## 4.9 虚拟专用网VPN与网络地址转换NAT

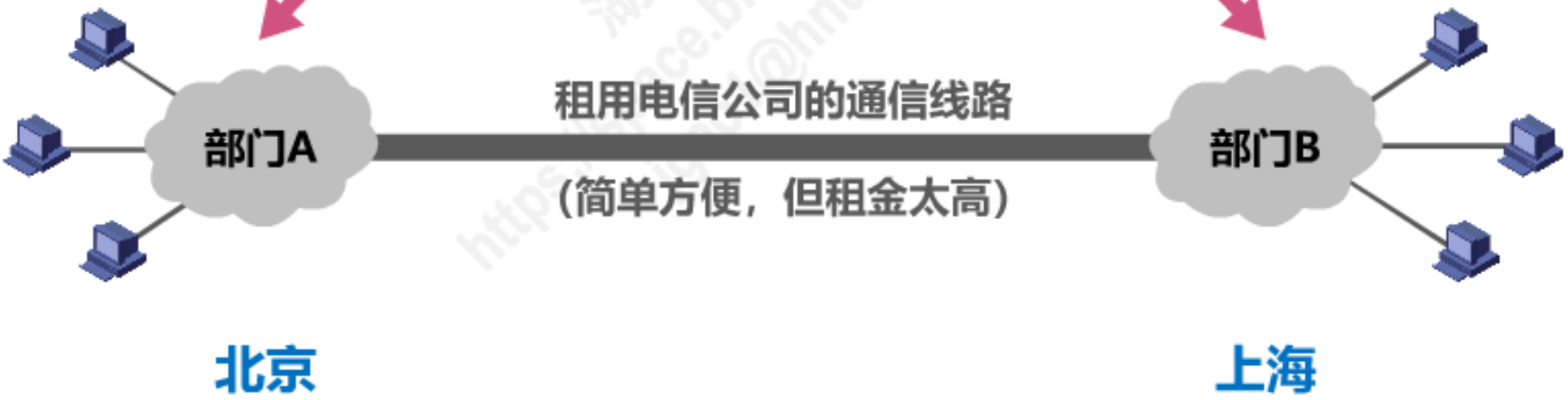


## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)



## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

**利用公用的因特网**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。

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

**利用公用的因特网**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。由于IPv4地址的紧缺，一个机构能够申请到的IPv4地址数量往往远小于本机构所拥有的主机数量。因此，**虚拟专用网中的各主机所分配的地址应该是本机构可自由分配的专用地址**，而不是需要申请的、在因特网上使用的公有地址。

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

**利用公用的因特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。由于IPv4地址的紧缺，一个机构能够申请到的IPv4地址数量往往远小于本机构所拥有的主机数量。因此，虚拟专用网中的各主机所分配的地址应该是本机构可自由分配的专用地址，而不是需要申请的、在因特网上使用的公有地址。**

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

| Address Block | Name | RFC | Allocation Date | Termination Date | Source | Destination | Forwardable | Globally Reachable | Reserved-by-Protocol |
|---|---|---|---|---|---|---|---|---|---|
| 0.0.0.0/8 | "This host on this network" | [RFC1122], Section 3.2.1.3 | 1981-09 | N/A | True | False | False | False | True |
| 10.0.0.0/8 | Private-Use | [RFC1918] | 1996-02 | N/A | True | True | True | False | False |
| 100.64.0.0/10 | Shared Address Space | [RFC6598] | 2012-04 | N/A | True | True | True | False | False |
| 127.0.0.0/8 | Loopback | [RFC1122], Section 3.2.1.3 | 1981-09 | N/A | False [1] | False [1] | False [1] | False [1] | True |
| 169.254.0.0/16 | Link Local | [RFC3927] | 2005-05 | N/A | True | True | False | False | True |
| 172.16.0.0/12 | Private-Use | [RFC1918] | 1996-02 | N/A | True | True | True | False | False |
| 192.0.0.0/24 [2] | IETF Protocol Assignments | [RFC6890], Section 2.1 | 2010-01 | N/A | False | False | False | False | False |
| 192.0.0.0/29 | IPv4 Service Continuity Prefix | [RFC7335] | 2011-06 | N/A | True | True | True | False | False |
| 192.0.0.8/32 | IPv4 dummy address | [RFC7600] | 2015-03 | N/A | True | False | False | False | False |
| 192.0.0.9/32 | Port Control Protocol Anycast | [RFC7723] | 2015-10 | N/A | True | True | True | True | False |
| 192.0.0.10/32 | Traversal Using Relays around NAT Anycast | [RFC8155] | 2017-02 | N/A | True | True | True | True | False |
| 192.0.0.170/32, 192.0.0.171/32 | NAT64/DNS64 Discovery | [RFC7050], Section 2.2 | 2013-02 | N/A | False | False | False | False | True |
| 192.0.2.0/24 | Documentation (TEST-NET-1) | [RFC5737] | 2010-01 | N/A | False | False | False | False | False |
| 192.31.196.0/24 | AS112-v4 | [RFC7535] | 2014-12 | N/A | True | True | True | True | False |
| 192.52.193.0/24 | AMT | [RFC7450] | 2014-12 | N/A | True | True | True | True | False |
| 192.88.99.0/24 | Deprecated (6to4 Relay Anycast) | [RFC7526] | 2001-06 | 2015-03 | | | | | |
| 192.168.0.0/16 | Private-Use | [RFC1918] | 1996-02 | N/A | True | True | True | False | False |
| 192.175.48.0/24 | Direct Delegation AS112 Service | [RFC7534] | 1996-01 | N/A | True | True | True | True | False |
| 198.18.0.0/15 | Benchmarking | [RFC2544] | 1999-03 | N/A | True | True | True | False | False |
| 198.51.100.0/24 | Documentation (TEST-NET-2) | [RFC5737] | 2010-01 | N/A | False | False | False | False | False |
| 203.0.113.0/24 | Documentation (TEST-NET-3) | [RFC5737] | 2010-01 | N/A | False | False | False | False | False |
| 240.0.0.0/4 | Reserved | [RFC1112], Section 4 | 1989-08 | N/A | False | False | False | False | True |
| 255.255.255.255/32 | Limited Broadcast | [RFC8190] [RFC919], Section 7 | 1984-10 | N/A | False | True | False | False | True |

## 4.9 虚拟专用网VPN与网络地址转换NAT

- 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

- 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

- 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 虚拟专用网VPN(Virtual Private Network)

如下图所示，同一机构内不同部门的内部网络所构成的虚拟专用网VPN又称为**内联网VPN**。

有时一个机构的VPN需要有某些外部机构（通常就是合作伙伴）参加进来。这样的VPN就称为**外联网VPN**。

在外地工作的员工需要访问公司内部的专用网络时，只要在任何地点接入到因特网，运行驻留在员工PC中的VPN软件，在员工的PC和公司的主机之间建立VPN隧道，即可访问专用网络中的资源。这种VPN称为**远程接入VPN**。

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)

虽然因特网采用了无分类编址方式来减缓IPv4地址空间耗尽的速度，但由于因特网用户数目的激增，特别是大量小型办公室网络和家庭网络接入因特网的需求不断增加，IPv4地址空间即将面临耗尽的危险仍然没有被解除。

1994年提出了一种网络地址转换NAT的方法再次**缓解了IPv4地址空间即将耗尽的问题**。

NAT能使大量**使用内部专用地址的专用网络用户共享少量外部全球地址来访问因特网上的主机和资源**。

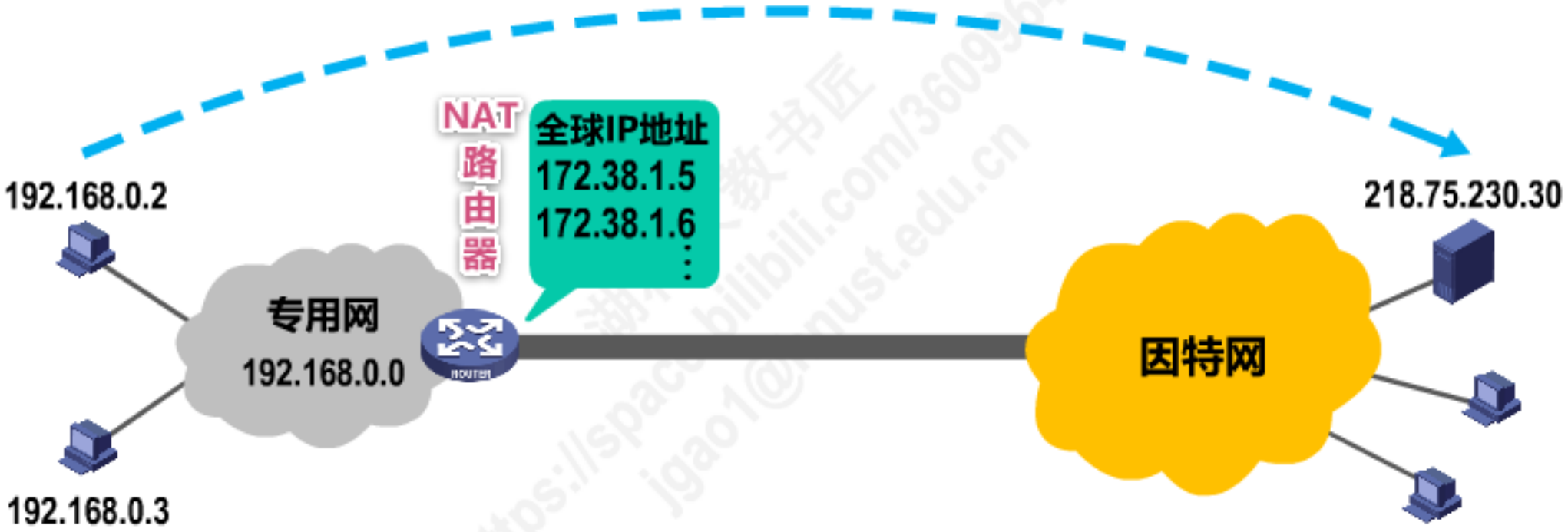
## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)


专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)




专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

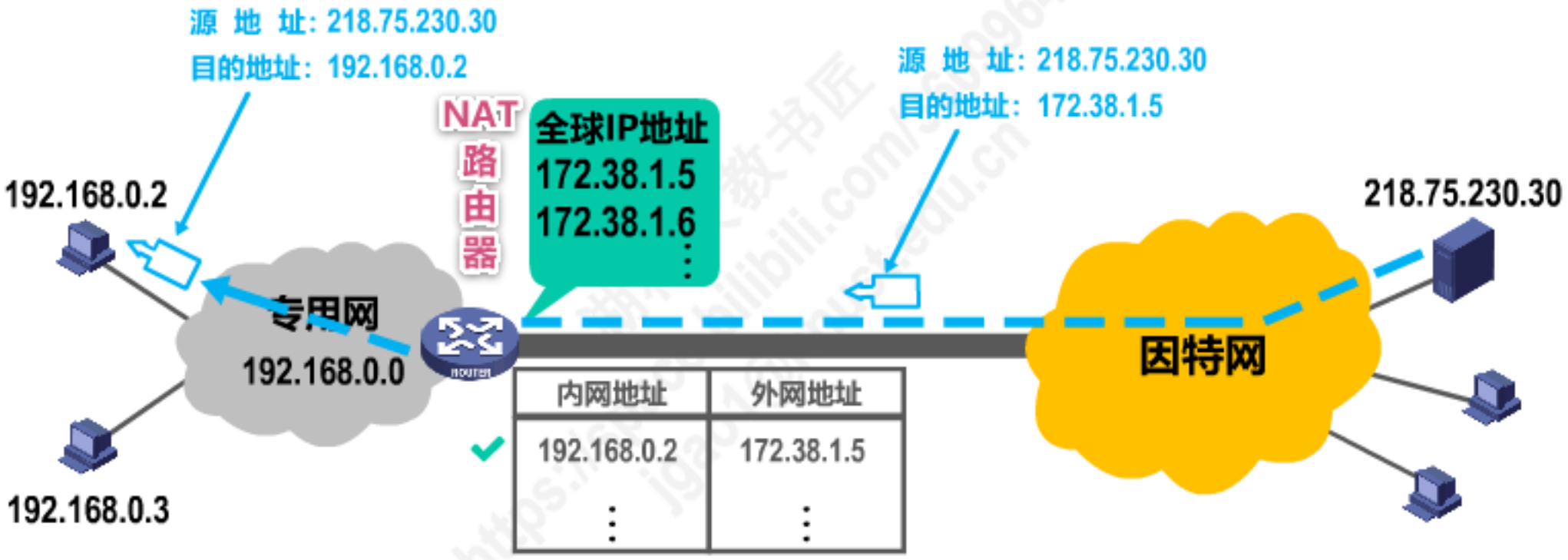
## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)


专用（私有）地址:
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)




专用（私有）地址:
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)

该转换方法存在一个问题：如果NAT路由器具有N个全球IP地址，那么至多只能有N个内网主机能够同时和因特网上的主机通信。


| 内网地址 | 外网地址 |
|---|---|
| 192.168.0.2 | 172.38.1.5 |
| 192.168.0.3 | 172.38.1.6 |
| ⋮ | ⋮ |

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)

由于绝大多数的网络应用都是使用运输层协议TCP或UDP来传送数据，因此可以利用运输层的端口号和IP地址一起进行转换。

这样，用一个全球IP地址就可以使多个拥有本地地址的主机同时和因特网上的主机进行通信。这种将端口号和IP地址一起进行转换的技术叫作网络地址与端口号转换NAPT(Network Address and Port Translation)。


| NAPT转换表 | | | |
|---|---|---|---|
| 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 | 192.168.0.2：30000 | 172.38.1.5：40001 |
| 出 | 源IP地址：TCP源端口 | 192.168.0.3：30000 | 172.38.1.5：40002 |
| 入 | 目的IP地址：TCP目的端口 | 172.38.1.5：40001 | 192.168.0.2：30000 |
| 入 | 目的IP地址：TCP目的端口 | 172.38.1.5：40002 | 192.168.0.3：30000 |

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)


对于一些P2P网络应用，需要外网主机主动与内网主机进行通信，在通过NAT时会遇到问题，需要网络应用自己使用一些特殊的NAT穿越技术来解决问题。

## 4.9 虚拟专用网VPN与网络地址转换NAT

### 网络地址转换NAT(Network Address Translation)

对于一些P2P网络应用，需要外网主机主动与内网主机进行通信，在通过NAT时会遇到问题，需要网络应用自己使用一些特殊的NAT穿越技术来解决问题。

另外，由于NAT对外网屏蔽了内网主机的网络地址，能为内网的主机提供一定的安全保护。


# 4.9 虚拟专用网VPN与网络地址转换NAT

专用（私有）地址：
10.0.0.0~10.255.255.255(10/8地址块)
172.16.0.0~172.31.255.255(172.16/12地址块)
192.168.0.0~192.168.255.255(192.168/16地址块)

## 虚拟专用网VPN(Virtual Private Network)

- 利用公用的因特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。
- 同一机构内不同部门的内部网络所构成的虚拟专用网VPN又称为内联网VPN。
- VPN要保证传输数据的安全性，会将原始的内部数据报进行加密，然后再将其封装成为在因特网上发送到的外部数据报。
- 有时一个机构的VPN需要有某些外部机构（通常就是合作伙伴）参加进来。这样的VPN就称为外联网VPN。
- 在外地工作的员工需要访问公司内部的专用网络时，只要在任何地点接入到因特网，运行驻留在员工PC中的VPN软件，在员工的PC和公司的主机之间建立VPN隧道，即可访问专用网络中的资源。这种VPN称为远程接入VPN。

## 网络地址转换NAT(Network Address Translation)

- 由于IP地址的紧缺，一个机构能够申请到的IP地址数量往往远小于本机构所拥有的主机数量。因此，虚拟专用网中的各主机所分配的地址应该是本机构可自由分配的专用地址，而不是需要申请的、在因特网上使用的公有地址。
- 虽然因特网采用了无分类编址方式来减缓IP地址空间耗尽的速度，但由于因特网用户数目的激增，特别是大量小型办公室网络和家庭网络接入因特网的需求不断增加，IPv4地址空间即将面临耗尽的危险仍然没有被解除。
- 1994年提出了一种网络地址转换NAT的方法再次缓解了IP地址空间耗尽的问题。
- NAT能使大量使用内部专用地址的专用网络用户共享少量外部全球地址来访问因特网上的主机和资源。
- 由于绝大多数的网络应用都是使用运输层协议TCP或UDP来传送数据，因此可以利用运输层的端口号和IP地址一起进行转换。这样，就可用一个全球IP地址就可以使多个拥有本地地址的主机同时和因特网上的主机进行通信。这种将端口号和IP地址一起进行转换的技术叫作网络地址与端口号转换NAPT(Network Address and Port Translation)。
- 对于一些P2P网络应用，需要外网主机主动与内网主机进行通信，在通过NAT时会遇到问题，需要网络应用自己使用一些特殊的NAT穿越技术来解决问题。
- 由于NAT对外网屏蔽了内网主机的网络地址，能为内网的主机提供一定的安全保护。