来在多播路由器之间传播路由信息）则尚未标准化。
- 在多播过程中一个多播组中的成员是动态变化的。
  - 例如，在收听网上的某个广播节目时，随时会有主机加入或离开这个多播组。
- 多播路由选择实际上就是要以源主机为根结点，在多播组成员之间的构造一棵多播转发树。
- 在一个特定的“发送源，目的组”对上的IP多播流量都是通过这个转发树从发送源传输到接受者的，这个转发树连接了该多播组中所有主机。

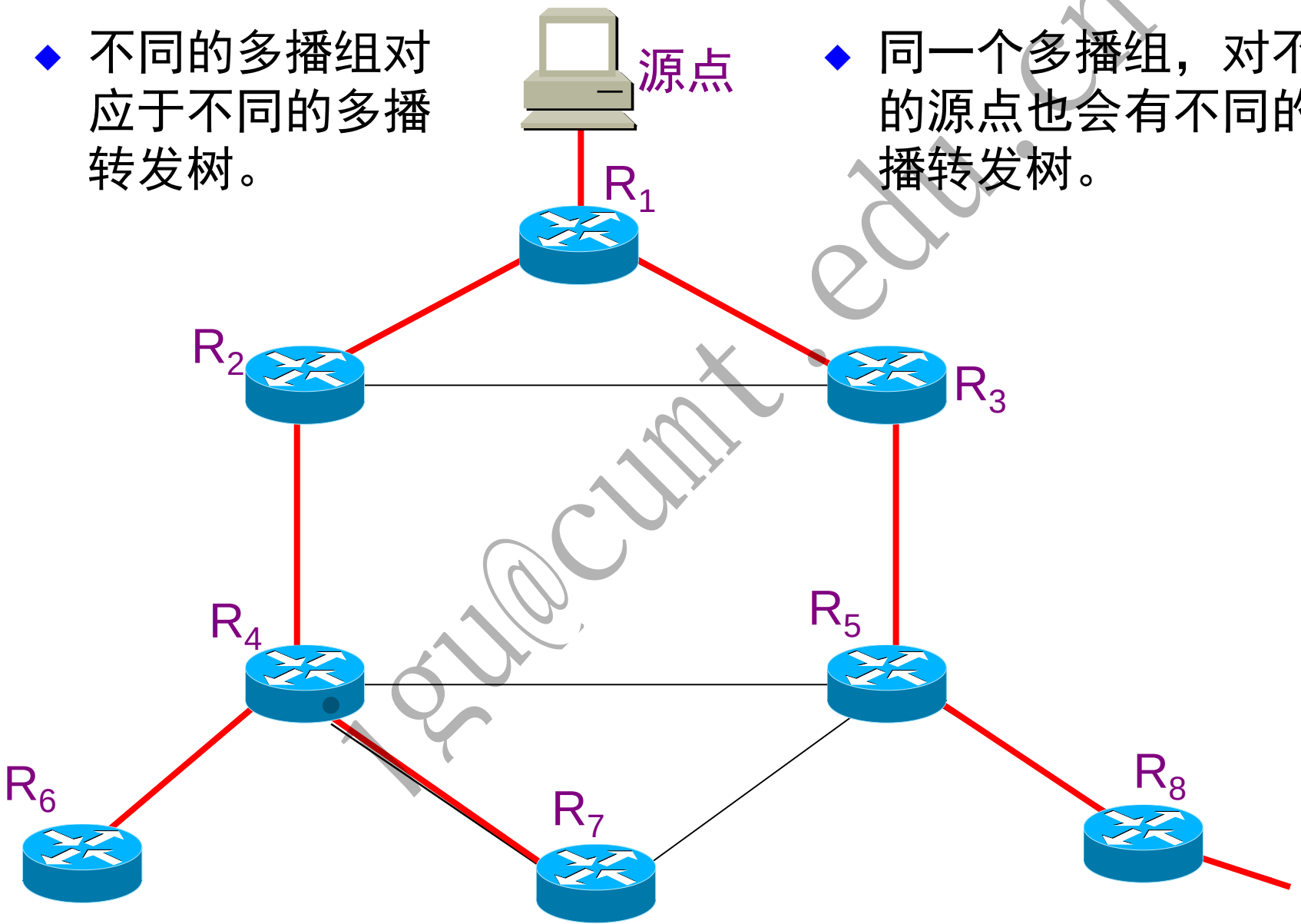
IP多播转发树



在多播转发树上，每个多播路由器向树的叶节点方向转发收到的多播数据报，但在多播转发树上的路由器不会收到重复的多播数据报（即多播数据报不应在互联网中兜圈子）。

以源点为根的多播转发树

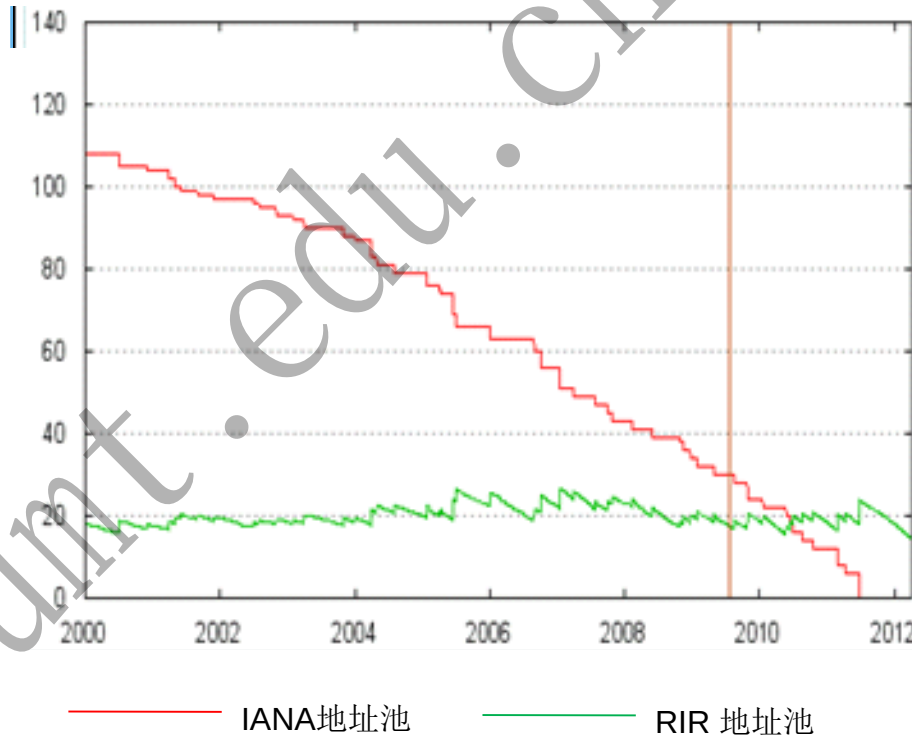
- 不同的多播组对应于不同的多播转发树。
- 同一个多播组，对不同的源点也会有不同的多播转发树。



- 已有的多种实用多播路由选择协议在转发多播数据报使用了以下三种方法：
  - 洪泛与剪除
  - 隧道技术(tunneling)
  - 基于核心的发现技术
- 不同的IP多播路由协议使用不同的技术来构造这些多播转发树，一旦这个树构造完成，所有的多播流量都将通过它来传播。
- 根据网络中多播组成员的分布，IP多播路由协议可以分为密集模式和稀疏模式两种基本类型。

Q36：如何缓解IPv4地址的紧缺？

2009年10月22日



- 到2011年2月，32位的IPv4顶级地址(top-level)已经耗尽。
- 所有IPv4地址空间已分配给全球五大区域互联网注册机构。ISP 已经不能再申请到新的 IPv4地址块了。
- 中国在2014-2015年逐步停止向新用户和应用分配IP地址。

本地地址与全球地址

- 本地地址——仅在机构内部使用的 IP 地址，可以由本机构自行分配，而不需要向因特网的管理机构申请。
- 全球地址——全球唯一的IP地址，必须向因特网的管理机构申请。

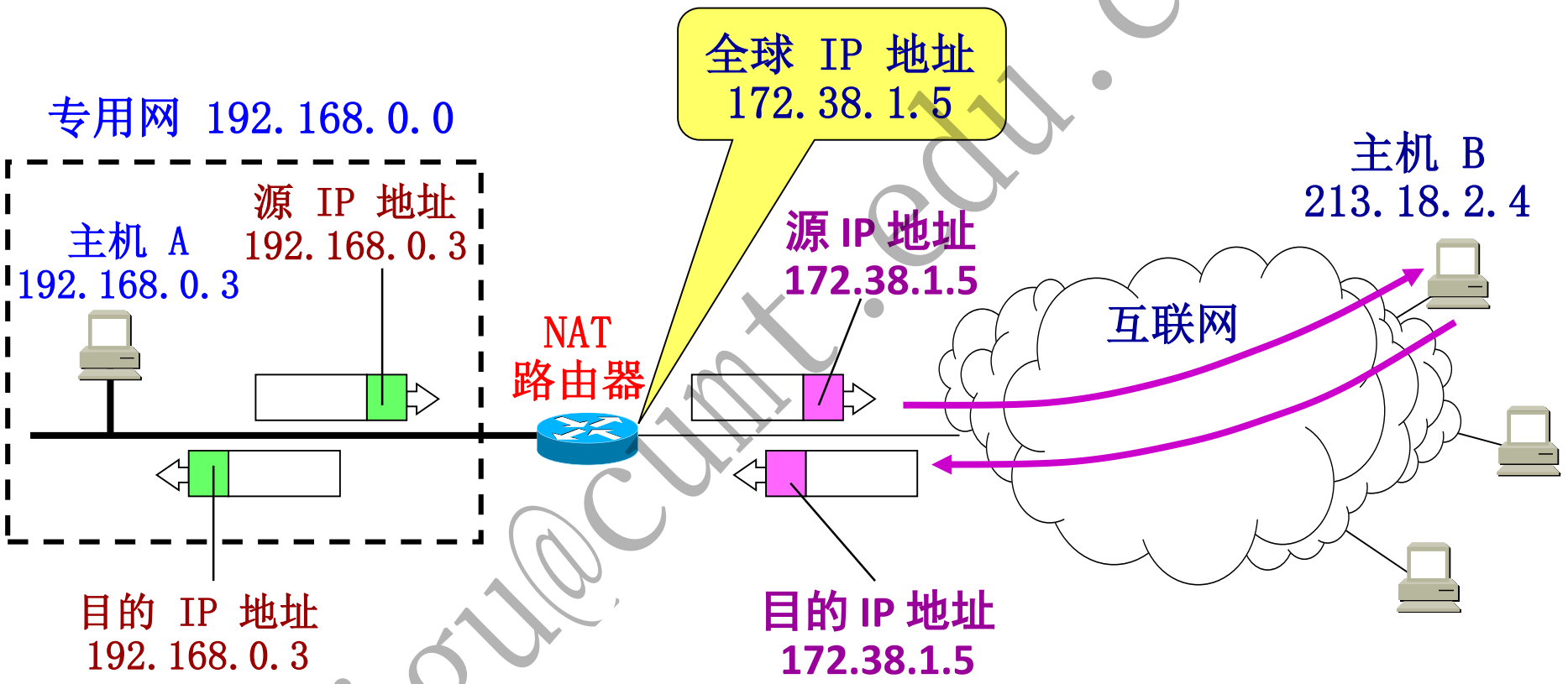
RFC 1918 指明的专用地址(private address)

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 到 172.31.255.255
- 192.168.0.0 到 192.168.255.255
- 这些地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信，即专用地址只能用作本地地址而不能用作全球地址。
  - 在因特网中的所有路由器对目的地址是专用地址的数据报一律不进行转发。

网络地址转换 NAT

- 网络地址转换 NAT (Network Address Translation) 方法于1994年提出。
- 需要在专用网连接到因特网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 NAT路由器，它至少有一个有效的外部全球地址 IP_G。
- 所有使用本地地址的主机在和外界通信时都要在 NAT 路由器上将其本地地址转换成 IP_G 才能和因特网连接。

网络地址转换的过程



NAT 路由器的工作原理

网络地址转换的过程

- 可以看出，在内部主机与外部主机通信时，在NAT路由器上发生了两次地址转换：
  - 离开专用网时：替换源地址，将内部地址替换为全球地址；
  - 进入专用网时：替换目的地址，将全球地址替换为内部地址；

NAT地址转换表举例

方向	字段	旧的IP地址	新的IP地址
出	源IP地址	192.168.0.3	172.38.1.5
入	目的IP地址	172.38.1.5	192.168.0.3
出	源IP地址	192.168.0.7	172.38.1.6
入	目的IP地址	172.38.1.6	192.168.0.7

网络地址与端口号转换 NAPT

- 为了更加有效地利用 NAT 路由器上的全球IP地址，现在常用的 NAT 转换表把运输层的端口号也利用上。这样，就可以使多个拥有本地地址的主机，共用一个 NAT 路由器上的全球 IP 地址，因而可以同时和互联网上的不同主机进行通信。
- 使用端口号的 NAT 叫作网络地址与端口号转换NAPT (Network Address and Port Translation)，而不使用端口号的 NAT 就叫作传统的 NAT (traditional NAT)。

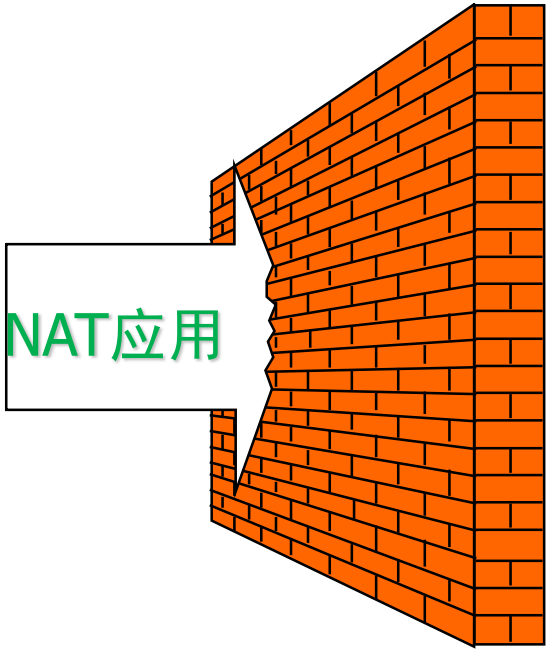
NAPT 地址转换表

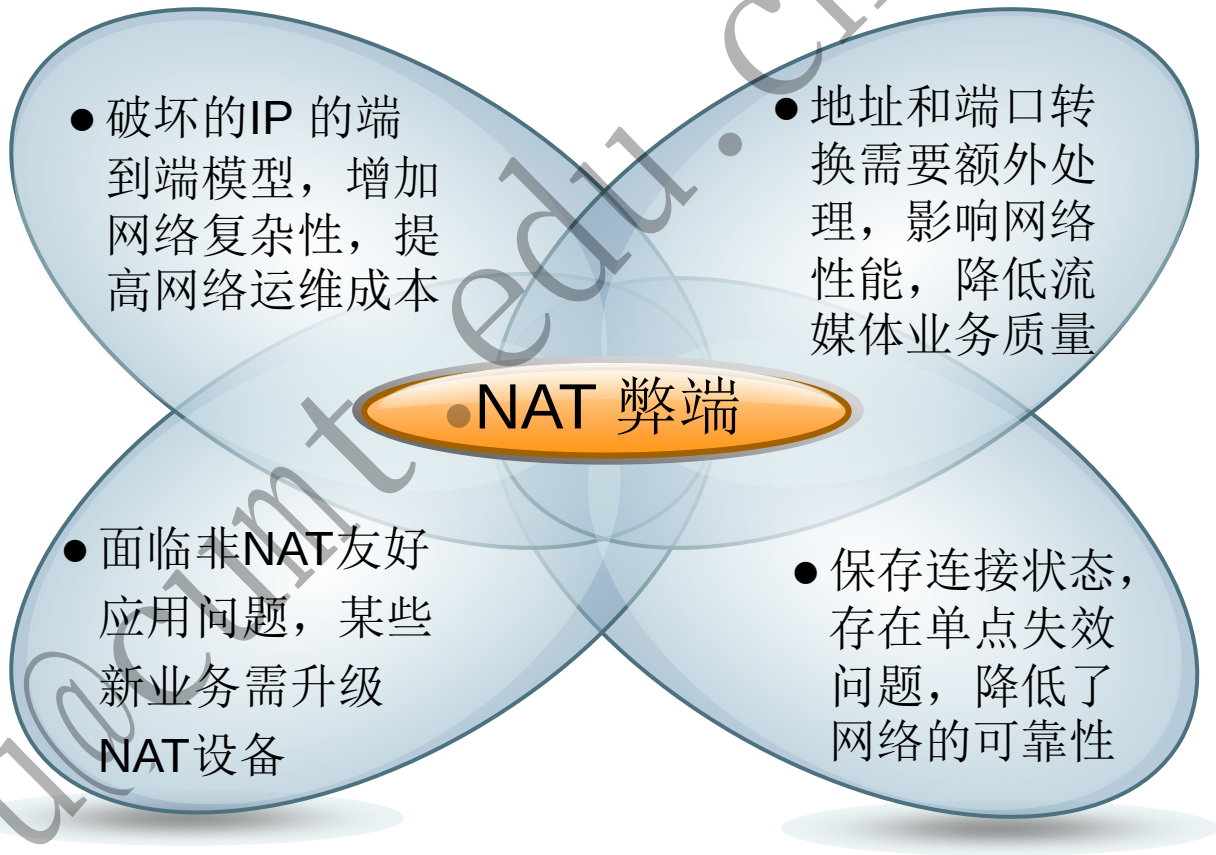
NAPT 地址转换表举例

方向	字段	旧的IP地址和端口号	新的IP地址和端口号
出	源IP地址:TCP源端口	192.168.0.3:30000	172.38.1.5:40001
出	源IP地址:TCP源端口	192.168.0.4:30000	172.38.1.5:40002
入	目的IP地址:TCP目的端口	172.38.1.5:40001	192.168.0.3:30000
入	目的IP地址:TCP目的端口	172.38.1.5:40002	192.168.0.4:30000

NAPT把专用网内不同的源 IP 地址，都转换为同样的全球 IP 地址。但对源主机所采用的 TCP 端口号（不管相同或不同），则转换为不同的新的端口号。因此，当 NAPT 路由器收到从互联网发来的应答时，就可以从 IP 数据报的数据部分找出运输层的端口号，然后根据不同的目的端口号，从 NAPT 转换表中找到正确的目的主机。

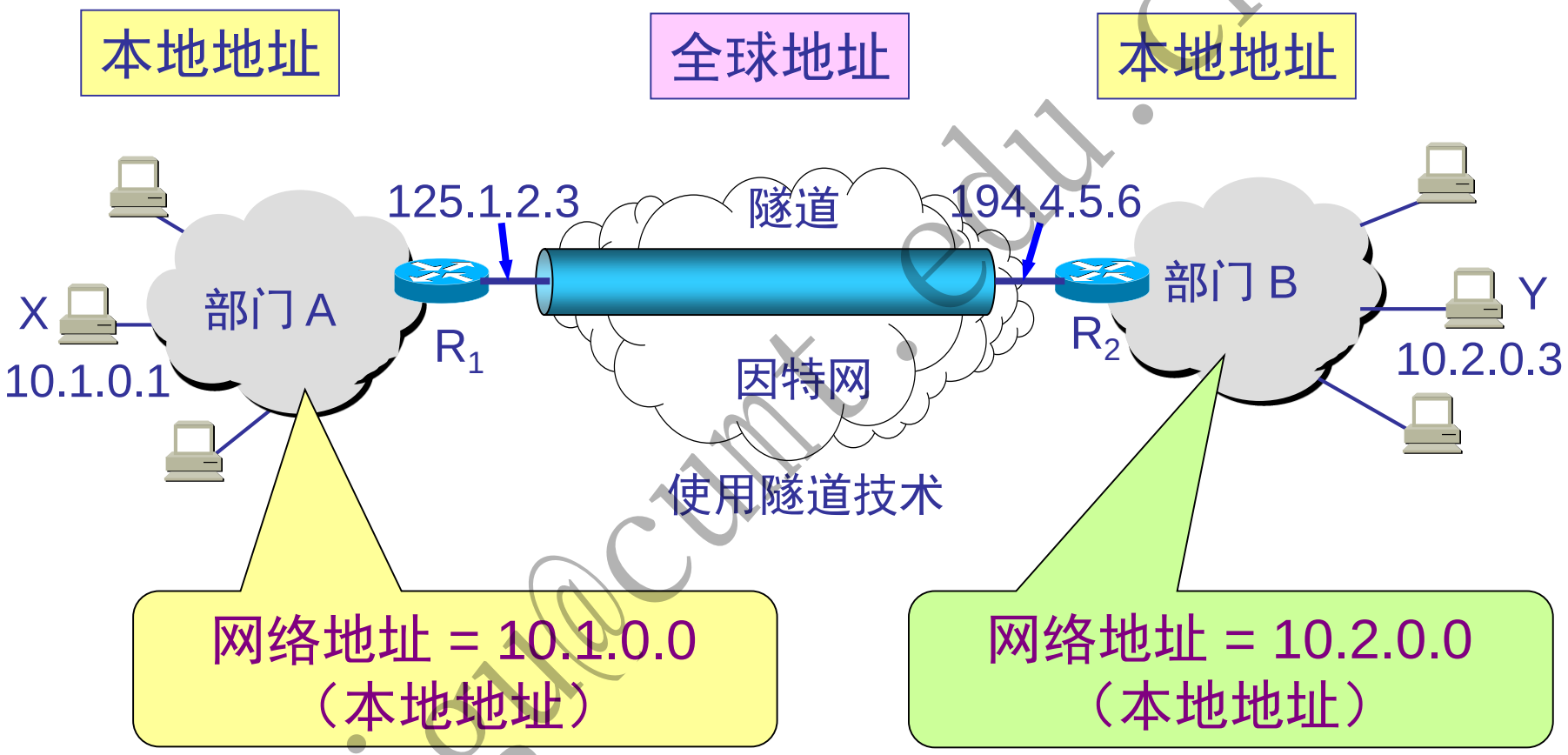
NAT局限性





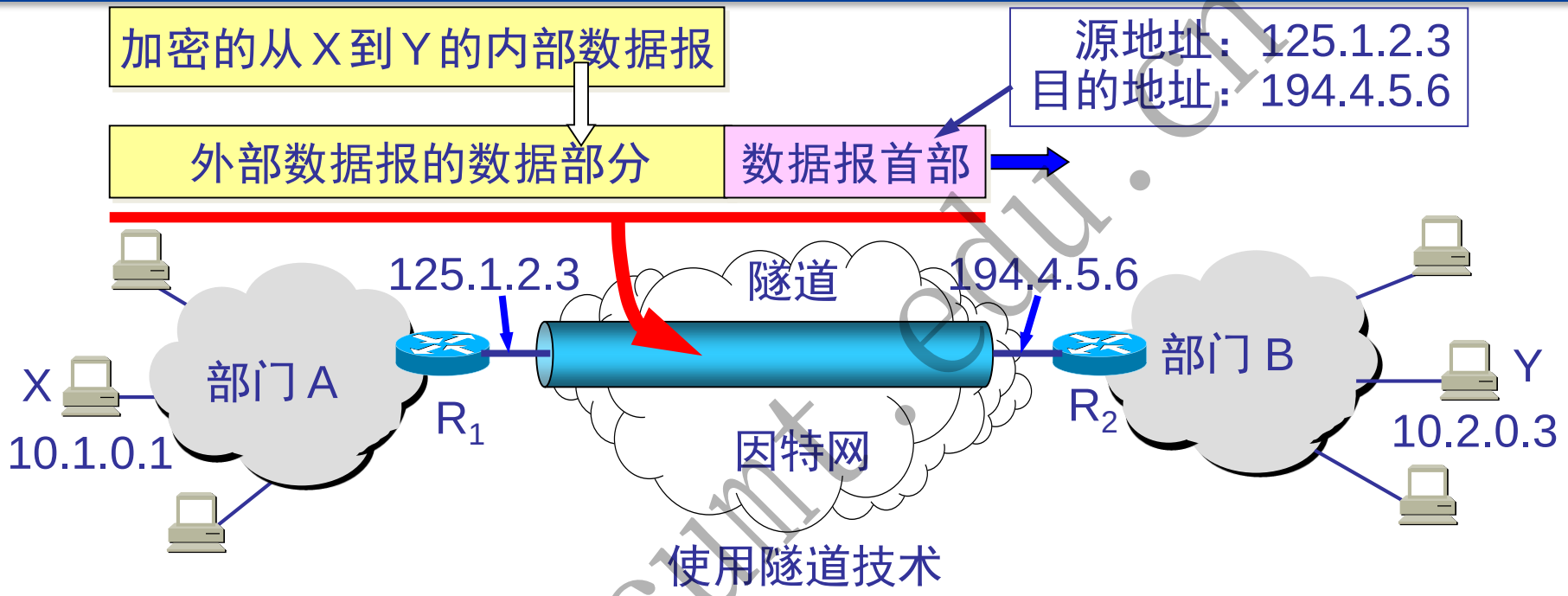
- **NAT延缓了IPv4地址耗尽，但也为网络带来消极影响；**
- **NAT是一种救急措施而非最终解决方案；**

Q37：如何跨机构实现安全通信？



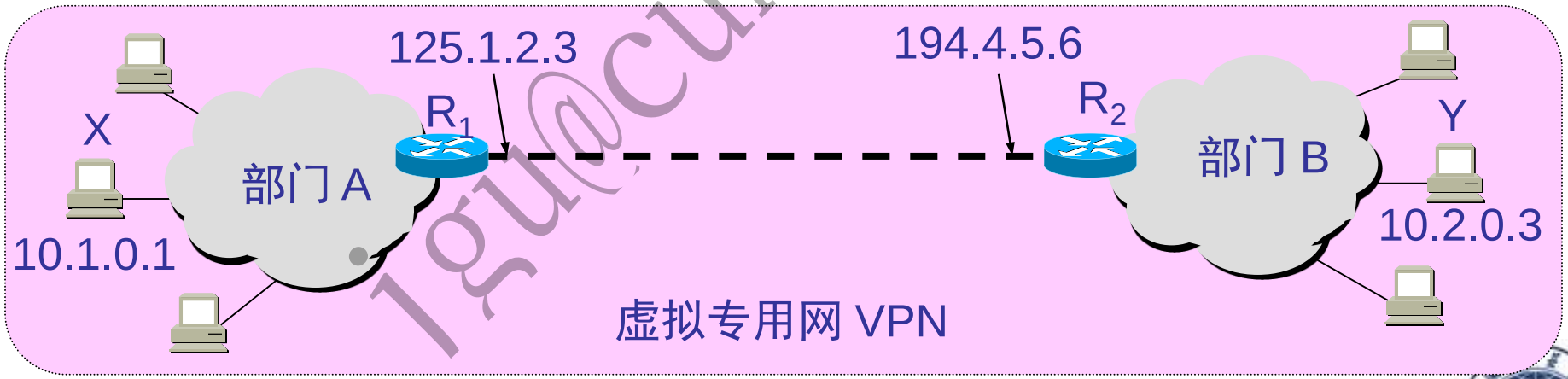
用隧道技术实现虚拟专用网

用隧道技术实现虚拟专用网



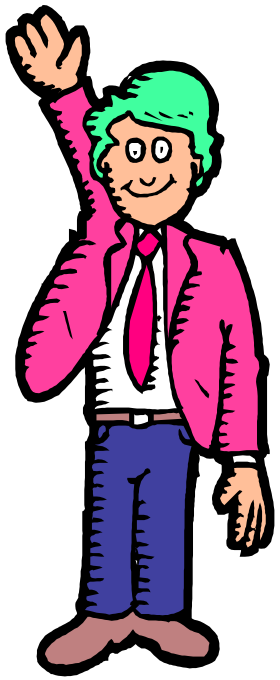
内联网 intranet 和外联网 extranet（都是基于 TCP/IP 协议）

- 由部门 A 和 B 的内部网络所构成的虚拟专用网 VPN 又称为内联网(intranet)，表示部门 A 和 B 都是在同一个机构的内部。
- 一个机构和某些外部机构共同建立的虚拟专用网 VPN 又称为外联网(extranet)。



远程接入VPN
(remote access VPN)

- 有的公司可能没有分布在不同场所的部门，但有很多流动员工在外地工作。公司需要和他们保持联系，远程接入 VPN 可满足这种需求。
- 在外地工作的员工拨号接入因特网，而驻留在员工 PC 机中的 VPN 软件可在员工的 PC 机和公司的主机之间建立 VPN 隧道，因而外地员工与公司通信的内容是保密的，员工们感到好像就是使用公司内部的本地网络。



THANK YOU!