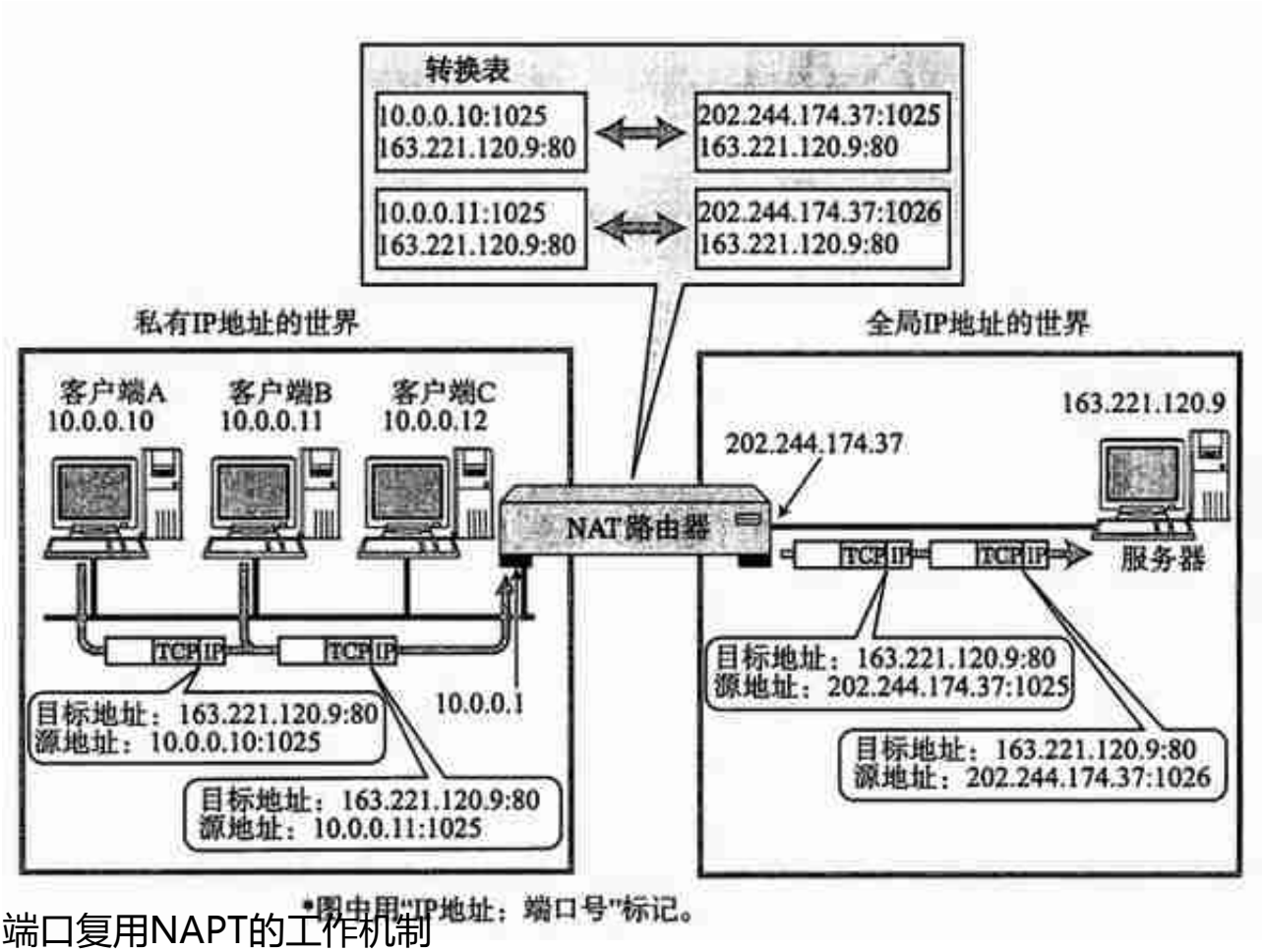
1. 什么是NAT

1.1. NAT定义

NAT（Network Address Translator，网络地址转换）是用于在本地网络中使用私有地址，在连接互联网时转而使用全局 IP
地址的技术。NAT实际上是为解决IPv4地址短缺而开发的技术。

1.2. NAT工作机制

如下图所示，以 10.0.0.10 的主机与 163.221.120.9 的主机进行通信为例讲解 NAT 的工作机制。利用 NAT，途中的 NAT 路由器将发送源地址从 10.0.0.10
转换为全局的 IP 地址（202.244.174.37）再发送数据。反之，当响应数据从 163.221.120.9 发送过来时，目标地址（202.244.174.37）先被转换成私有 IP 地址 10.0.0.10 以后再被转发。



端口复用NAPT的工作机制

主机 163.221.120.9 的端口号是 80，私网中有 2 个客户端 10.0.0.10 和 10.0.0.11 同时进行通信，并且这 2 个客户端的本地端口都是 1025。此时，仅仅转换 IP 地址为全局地址 202.244.174.37
，会令转换后的数字完全一致。因此，为了区分这 2 个会话，只要将 10.0.0.11 的端口号转换为 1026 就可以解决问题。NAPT 路由器通过生成转换表，就可以正确地转换地址跟端口的组合，使客户端A、B能同时与服务器之间进行通信。

关键点：利用端口号的唯一性实现了公网 IP 到私网 IP 的转换，理论上最多可以让 65535 台主机共用一个公网 IP 地址

1.4. NAT技术的优缺点

1.4.1. 优点

- 节省合法的公有 IP 地址（最大的优点）
- 当网络发生变化时，避免重新编址。
- 对外隐藏内部地址，增加网络安全性

1.4.2. 缺点

- 无法从 NAT 的外部向内部服务器建立连接（NAT穿越）
- 转换表的生成和转换操作都会产生一定的开销
- 通信过程中一旦 NAT 遇到异常需重新启动时，所有的 TCP 连接都将被重置。即使备置两台 NAT 做容灾备份，TCP 连接还是会被断开。