计算机网络与通信技术

第四章 网络层

北京交通大学 刘彪

计算机网络与通信技术

知识点：VPN和NAT

北京交通大学 刘彪

1、虚拟专用网 VPN

- 由于 IP 地址的紧缺，一个机构能够申请到的IP地址数往往远小于本机构所拥有的主机数。
- 考虑到互联网并不很安全，一个机构内也并不需要把所有的主机接入到外部的互联网。
- 假定在一个机构内部的计算机通信也是采用 TCP/IP 协议，那么从原则上讲，对于这些仅在机构内部使用的计算机就可以由本机构自行分配其 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，而不需要向互联网的管理机构申请。
- 全球地址——全球唯一的 IP 地址，必须向互联网的管理机构申请。

本地地址与全球地址

- 问题：在内部使用的本地地址就有可能和互联网中某个 IP 地址重合，这样就会出现地址的二义性问题。
- 解决：RFC 1918 指明了一些专用地址 (private address)。专用地址只能用作本地地址而不能用作全球地址。在互联网中的所有路由器，对目的地址是专用地址的数据报一律不进行转发。

专用IP地址

三个专用 IP 地址块：

(1) 10.0.0.0 到 10.255.255.255

A类，或记为10.0.0.0/8，它又称为 24 位块

(2) 172.16.0.0 到 172.31.255.255

B类，或记为172.16.0.0/12，它又称为 20 位块

(3) 192.168.0.0 到 192.168.255.255

C类，或记为192.168.0.0/16，它又称为 16 位块

专用网

- 采用这样的专用 IP 地址的互连网络称为专用互联网或本地互联网，或更简单些，就叫做专用网。
- 因为这些专用地址仅在本机构内部使用。专用IP地址也叫做可重用地址(reusable address)。

虚拟专用网 VPN

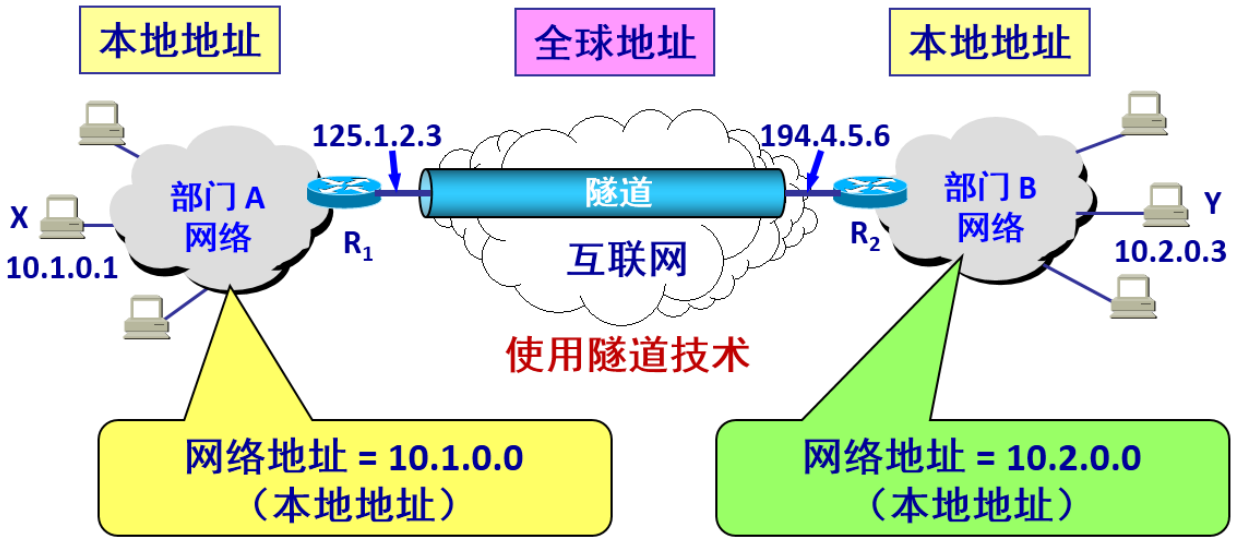
- 利用公用的互联网作为本机构各专用网之间的通信载体，这样的专用网又称为虚拟专用网VPN (Virtual Private Network)。
- “专用网”是因为这种网络是为本机构的主机用于机构内部的通信，而不是用于和网络外非本机构的主机通信。
- “虚拟”表示“好像是”，但实际上并不是，因为现在并没有真正使用通信专线，而VPN只是在效果上和真正的专用网一样

虚拟专用网 VPN 构建

- 如果专用网不同网点之间的通信必须经过公用的互联网，但又有保密的要求，那么所有通过互联网传送的数据都必须加密。
- 一个机构要构建自己的 VPN 就必须为它的每一个场所购买专门的硬件和软件，并进行配置，使每一个场所的 VPN 系统都知道其他场所的地址。

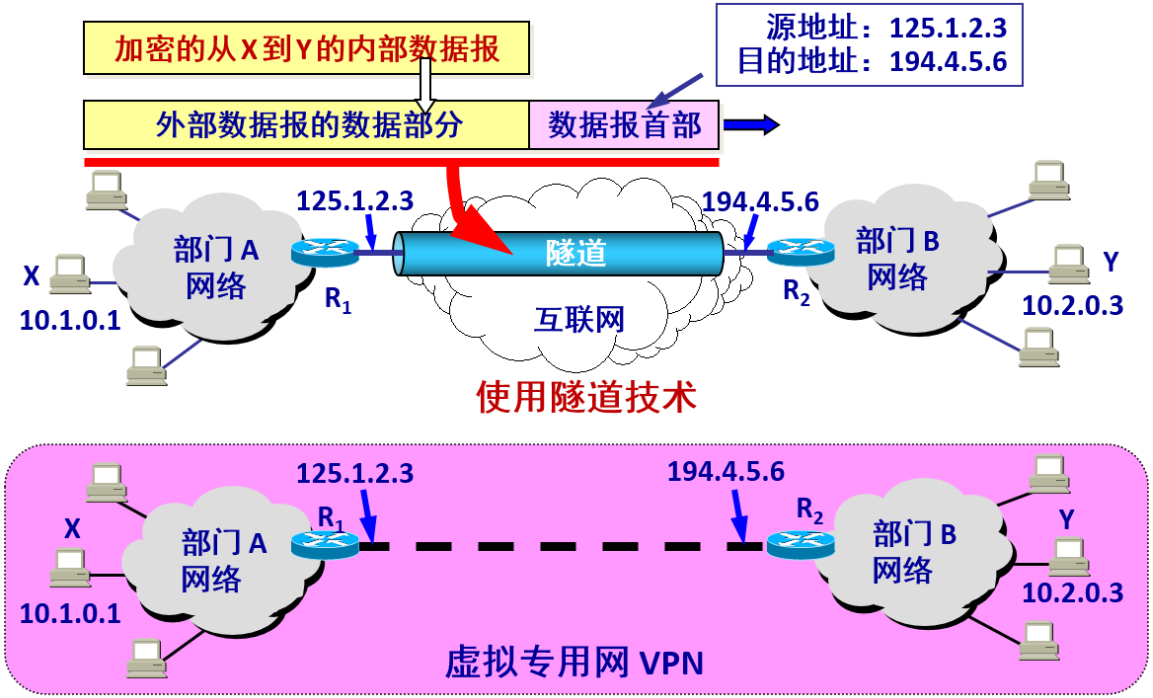
用隧道技术实现虚拟专用网

4.13 VPN和NAT



用隧道技术实现虚拟专用网

4.13 VPN和NAT



远程接入VPN

- 远程接入 VPN (remote access VPN)可以满足外部流动员工访问公司网络的需求。
- 在外地工作的员工拨号接入互联网，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。

2、 网络地址转换 NAT

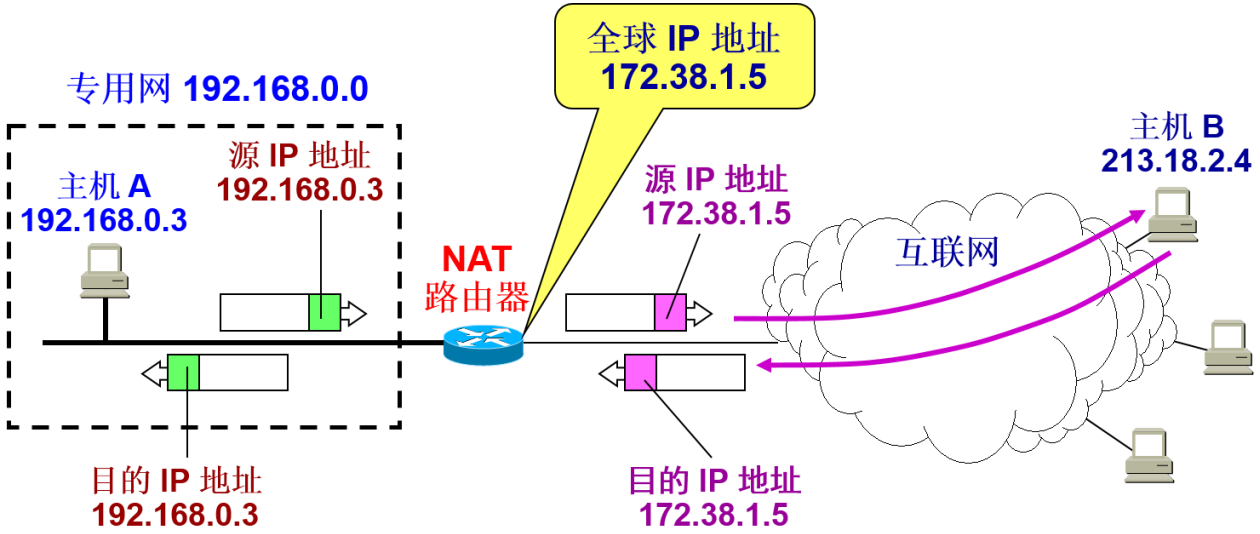
- 问题：在专用网上使用专用地址的主机如何与互联网上的主机通信（并不需要加密）？
- 解决：
  - (1) 再申请一些全球 IP 地址。但这在很多情况下是不容易做到的。
  - (2)采用网络地址转换 NAT。这是目前使用得最多的方法。

网络地址转换 NAT

- 网络地址转换 NAT (Network Address Translation) 方法于1994年提出。
- 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 软件的路由器叫做 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

4.13 VPN和NAT



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；
  - 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。这样就可以使专用网内较多数量的主机，轮流使用 NAT 路由器有限数量的全球 IP 地址。
- 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。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 叫做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 就叫做传统的 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。