



电子信息学院
School of Electronic and Information Engineering

《计算机通信与网络》报告



姓 名:	王旭
班 级:	22 通信 2 班
学 号:	2215404064
指导教师:	沈纲祥/李泳成

苏州大学电子信息学院

2024 年 12 月

NAT 技术在企业网中的应用

一、实验目的

- (1) IP 地址分配，交换机接入计算机
- (2) 路由协议实现网络内部通信
- (3) PAT 技术实现网络内外部通信

二、实验原理

NAT 技术允许专用局域网内部网络使用私有 IP 地址，当内部主机要与外部网络进行数据传输时，就将私有 IP 地址转换成合法的公用 IP 地址，从而实现内部网络对互联网的访问，通过互联网实现与外部主机的通信。NAT 技术通常被集成到路由器、防火墙或者单独的 NAT 设备中，以具有 NAT 功能的路由器为例，NAT 技术的工作原理如图 1 所示。

RFC 1918 指明了三个私有 IP 地址块，分别是 10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16，这些地址只能分配给局域网内部节点，但允许不同局域网使用相同的私有 IP 地址，因此，可以大大节约宝贵的 IP 地址资源。此外，NAT 技术还可以实现多台计算机共享互联网连接，即只申请一个合法公用 IP 地址，就把整个专用局域网中的计算机接入互联网中，这一功能也很好地解决了 IP 地址紧缺的问题。

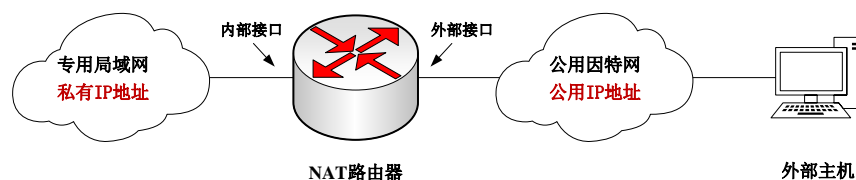


图 1 NAT 技术工作原理

NAT 技术可通过静态转换、动态转换和端口多路复用三种方式实现，分别称为静态 NAT、动态 NAT 和网络地址与端口号转换（Network Address and Port Translation, NAPT）。

静态 NAT 是指一个局域网的私有 IP 地址对应于一个公用 IP 地址，具有一对一映射关系，是固定不变的。在静态 NAT 技术下，可以实现外部网络用户对局域网内部的某些特定终端的访问，例如，一般局域网中需要为外部用户提供服务的服务器的 IP 地址需要采用静态 NAT 转换，从而实现外部用户使用固定地址对服务器进行访问。

动态 NAT 在将局域网私有 IP 地址转换成公用 IP 地址时，对应的公用 IP 地址是随机

的。动态 NAT 将私有 IP 地址映射到一组公用 IP 地址池上，因此内部网络私有 IP 地址与公用 IP 地址具有多对一的映射关系，内部网络主机可以轮流使用公用 IP 地址，但公用 IP 地址池中 IP 地址数量限制了内部网络同时访问因特网的主机数量。

为克服传统 NAT 技术访问因特网主机数量受到公用 IP 地址数量的限制,NAPT 将 NAT 的 IP 地址转换进一步扩展到“IP 地址+端口号”的形式转换，采用传输层 TCP/UDP 的端口多路复用方式，能够实现多个私有 IP 地址到一个公用 IP 地址的映射，即将内部网络多个不同的源 IP 地址都转换成同样的公用 IP 地址，但转换到该公用 IP 地址的不同端口号上。因此，NAPT 技术可以实现多个内部网络主机共用一个公用 IP 地址，并同时与互联网上的不同主机进行通信，从而实现最大限度地节约 IP 地址资源。此外，NAPT 技术可将内部网络所有主机有效隐藏在一个公用 IP 地址后面，避免来自外部网络的攻击。因此，NAPT 能够节省网络建设和接入费用，是网络应用非常广泛的一种方式。

表 1 NAT 技术实现方式优缺点对比

特性	静态 NAT	动态 NAT	NAPT
优点	稳定性高，适合固定服务	节省 IP，灵活性好	极大节省 IP，提高安全性
缺点	IP 浪费，配置不灵活	安全性较低，连接可能不稳定	配置复杂，可能影响性能

三、实验环境

本实验基于思科模拟器（Cisco Packet Tracer），Cisco Packet Tracer 是一款功能强大且易于使用的网络模拟软件，它以其直观的图形用户界面、丰富的网络设备库和动态学习环境而受到广泛欢迎。这款软件不仅免费提供给教育机构和个人学习者，降低了学习网络技术的门槛，还支持各种复杂的网络协议和配置，如 VLAN、STP、VTP、RIP 和 OSPF 等。Packet Tracer 允许用户在安全的虚拟环境中进行实验和模拟，无需担心对真实网络造成损害，同时提供了跨平台兼容性，支持 Windows、Mac OS X 和 Linux 操作系统。此外，Cisco 定期更新软件，增加新的设备和功能，以保持与最新网络技术同步。Packet Tracer 还有一个活跃的用户社区，提供大量的教程和论坛讨论，帮助用户学习和解决问题。

四、实验过程与分析

实验要求

某小型企业的组网需求为：企业内部多个部门的主机规划在两个 C 类网段下，分别为 192.168.1.0/24 和 192.168.2.0/24，要求所有主机均能接入互联网，并能访问互联网的 web 服务器，但该企业只有一个连接到 ISP 的公用 IP 地址 202.196.32.1。为满足企业组网需求，规划了如图 2 所示的企业网络结构图。专用局域网即企业网内部按照三层网络结构进行设计，接入层主要负责将 PC 机等终端接入到网络，汇聚层主要设备是汇聚交换机，着重提供基于策略的连接，核心层主要利用路由器实现数据的高速转发，本网络核心层的路由器 Router0 具有 NAT 功能，能够实现私有 IP 地址和公用 IP 地址的转换。除专用局域网以外区域模拟互联网，主要由一台路由器和一台 Web 服务器组成。

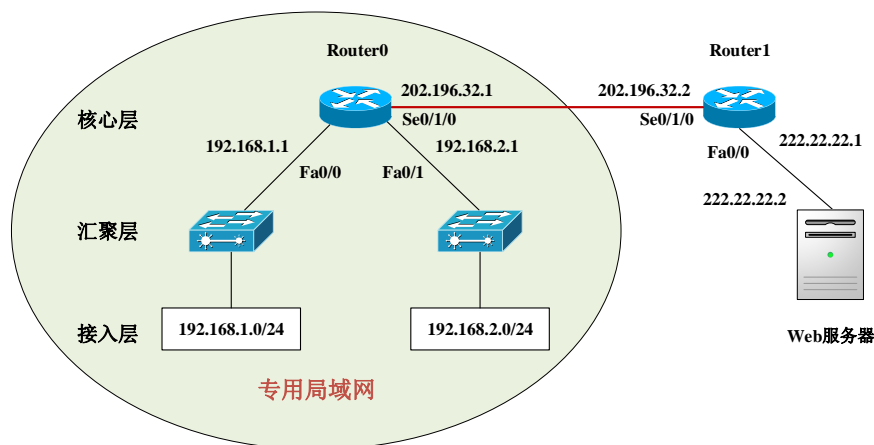


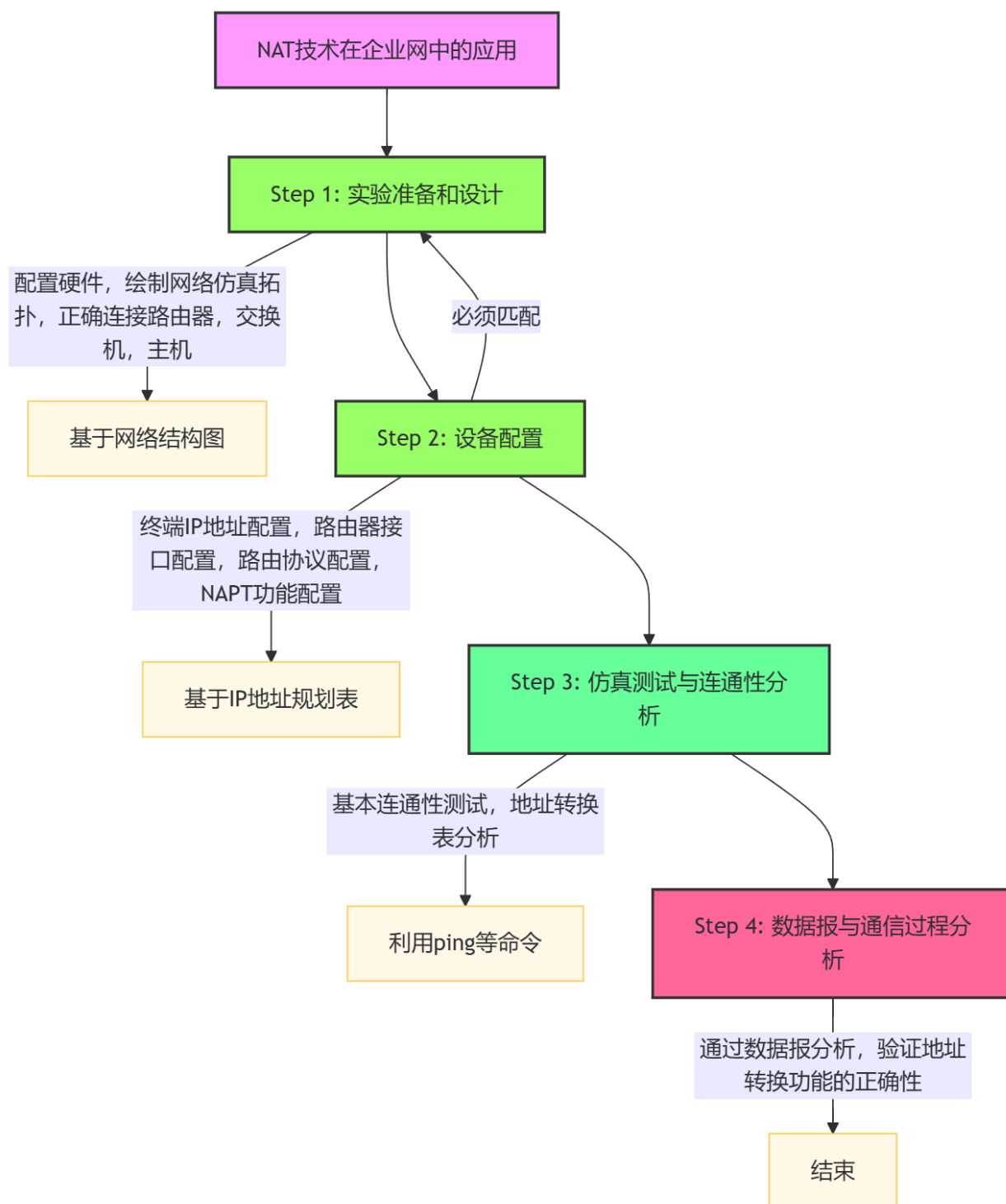
图 2 企业网络结构图

根据该企业对组网的要求，对各专用局域网内部网络、路由器各接口以及 Web 服务器进行 IP 地址规划，具体如表 2 所示。

表 2 IP 地址规划表

名称	接口	IP 地址	名称	接口	IP 地址
Router0	Fa0/0	192.168.1.1	Router1	Fa0/0	222.22.22.1
	Fa0/1	192.168.2.1		Se0/1/0	202.96.32.2
	Se0/1/0	202.96.32.1	内部网络 1	Fa	192.168.1.0/24
Web 服务器	Fa	222.22.22.2	内部网络 2	Fa	192.168.2.0/24

实验过程



为保证网络设计可行性, 根据图 2 所示的网络结构图和表 2 所示的 IP 地址规划表, 采用思科模拟器 Packet Tracer 仿真软件完成仿真设计和测试分析。某小型企业网络仿真设计图如图 3 所示, 由两个内部网络的若干台 PC 机、两台交换机、两台路由器和一台 Web 服务器组成。

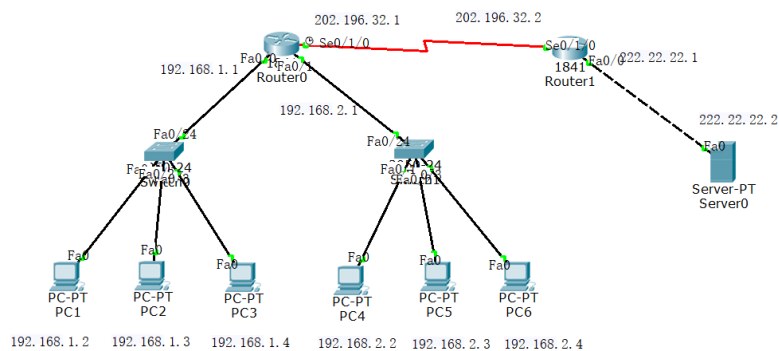


图 3 某小型企业网络仿真设计图

- (1) 参照企业网络结构图选取 PC 机、交换机、路由器和服务器，并进行线路连接，PC 机与交换机、交换机与路由器通过快速以太网口相连，使用直通双绞线；路由器在安装模块 WIC-2T 的情况下，即 2 端口串行广域网接口卡，路由器与路由器之间通过串口相连，使用串口线，路由器与服务器通过快速以太网口相连，使用交叉双绞线。仿真搭建结果如图 4 所示：

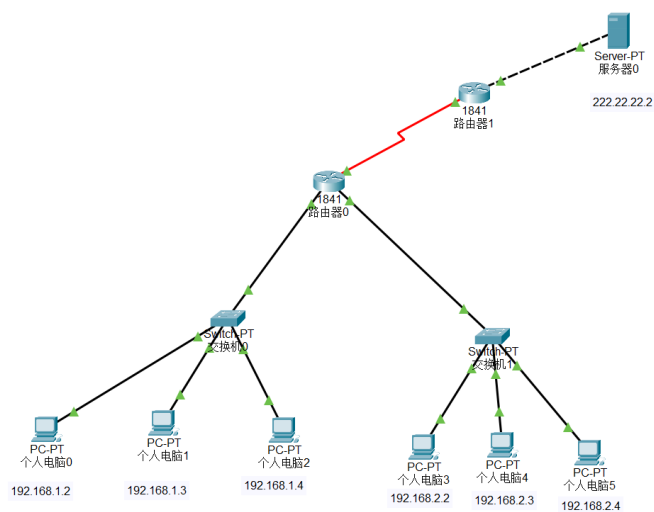


图 4 仿真设计图

- (2) 按照各部门 IP 地址规划表，为 PC 机设置 IP 地址、掩码和网关，网关设置为与该网络相连路由器快速以太网口配置的 IP 地址，例如内部网络 1 中的 PC1 的 IP 地址设置为 192.168.1.2，掩码设置默认的 255.255.255.0，即不划分子网，网关设置为 Router0 的快速以太网口 Fa0/0 配置的 IP 地址，即 192.168.1.1。

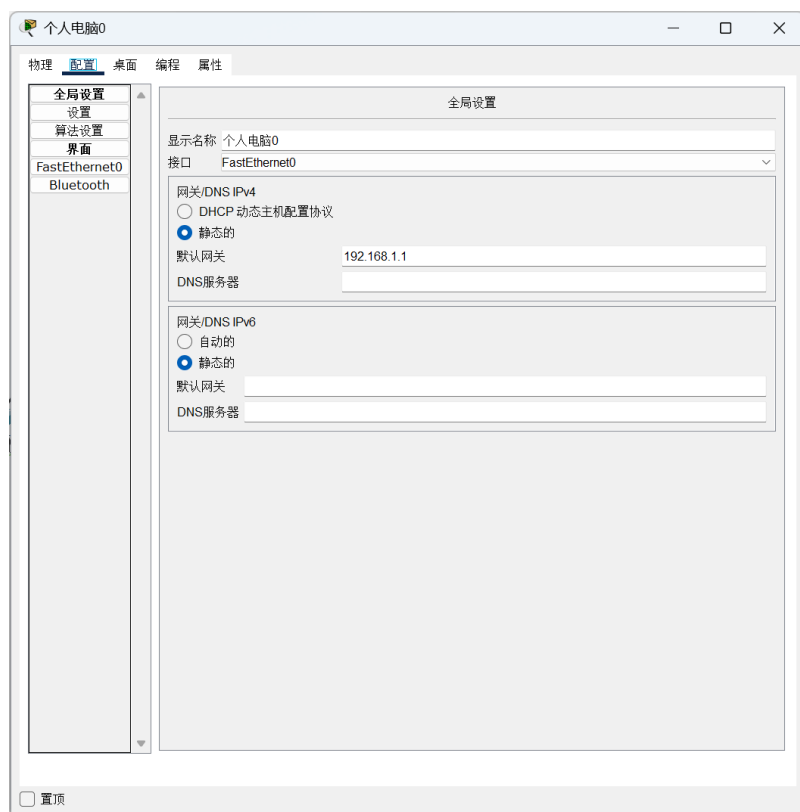


图 5 IP 配置图

(3) 按照路由器 IP 地址表对两台路由器端口 IP 地址进行配置，包括快速以太网端口、串口 IP 地址设置，具体如下。

a) 设置路由器 Router0 快速以太网端口 IP 地址：

```
Router0#conf t                //进入全局配置模式
Router0(config)#int fa0/0      //进入以太网端口 0
Router0(config-if)#ip add 192.168.1.1 255.255.255.0 //设置端口 IP 地址
Router0(config-if)#exit        //退出以太网端口 0 配置
Router0(config)#int fa0/1      //进入以太网端口 0
Router0(config-if)#ip add 192.168.2.1 255.255.255.0 //设置端口 IP 地址
```

b) 设置路由器 Router0 串口 se0/1/0 的 IP 地址：

```
Router0#conf t                //进入全局配置模式
Router0(config)#int se0/1/0    //进入串口 1
Router0(config-if)#ip add 202.196.32.1 255.255.255.0 //设置端口 IP 地址
```

c) 设置路由器 Router1 快速以太网端口 IP 地址：

```
Router1#conf t                //进入全局配置模式
Router1(config)#int fa0/0      //进入以太网端口 0
```

Router1(config-if)#ip add 222.22.22.1 255.255.255.0 //设置端口 IP 地址
Router1(config-if)#exit //退出以太网端口 0 配置

Router1(config)#int fa0/1 //进入以太网端口 0

Router1(config-if)#ip add 192.168.2.1 255.255.255.0 //设置端口 IP 地址

d) 设置路由器 Router1 串口 se0/1/0 的 IP 地址:

Router1#conf t //进入全局配置模式

Router1(config)#int se0/1/0 //进入串口 1

Router1(config-if)#ip add 202.196.32.2 255.255.255.0 //设置端口 IP 地址

(4) 配置两台路由器的路由协议，本设计采用路由信息协议（Routing Information Protocol, RIP）:

a) 对路由器 Router0 配置路由器协议 RIP:

Router0#conf t //进入全局配置模式

Router0(config)#router RIP //设置路由协议为 RIP

Router0(config-router)#version 2

Router0(config-router)#network 202.196.32.0 //连通网络 202.196.32.0/24

b) 对路由器 Router1 配置路由器协议 RIP:

Router1#conf t //进入全局配置模式

Router1(config)#router RIP //设置路由协议为 RIP

Router1(config-router)#version 2

Router1(config-router)#network 202.196.32.0 //连通网络 202.196.32.0/24

Router1(config-router)#network 222.22.22.0 //连通网络 222.22.22.0/24

(5) 配置 Router0 的 NAT 功能:

a) 对内部网络 1 的私有 IP 地址进行映射:

Router0(config)#access-list 1 permit 192.168.1.0 0.0.0.255

//定义访问控制列表 1，指定允许访问互联网的内部网络

Router0(config)#ip nat inside source list 1 int se 0/1/0 overload

//将访问控制列表 1 的 IP 地址通过串口 1 进行网络地址与端口号转换

Router0(config)#int fa 0/0 //进入以太网端口 0

Router0(config-if)#ip nat inside //设置为内部端口，连接内部网络

Router0(config-if)#exit //退出以太网端口 0 配置

Router0(config)#int se 0/1/0 //进入串口 0

Router0(config-if)#ip nat outside //设置为外部端口，连接外部网络

b) 对内部网络 2 的私有 IP 地址进行映射，代码含义类似于内部网络 1 的设置，此处不再赘述：

Router0(config)#access-list 2 permit 192.168.2.0 0.0.0.255

Router0(config)#ip nat inside source list 2 int se 0/1/0 overload

Router0(config)#int fa 0/1

Router0(config-if)#ip nat inside

Router0(config-if)#exit

Router0(config)#int se 0/1/0

Router0(config-if)#ip nat outside

五、实验连通性测试

1、连通性测试：

使用 ping 命令完成连通性测试，主要测试第（5）步 Router0 的 NAPT 功能配置前后的连通性。测试结果如下：

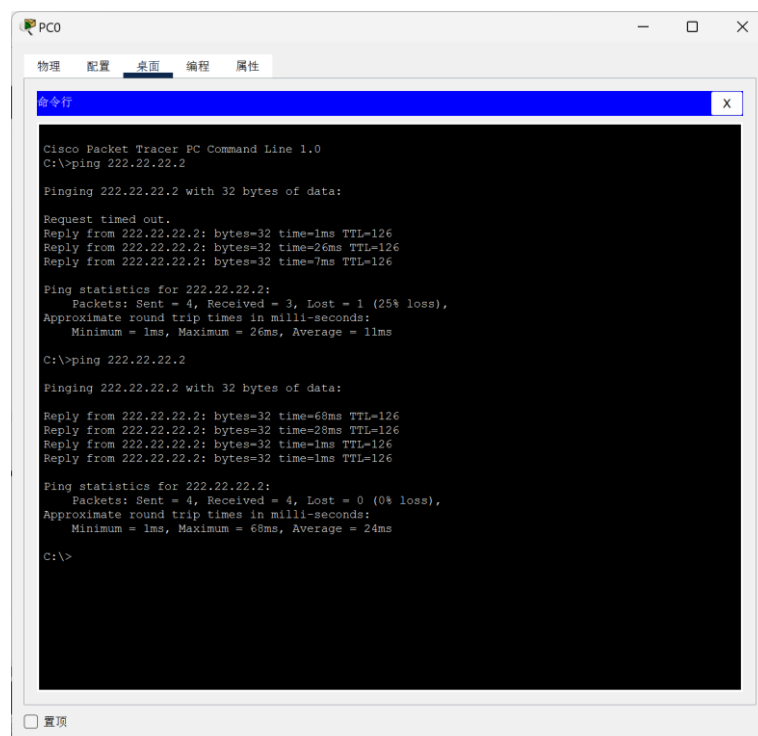


图 6 连通性测试

结果分析：

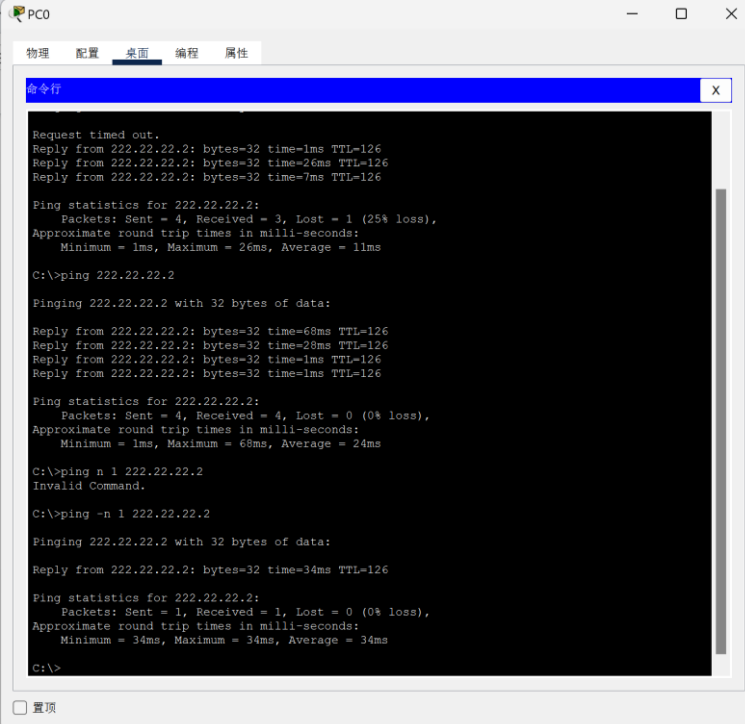
在启用 NAPT 功能之前，PC0 与外部服务器（IP 地址为 222.22.22.2）之间的通信存在

问题，表现为 25%的数据包丢失，部分请求因此超时。这种情况可能是因为私有 IP 地址没有被正确地转换成公网 IP 地址，导致连接问题。

启用 NAPT 功能之后，数据包丢失的问题得到了解决，丢包率降到了 0%，所有的数据包都能够顺利地到达目的地，而且网络的响应时间也有所减少，延迟变得更加一致。这表明 NAPT 功能成功地将内部网络中的私有 IP 地址映射到了可以与外部网络通信的公网 IP 地址，显著提高了网络的连通性和稳定性。

2、NAPT 地址转换表分析：

NAPT 地址转换表分析：首先，保证有数据包传输，实现 IP 地址转换，可以利用 Web 浏览器内部网络的每台 PC 机都完成对 Web 服务器的访问，即在地址栏输入 `http://222.22.22.2`；也可以用连通性测试的 `ping` 命令发送 ICMP 数据包，本文每台 PC 机利用命令“`ping -n 1 222.22.22.2`”实现发送一个数据包到 Web 服务器的操作。然后，在具有 NAPT 功能的路由器 Router0 中输入命令“`show ip nat translations`”，查看地址转换表，分析地址转换表中协议类型（Pro）、内部全局地址（Inside global）、内部本地地址（Inside local）、外部本地地址（Outside local）和外部全局地址（Outside global）等数据。



```
Request timed out.
Reply from 222.22.22.2: bytes=32 time=1ms TTL=126
Reply from 222.22.22.2: bytes=32 time=26ms TTL=126
Reply from 222.22.22.2: bytes=32 time=7ms TTL=126

Ping statistics for 222.22.22.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 26ms, Average = 11ms

C:\>ping 222.22.22.2

Pinging 222.22.22.2 with 32 bytes of data:

Reply from 222.22.22.2: bytes=32 time=68ms TTL=126
Reply from 222.22.22.2: bytes=32 time=28ms TTL=126
Reply from 222.22.22.2: bytes=32 time=1ms TTL=126
Reply from 222.22.22.2: bytes=32 time=1ms TTL=126

Ping statistics for 222.22.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 68ms, Average = 24ms

C:\>ping -n 1 222.22.22.2
Invalid Command.

C:\>ping -n 1 222.22.22.2

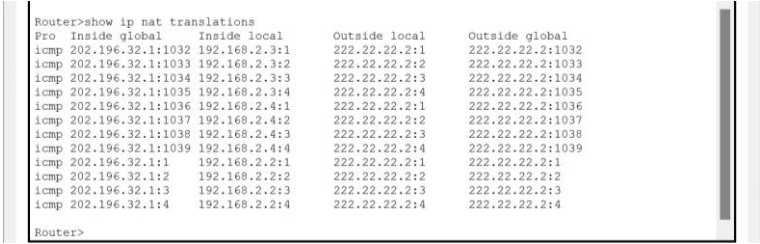
Pinging 222.22.22.2 with 32 bytes of data:

Reply from 222.22.22.2: bytes=32 time=34ms TTL=126

Ping statistics for 222.22.22.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 34ms, Average = 34ms

C:\>
```

图 7 ping-n 1 222.22.22.2 结果



Pro	Inside global	Inside local	Outside local	Outside global
icmp	202.196.32.1:1032	192.168.2.3:1	222.22.22.2:1	222.22.22.2:1032
icmp	202.196.32.1:1033	192.168.2.3:2	222.22.22.2:2	222.22.22.2:1033
icmp	202.196.32.1:1034	192.168.2.3:3	222.22.22.2:3	222.22.22.2:1034
icmp	202.196.32.1:1035	192.168.2.3:4	222.22.22.2:4	222.22.22.2:1035
icmp	202.196.32.1:1036	192.168.2.4:1	222.22.22.2:1	222.22.22.2:1036
icmp	202.196.32.1:1037	192.168.2.4:2	222.22.22.2:2	222.22.22.2:1037
icmp	202.196.32.1:1038	192.168.2.4:3	222.22.22.2:3	222.22.22.2:1038
icmp	202.196.32.1:1039	192.168.2.4:4	222.22.22.2:4	222.22.22.2:1039
icmp	202.196.32.1:1	192.168.2.2:1	222.22.22.2:1	222.22.22.2:1
icmp	202.196.32.1:2	192.168.2.2:2	222.22.22.2:2	222.22.22.2:2
icmp	202.196.32.1:3	192.168.2.2:3	222.22.22.2:3	222.22.22.2:3
icmp	202.196.32.1:4	192.168.2.2:4	222.22.22.2:4	222.22.22.2:4

图 8 地址转换表结果

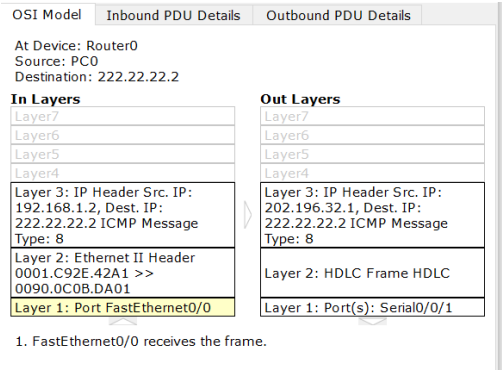
结果分析：

执行 Router0 上的 show ip nat translations 命令可以清楚地查看 NAT 功能的映射细节。地址转换表详细列出了私有 IP 与公网 IP 之间的对应关系，以及相关的协议、内部本地地址、内部全局地址和外部地址等信息。具体来说：多个内部私有 IP 地址（例如 192.168.2.2、192.168.2.3 等）被分配到同一个公网 IP 地址（如 202.196.32.1）的不同端口。每个映射条目都拥有一个独特的端口号，这确保了数据包能够被准确地送回到它们原始的发送设备。

这说明 NAT 通过结合“IP 地址+端口号”的映射策略，有效地实现了对私有 IP 地址的复用，解决了传统 NAT 中公网 IP 地址数量有限的问题。此外，这种机制还允许多个内部设备同时连接到外部网络，极大地提升了公网 IP 地址的使用效率。

3、数据报分析：

进一步在 PacketTracer 模拟模式下，模拟 PC 机与 Web 服务器的通信过程，进而通过数据报分析观察地址转换的具体过程。如图 9 所示。



OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: Router0

Source: PC0

Destination: 222.22.22.2

In Layers

Out Layers

Layer 7

Layer 6

Layer 5

Layer 4

Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 222.22.22.2 ICMP Message Type: 8

Layer 2: Ethernet II Header 0001.C92E.42A1 >> 0090.0C0B.DA01

Layer 1: Port FastEthernet0/0

Layer 7

Layer 6

Layer 5

Layer 4

Layer 3: IP Header Src. IP: 202.196.32.1, Dest. IP: 222.22.22.2 ICMP Message Type: 8

Layer 2: HDLC Frame HDLC

Layer 1: Port(s): Serial0/0/1

1. FastEthernet0/0 receives the frame.

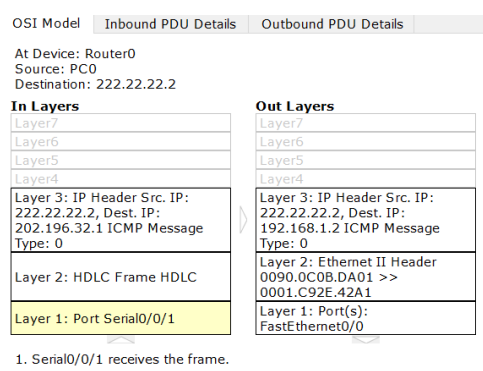


图 9 模拟通信

结果分析：

从图示中可以观察到，在数据传输过程中，地址发生了变化：发送时地址转换为公网 IP，接收时则变回 PC 的私有 IP。

在 Packet Tracer 的模拟环境中，通过观察数据包的源地址和目标地址的变化，我们可以验证 NAT 的具体操作流程：发送数据包时：原本的私有 IP 地址（如 192.168.2.x）会被替换成公网 IP 地址（例如 202.196.32.1），并且会附加一个独特的端口号，以保证在公网中的识别度。接收数据包时：公网 IP 地址和端口号会被转换回对应的私有 IP 地址，确保数据能够正确地送达目的地。

这种双向的地址转换不仅确保了通信的连续性和精确性，还保护了内部网络的 IP 地址不被外部直接识别，从而增强了网络安全。同时，这种机制也有效地减少了外部网络对内部设备直接发起攻击的可能性。

六、实验思考与总结

通过参与“NAT 技术在企业网中的应用”实验，我深刻理解了网络地址转换（NAT）的工作原理、实施方法以及它在企业网络中的应用价值。实验不仅提升了企业内部网络的通信效率，而且通过设置端口地址转换（PAT），巧妙地应对了公共 IP 地址资源的紧张状况，这凸显了网络技术在资源管理和成本节约方面的关键作用。

在实验过程中，我使用思科的 Packet Tracer 模拟器来构建网络模型并模拟数据传输，这让我对 NAT 的配置步骤有了更深入的认识，尤其是在 NAPT 模式下，如何利用端口复用来允许多个设备使用同一个 IP 地址。这种实践学习方式加深了我对 IP 地址分类、访问控制列表（ACL）以及路由协议（例如 RIP）的应用理解，并提高了我在网络设备配置和问题解决方面的技能。

通过分析实验数据，如连通性测试结果和地址转换表，我更加明白了 NAPT 技术如何增强网络的连通性和稳定性，同时在保护网络结构和提升安全性方面发挥着重要作用。这

次实验的成功，让我更加清楚地看到了计算机通信网络课程中的理论如何与实际应用相结合，并且激励我在未来的学术探索中，更加注重技术的实际应用和问题解决能力。