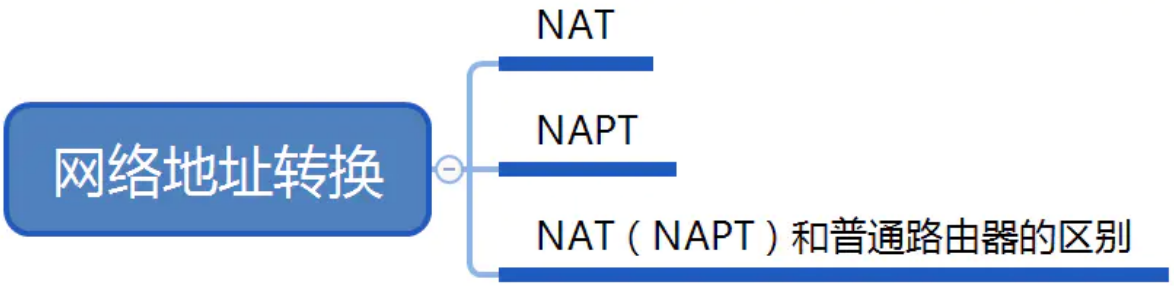
网络地址转换NAT

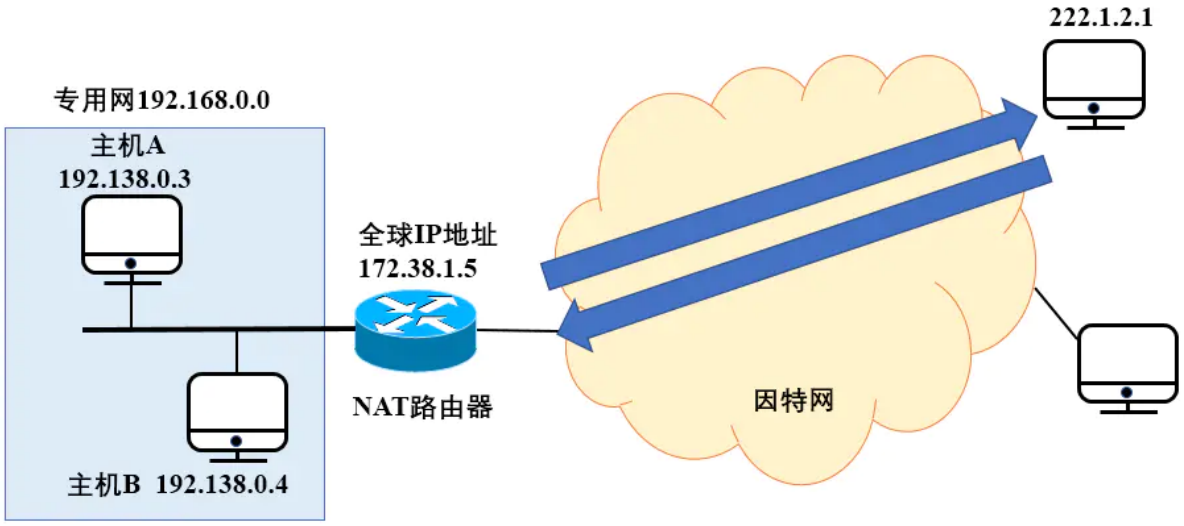
内容总览



1.网络地址转发NAT

通过前面已经知道，**在互联网中的所有路由器，对目的地址是私有网络的数据报一律不转发。**如果要实现专用网中的主机接入互联网就需要网络地址转换。

网络地址转换NAT（Network Address Translation）：在专用（私有）网连接到因特网的路由器上安装NAT软件，安装了NAT软件的路由器叫NAT路由器，它至少有一个有效的外部全球IP地址。



NAT实现专用网和互联网通信原理：**当所有使用本地主机地址的主机和外界通信时，都要在NAT路由器上将本地地址转换为全球IP地址，才能和互联网连接。**

> 例如，NAT路由器收到从专用网内部主机A发往互联网上主机B的IP数据报，源IP地址是192.168.0.3，而目的地址是 222.1.2.1。NAT路由器把IP数据报的源地址 192.168.0.3转换为新的源IP地址，即NAT路由器的全球IP地址 172.38.15，记录到NAT地址转换表中，然后再转发出去。因此，主机B收到这个IP数据报时，以为A的IP地址是 172.38.15。

> 当主机B给A发送应答时，IP数据报的目的地址是NAT路由器的IP地址 172.38.15，主机B并不知道主机A的IP地址，即使知道了也不能使用，因为主机A的IP地址是私有地址，互连网不会转发任何目的地址是私有地址的数据报。当NAT路由器收到的互联网B发送来的数据报时，要进行一次IP地址转换。通过NAT地址转换表（如下图），就可把IP数据报的上的目的地址 172.38.15转换为主机A的IP地址 192.168.0.3。

方向	字段	旧IP地址	新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

当NAT路由器具有n个全球IP地址时，专用网络中最多可以同时有n台主机接入到互联网。这样就可以使专用网内较多的主机，轮流使用NAT路由器有限数量的全球IP地址，这也表明了NAT地址转换表的内容会频繁更新。

从上面可以看出，**通过NAT路由器的通信必须由专用网内的主机发起。**如果互联网上的主机要发起通信，IP数据报到达NAT路由器时，NAT路由器就不知道应当把目的IP地址转换成专用网内的哪一个本地的IP地址。这是因为通信是专用网的主机发起时，NAT地址转换表中记录了主机与路由器IP地址的对应关系，所以互联网中的主机响应数据报时能找到正确的主机。

2.网络地址与端口号转换NAPT

由于NAT路由器的一个IP地址同一时刻只能给一个专用主机使用，为了更加有效率的利用NAT路由器上的全球IP地址，在NAT转换表中引入了运输层的端口号。这样就可以让多个主机同时公用一个NAT路由器上的全球IP地址。

使用了端口号的NAT也叫做**网络地址与端口号转换NAPT**（Network Address and Port Translation），没有使用端口号的NAT叫做传统的NAT，但是实际中并不作区分，都叫NAT更加简单。

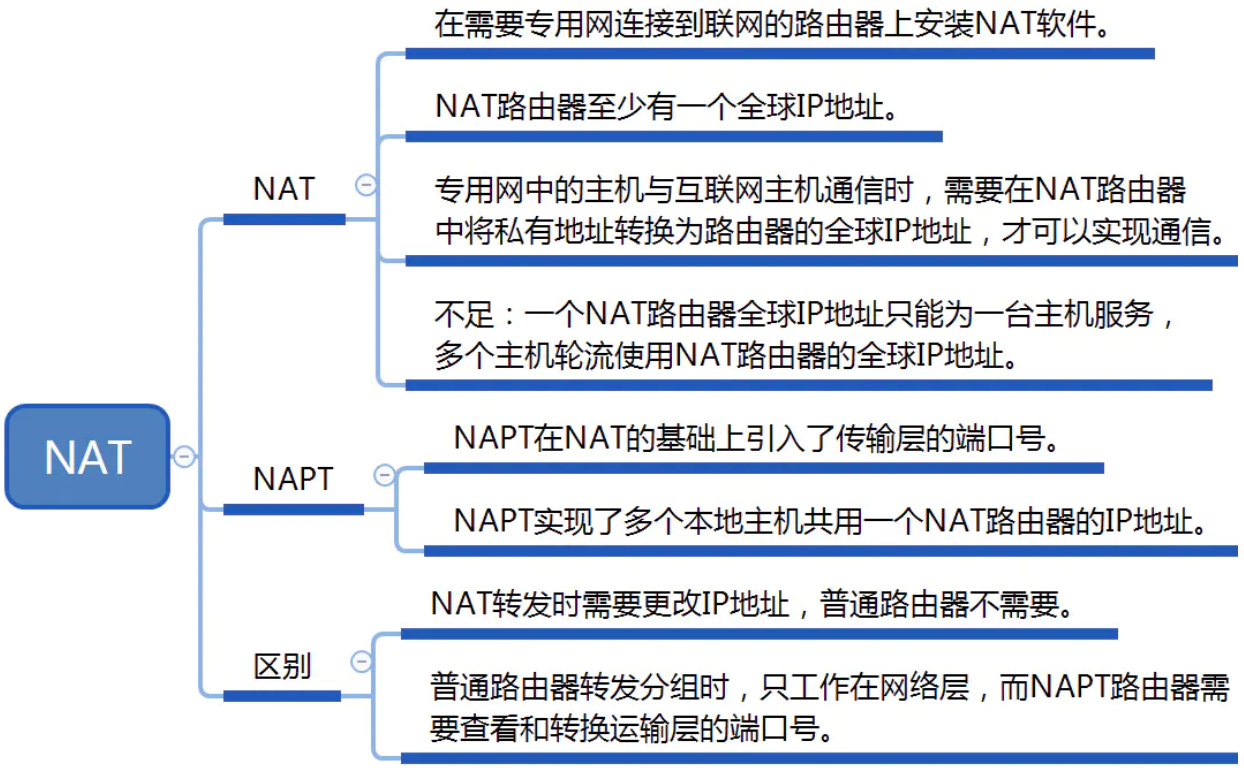
方向	字段	旧IP地址	新IP地址
出	源IP地址：端口号	192.168.0.3：30000	172.38.1.5：40001
入	目的IP地址：端口号	172.38.1.5：40001	192.168.0.3：30000
出	源IP地址：端口号	192.168.0.2：30000	172.38.1.5：40002
入	目的IP地址：端口号	172.38.1.5：40002	192.168.0.2：30000

从上表可以看出，专用网内主机193.168.0.3和192.168.0.2都向互联网发送IP数据报，它们的TCP端口号都使用了30000（不同主机可以使用相同的端口号），但是无论专用网中的主机使用的TCP端口号是相同的还是不同的，NAPT路由器都会把它们转换为不同的新的端口号，如上图中分别将两台主机的端口号转换为40001和40002。因此，当NAPT路由器接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地址转换表中找到正确的主机。

NAT（NAPT）和普通路由器的区别：

> (1) 普通路由器在转发IP数据报时，对于源地址和目的地址都是不改变的，而NAT路由器在转发IP数据报时，一定要更换其IP地址（转换源IP地址或目的IP地址）。
>
> (2) 普通路由器工作在网络层，而NAPT路由器还需要查看和转换运输层的端口号。

3.总结


NAT
NAT
在需要专用网连接到联网的路由器上安装NAT软件。
NAT路由器至少有一个全球IP地址。
专用网中的主机与互联网主机通信时，需要在NAT路由器中将私有地址转换为路由器的全球IP地址，才可以实现通信。
不足：一个NAT路由器全球IP地址只能为一台主机服务，多个主机轮流使用NAT路由器的全球IP地址。
NAPT
NAPT在NAT的基础上引入了传输层的端口号。
NAPT实现了多个本地主机共用一个NAT路由器的IP地址。
区别
NAT转发时需要更改IP地址，普通路由器不需要。
普通路由器转发分组时，只工作在网络层，而NAPT路由器需要查看和转换运输层的端口号。