网 络 工 程
本 科 实 验 报 告

实验名称： NAT 配置

学 员 姓 名	程景愉	学 号	202302723005
培 养 类 型	无军籍	年 级	2023
专 业	网络工程	所 属 学 院	计算机学院
指 导 教 员	张军	职 称	工程师
实 验 室	306-707	实 验 时 间	2025.09.30

国防科技大学教育训练部制

《本科实验报告》填写说明

实验报告内容编排应符合以下要求：

（1）采用 A4（21cm×29.7cm）白色复印纸，单面黑字。上下左右各侧的页边距均为 3cm；缺省文档网格：字号为小 4 号，中文为宋体，英文和阿拉伯数字为 Times New Roman，每页 30 行，每行 36 字；页脚距边界为 2.5cm，页码置于页脚、居中，采用小 5 号阿拉伯数字从 1 开始连续编排，封面不编页码。

（2）报告正文最多可设四级标题，字体均为黑体，第一级标题字号为 4 号，其余各级标题为小 4 号；标题序号第一级用“一、”、“二、”……，第二级用“（一）”、“（二）”……，第三级用“1.”、“2.”……，第四级用“（1）”、“（2）”……，分别按序连续编排。

（3）正文插图、表格中的文字字号均为 5 号。

目录

图目录

1 实验目的

- 了解 NAT（网络地址转换）的基本概念及其在网络中的作用；
- 掌握 NAT 的三种主要类型：静态 NAT、动态 NAT 和 PAT（端口地址转换）；
- 理解 NAT 的工作原理，特别是 NAPT 和 NAT Server 的工作机制；
- 掌握在华为防火墙上配置 NAT 的步骤和方法，能够通过实际操作验证 NAT 的功能；
- 通过实验，加深对 NAT 在网络安全中的应用的理解。

2 实验原理

2.1 NAT 的概念

2.1.1 NAT 概述

网络地址转换（Network Address Translation, NAT）是一种将私有网络地址转换为公共网络地址的技术。NAT 技术是为了解决 IPv4 地址资源短缺问题而提出的，它通过将内部网络的私有地址转换为公共地址，实现内部网络与外部网络的通信。NAT 技术是一种在网络层对 IP 地址进行转换的技术，主要用于解决 IPv4 地址资源短缺问题。

随着网络应用的增多, IPv4 地址枯竭的问题越来越严重。尽管 IPv6 可以从根本上解决 IPv4 地址空间不足问题，但目前众多网络设备和网络应用大多是基于 IPv4 的，因此在 IPv6 广泛应用之前，使用一些过渡技术（如 CIDR、私网地址等）是解决这个问题的主要方式，NAT 就是这众多过渡技术中的一种。

当私网用户访问公网的报文到达网关设备后，如果网关设备上部署了 NAT 功能，设备会将收到的 IP 数据报文头中的 IP 地址转换为另一个 IP 地址，端口号转换为另一个端口号之后转发给公网。在这个过程中，设备可以用同一个公网地址来转换多个私网用户发过来的报文，并通过端口号来区分不同的私网用户，从而达到地址复用的目的。

早期的 NAT 是指 Basic NAT，Basic NAT 在技术上实现比较简单，只支持地址转换，不支持端口转换。因此，Basic NAT 只能解决私网主机访问公网问题，无法解决 IPv4 地址短缺问题。后期的 NAT 主要是指网络地址端口转换 NAPT（Network Address Port Translation），NAPT 既支持地址转换也支持端口转换，允许多台私网主机共享一个公网 IP 地址访问公网，因此 NAPT 才可以真正改善 IP 地址短缺问题。

2.1.2 NAT 主要功能

NAT 主要有如下几个功能：

1. IP 地址转换：将内部网络的私有地址转换为公共地址，实现内部网络与外部网络的通信。
2. 端口转换：将内部网络的私有端口转换为公共端口，实现多个内部主机共享一个公共 IP 地址。
3. 地址复用：多个内部主机共享一个公共 IP 地址，提高地址利用率。
4. 安全防护：NAT 可以隐藏内部网络的真实 IP 地址，提高网络安全性。
5. 减少 IPv4 地址的消耗：NAT 技术可以减少 IPv4 地址的消耗，延长 IPv4 地址的使用寿命。

2.2 NAT 的类型

NAT 技术主要有三种类型：静态 NAT、动态 NAT 和 PAT（端口地址转换）。静态 NAT 是一种将内部网络的私有地址转换为公共地址的技术，将内部网络的私有地址与公共地址一一对应，实现内部网络与外部网络的通信。动态 NAT 是一种将内部网络的私有地址转换为公共地址的技术，将内部网络的私有地址与公共地址动态对应，实现内部网络与外部网络的通信。PAT 是一种将内部网络的私有地址转换为公共地址的技术，将内部网络的私有地址与公共地址动态对应，同时还将端口号进行转换，实现内部网络与外部网络的通信。

2.2.1 SNAT（源 NAT）

源 NAT 在 NAT 转换时，仅对报文中的源地址进行转换，主要应用于私网用户访问公网的场景。当私网用户主机访问 Internet 时，私网用户主机发送的报文到达 NAT 设备后，设备通过源 NAT 技术将报文中的私网 IPv4 地址转换成公网 IPv4 地址，从而使私网用户可以正常访问 Internet。

根据转换时是否同时转换源端口号，源 NAT 可以细分为如下几种类型，详见 Figure 1 。

类别	描述	使用场景
NAT No-PAT	NAT No-PAT是一种只转换地址，不转换端口的NAT。NAT No-PAT可以实现私网地址到公网地址的一对一转换。	NAT No-PAT适用于上网用户较少且公网地址数与同时上网的用户数量相同的场景。
NAPT（PAT）	NAPT是一种同时转换地址和端口的NAT。NAPT使用一个地址池，地址池里有多个公网地址可供转换。NAPT可以实现多个私网地址到一个或多个公网地址的转换。	NAPT适用于公网地址数量少，但需要上网的私网用户数量大的场景。
Easy IP	Easy IP是一种特殊的NAPT，Easy IP使用出接口的公网IP地址作为NAT转换后的地址。	Easy IP适用于仅有一个公网IPv4地址的场景，或者需要固定使用出接口的公网IPv4地址上网的场景。

Figure 1: 源 NAT 分类

2.2.2 DNAT（目的 NAT）

目的 NAT 在 NAT 转换时，仅对报文中的目的地址和目的端口号进行转换，主要应用于公网用户访问私网服务的场景。当公网用户主机发送的报文到达 NAT 设备后，设备通过目的 NAT 技术将报文中的公网 IPv4 地址转换成私网 IPv4 地址，从而使公网用户可以使用公网地址访问私网服务。

根据转换前后的地址是否存在一种固定的映射关系，目的 NAT 可以细分为如下几种类型，详见 Figure 2 。

类别	描述	使用场景
静态目的NAT	静态目的NAT是一种转换报文目的IP地址的方式，转换前后的地址存在一种固定的映射关系。	通常情况下，出于安全的考虑，不允许外部网络主动访问内部网络。但是在某些情况下，还是希望能够为外部网络访问内部网络提供一种途径。例如，公司需要将内部网络中的资源提供给外部网络中的客户和出差员工访问，此时，可以使用静态目的NAT。
动态目的NAT	动态目的NAT是一种动态转换报文目的IP地址的方式，转换前后的地址不存在一种固定的映射关系。	通常情况下，静态目的NAT可以满足大部分目的地址转换的场景。但是在某些情况下，希望转换后的地址不固定。例如，移动终端通过转换目的地址访问无线网络，此时，可以使用动态目的NAT。
NAT Server	NAT Server是一种特殊的静态目的NAT，NAT Server将发往私网服务器的报文中的公网地址转换为与之对应的私网地址。	在一些特殊场景下，例如，学校或公司内会部署一些服务器对公网用户提供服务。由于这些服务器的地址一般都用私网地址，公网用户无法直接访问，此时，可以使用NAT Server技术，将服务器的私网地址映射成公网地址后供公网用户访问。

Figure 2: 目的 NAT 分类

2.2.3 双向 NAT

双向 NAT 指的是在转换过程中同时转换报文的源信息和目的信息。双向 NAT 不是一个单独的功能，而是源 NAT 和目的 NAT 的组合。双向 NAT 是针对同一条流，在其经过设备时同时转换报文的源地址和目的地址。双向 NAT 主要应用在同时有外网用户访问内部服务器和私网用户访问内部服务器的场景。

2.2.4 STUN 中定义的 NAT 类型

在 STUN 标准中，根据私网 IP 地址和端口到 NAT 出口的公网 IP 地址和端口的映射方式，把 NAT 分为如下四种类型，详见 Figure 3 。

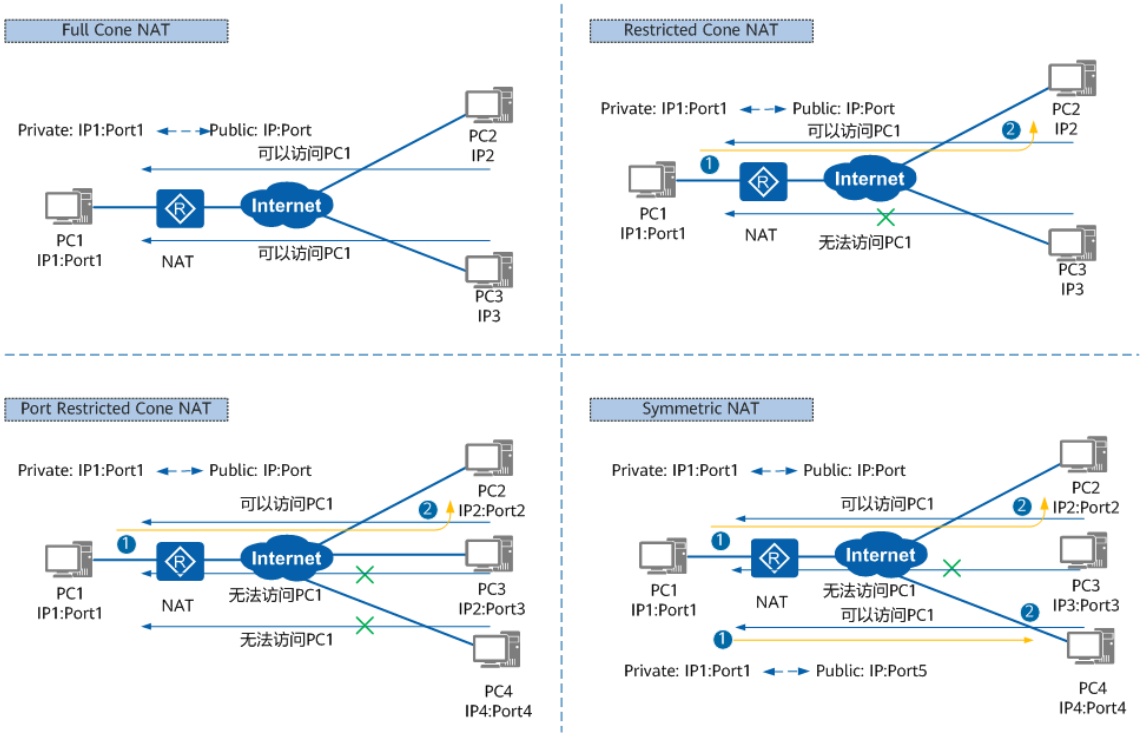

Figure 3: STUN 中定义的 NAT 类型

- Full Cone NAT（完全锥型 NAT）
- Restricted Cone NAT（限制锥型 NAT）
- Port Restricted Cone NAT（端口限制锥型 NAT）
- Symmetric NAT（对称 NAT）

2.3 NAT 的工作原理

根据前面的分类，我分别从源 NAT 和目的 NAT 中各选一种 NAT 为代表，介绍其工作原理。其他类型的 NAT 虽然在转换时，转换的内容有细微差别，但是工作原理都相似，不再重复介绍。此外，双向 NAT 是源 NAT 和目的 NAT 的组合，双向 NAT 的工作原理也不再重复介绍。

2.3.1 NAPT 工作原理

NAPT 在进行地址转换的同时还进行端口转换，可以实现多个私网用户共同使用一个公网 IP 地址上网。NAPT 根据端口来区分不同用户，真正做到了地址复用。

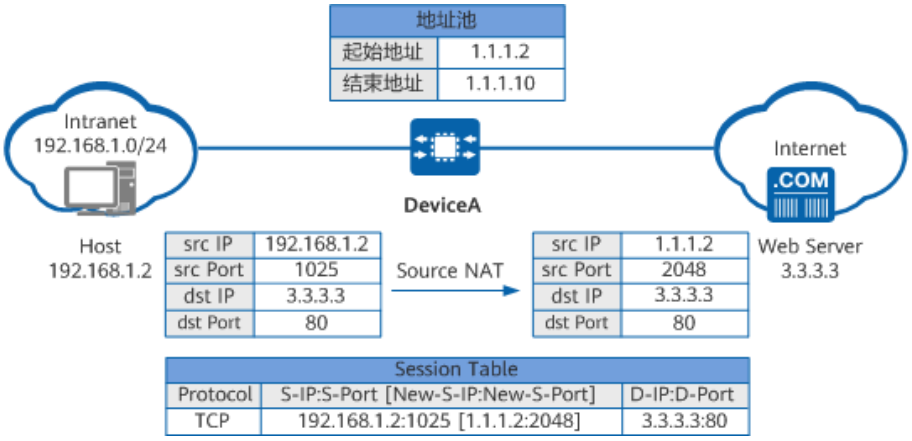

Figure 4: NAPT 工作原理示意图

当 Host 访问 Web Server 时，设备的处理过程如下：

1. 设备收到 Host 发送的报文后查找 NAT 策略，发现需要对报文进行地址转换。
2. 设备根据源 IP Hash 算法从 NAT 地址池中选择一个公网 IP 地址，替换报文的源 IP 地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至 Internet。
3. 设备收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的目的地址替换为 Host 的 IP 地址，将报文的目的端口号替换为原始的端口号，然后将报文发送至 Intranet。

2.3.2 NAT Server 工作原理

使用 NAT Server 时，需要先在设备上配置公网地址和私网地址的固定映射关系。配置完成后，设备将会生成 Server-Map 表项，存放公网地址和私网地址的映射关系。该表项将一直存在除非 NAT Server 的配置被删除。

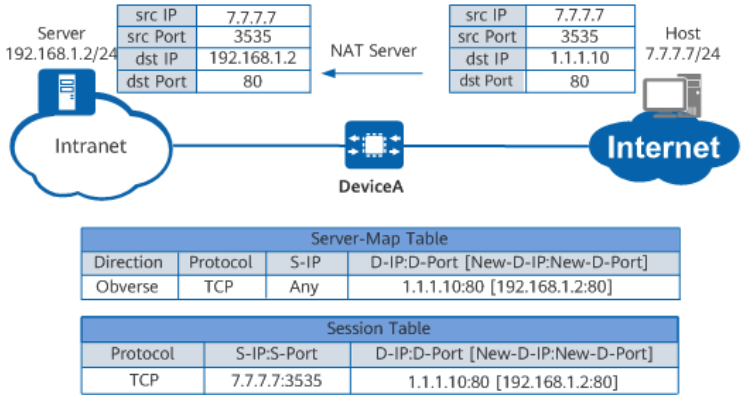

Figure 5: NAT Server 工作原理示意图

内部 Server 的私网 IPv4 地址为 192.168.1.2/24，对外的公网 IPv4 地址为 1.1.1.10，端口号都为 80，它们之间的映射关系在设备上已提前配置好。当 Host 访问 Server 时，设备的处理过程如下：

1. 设备收到 Internet 上用户访问 1.1.1.10 的报文的首包后，查找并匹配到 Server-Map 表项，将报文的目的 IP 地址转换为 192.168.1.2。
2. 设备建立会话表，然后将报文发送至 Intranet。
3. 设备收到 Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的源地址替换为 1.1.1.10，然后将报文发送至 Internet。

4. 后续 Host 继续发送给 Server 的报文，设备都会直接根据会话表项的记录对其进行转换，而不会再去查找 Server-map 表项。

2.4 NAT 的应用

上文已介绍过不同的 NAT 类型适用于不同的应用场景。下面介绍几种典型的 NAT 应用。

2.4.1 私网用户通过 NAPT 访问 Internet

在许多小区、学校和企业的私网规划中，由于公网地址资源有限，通常给私网用户分配私网 IPv4 地址。此时，可以配置源 NAT 来实现私网用户访问 Internet。用户可以根据自己拥有的公网 IPv4 地址的个数，选择使用 NAPT 或者 Easy IP。

当用户拥有的公网 IP 地址个数较多时，配置了 NAT 设备出接口的 IP 地址和其他应用之后，还有可用的空闲公网 IP 地址时，可以选择 NAPT。NAPT 使用地址池内的 IPv4 地址作为私网主机转换后的公网 IPv4 地址。如 Figure 6 所示，在设备上配置 NAPT，实现私网主机访问 Internet 功能。

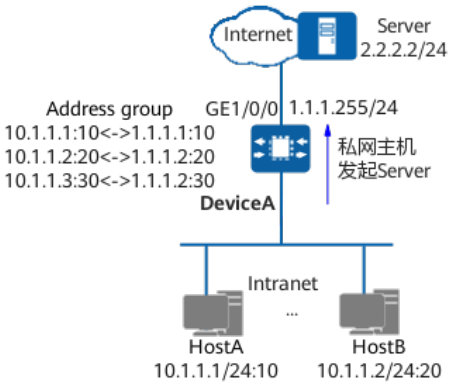

Figure 6: 私网用户通过 NAPT 访问 Internet

2.4.2 私网用户通过 Easy IP 访问 Internet

当用户拥有的公网 IPv4 地址个数较少时，配置了 NAT 设备出接口的 IPv4 地址和其他应用之后，没有可用的空闲公网 IPv4 地址时，可以选择 Easy IP。Easy IP 使用出接口的 IPv4 地址作为私网主机转换后的公网 IPv4 地址。如 Figure 7 所示，在设备上配置 Easy IP，实现私网主机访问 Internet 功能。

2.4.3 公网用户通过 NAT Server 访问私网服务器

在某些场合，私网中有一些服务器需要向公网用户提供服务，比如私网中部署的一些 Web 服务器、FTP 服务器等，NAT 支持这样的应用，此时可以配置 NAT Server 来实现公网用户访问私网服务器。如下图所示，在设备上配置 NAT Server，固定“公网 IP 地址＋端口号”与“私网 IP 地址＋端口号”间的映射关系，实现公网主机通过该映射关系访问私网服务器功能。

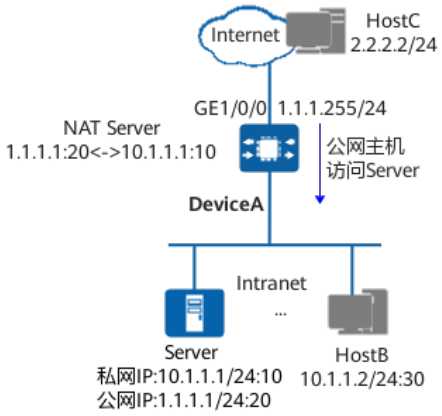

Figure 7: 公网用户通过 NAT Server 访问私网服务器

3 实验环境

3.1 实验背景

本实验在华为 USG6303E-AC 防火墙上进行，通过配置 NAT，实现私网用户访问公网的功能。实验中将介绍 NAT 的配置步骤和注意事项，并通过实际操作验证 NAT 的工作原理和效果。

3.2 实验设备

设备名称	设备型号	设备数量
防火墙	华为 USG6303E-AC	1
PC	联想启天 M410 Windows 10	3

另有网线若干。

4 实验步骤及结果

4.1 实验拓扑

按实验背景，绘制拓扑图如下：

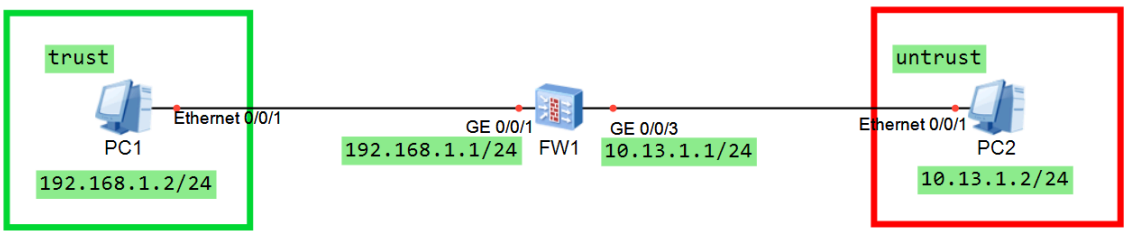

Figure 8: 实验拓扑图

4.2 按照拓扑图接线

按照拓扑图接线。

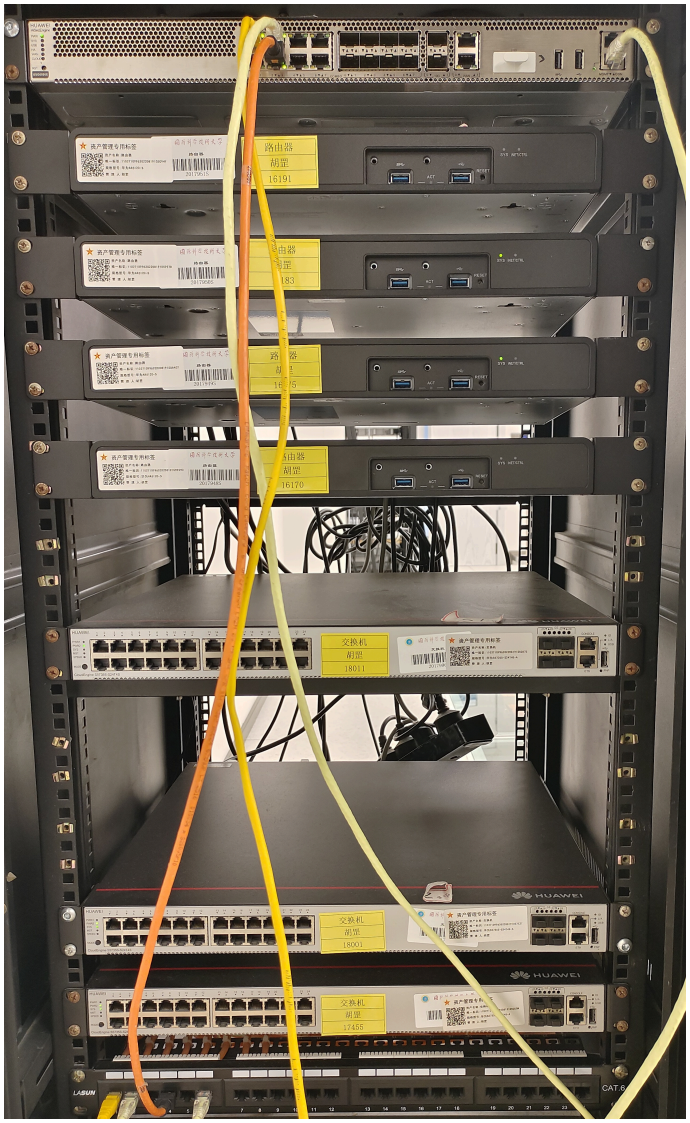

Figure 9: 机柜接线图

4.3 配置基本网络

4.3.1 配置 PC

- 配置 PC1 的 IP 地址为 `192.168.1.2/24`，网关为 `192.168.1.1`；
- 配置 PC2 的 IP 地址为 `10.13.1.2/24`，网关为 `10.13.1.1`；

步骤简单，展示图略。这样配置之后，PC1、PC2 分别属于 `trust`、`untrust` 区域；管理 PC 通过 MGMT 网口管理防火墙。

4.4 配置防火墙

4.4.1 配置接口

配置 `trust` 区域接口 `G0/0/1` 的 IP 地址为 `192.168.1.1/24`，区域为 `trust`；

Figure 10: trust 接口配置

配置 untrust 区域接口 G0/0/2 的 IP 地址为 10.13.1.2/24，区域为 untrust。

Figure 11: untrust 接口配置

4.4.2 配置安全策略

如 Figure 12 所示配置安全策略：允许 trust 区域的用户访问 untrust 区域的网络（图中 dmz 策略非本实验重点）。

Figure 12: 安全策略配置

4.4.3 配置 NAT

进入“策略”→“NAT 策略”界面，配置 NAT 策略，如 Figure 13 所示。

配置源 NAT，将 trust 区域的用户的私网 IP 地址转换为 untrust 区域的公网 IP 地址:

Figure 13: trust 访问外网源地址转换

4.5 验证 NAT 功能

配置完成后，PC1 访问外网，查看 NAT 策略表，如 Figure 14 所示:

Figure 14: NAT 转换表（ping 之前）

注意到图中的命中次数为 3。

下面在 PC1 上 ping 外网（PC2），如 Figure 15 所示，可以 ping 通。

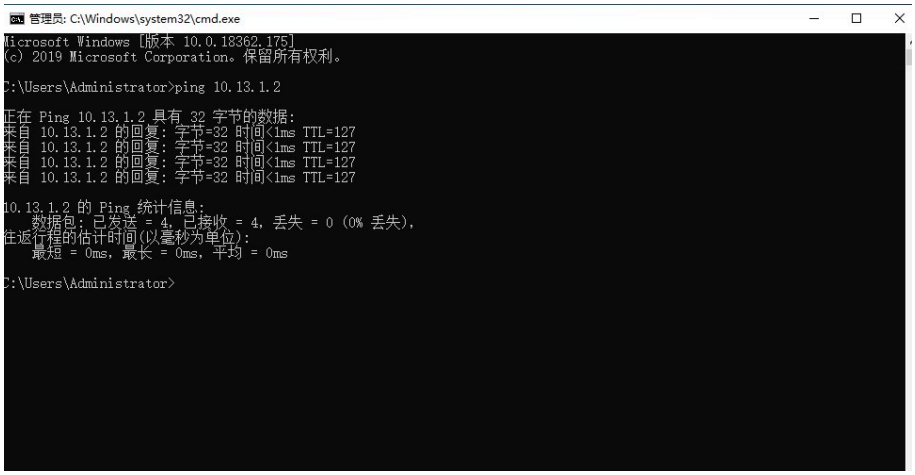

Figure 15: PC1 ping PC2

此时再次查看 NAT 策略表，如 Figure 16 所示:

Figure 16: NAT 转换表（ping 之后）

注意到图中的命中次数为 4，命中转换策略，说明 NAT 转换成功。

5 实验总结

本次实验通过在华为 USG6303E-AC 防火墙上配置 NAT，成功实现了私网用户访问公网的功能。通过实验，我深入了解了 NAT 的基本概念、类型及其工作原理。实验过程中配置了防火墙的接口、安全策略和 NAT 策略，并通过验证 NAT 功能，确认了 NAT 转换的成功。

实验的主要收获如下:

1. NAT 的基本概念：NAT 是一种将私有网络地址转换为公共网络地址的技术，主要用于解决 IPv4 地址资源短缺问题，同时也能提高网络的安全性。
2. NAT 的类型：我掌握了静态 NAT、动态 NAT 和 PAT 的区别及其适用场景，特别是 PAT（端口地址转换）在地址复用中的重要作用。
3. NAT 的工作原理：通过实验，我深入理解了 NAPT 和 NAT Server 的工作机制，特别是 NAPT 如何通过端口号区分不同用户，实现地址复用。
4. NAT 的配置：我学会了在华为防火墙上配置 NAT 的步骤，包括接口配置、安全策略配置和 NAT 策略配置，并通过实际操作验证了 NAT 的功能。
5. NAT 的应用：通过实验，我认识到 NAT 在网络安全和地址复用中的广泛应用，特别是在私网用户访问公网和公网用户访问私网服务器等场景中的重要作用。

实验过程中，我也遇到了一些挑战，例如在配置 NAT 策略时，需要确保安全策略的正确配置，否则会导致 NAT 转换失败。通过实验，我不仅加深了对 NAT 技术的理解，还提高了在实际网络环境中配置和调试 NAT 的能力。

总的来说, 本次实验达到了预期的目标, 帮助我更好地掌握了NAT技术及其在网络中的应用。未来, 我可以进一步探索NAT在复杂网络环境中的高级应用, 如双向NAT和NAT与VPN的结合等。

参考文献

[1] 华为技术支持. 什么是NAT?NAT的类型有哪些?- 华为[EB/OL]. 中国: 华为, 2024. https://info.support.huawei.com/info-finder/encyclopedia/zh/NAT.html.