网络地址转换NAT

网络地址转换 NAT

问题：在专用网上使用专用地址的主机如何与互联网上的主机通信（并不需要加密）？

解决：

(1) 再申请一些全球 IP 地址。但这在很多情况下是不容易做到的。

(2)采用网络地址转换 NAT。这是目前使用得最多的方法。

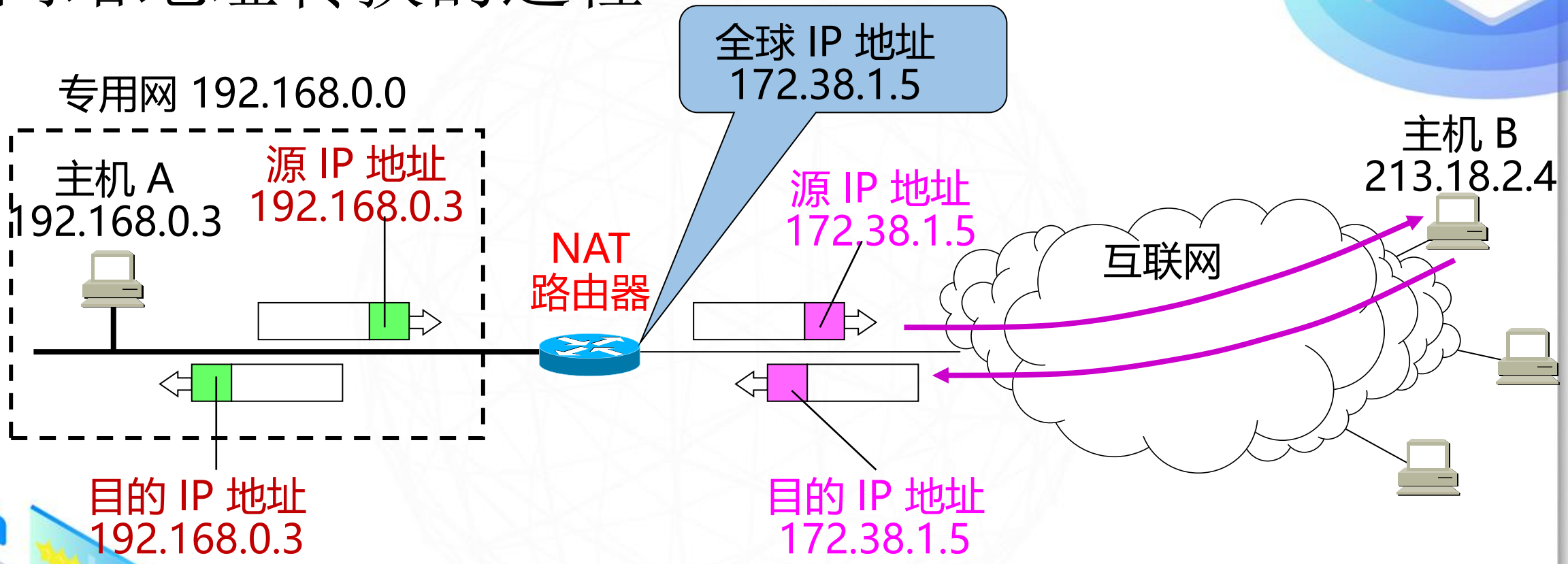
网络地址转换 NAT

网络地址转换 NAT需要在专用网连接到互联网的路由器上安装 NAT 软件。

装有 NAT 软件的路由器叫作 NAT路由器，它至少有一个有效的外部全球IP地址。

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全球 IP 地址，才能和互联网连接。

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

内部主机 A 用本地地址 IP_A 和互联网上主机 B 通信所发送的数据报必须经过 NAT 路由器。

NAT 路由器将数据报的源地址 IP_A 转换成全球地址 IP_G，并把转换结果记录到NAT地址转换表中，目的地址 IP_B 保持不变，然后发送到互联网。

NAT 路由器收到主机 B 发回的数据报时，知道数据报中的源地址是 IP_B 而目的地址是 IP_G。

根据 NAT 转换表，NAT 路由器将目的地址 IP_G 转换为 IP_A，转发给最终的内部主机 A。

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；

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

NAT地址转换表举例

网络地址转换 NAT

当 NAT 路由器具有 *n* 个全球 IP 地址时，专用网内最多可以同时有 *n* 台主机接入到互联网。

通过 NAT 路由器的通信必须由专用网内的主机发起。专用网内部的主机不能充当服务器用，因为互联网上的客户无法请求专用网内的服务器提供服务。

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。

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。

网络地址与端口号转换 NAPT

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)

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，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。