**西安电子科技大学**

**组网与运维综合实验 课程实验报告**

**实验名称 配置NAT**

网络与信息安全 学院 2118021 班

成 绩

姓名 夏雨轩 学号 21009201006

同作者 无

实验日期 2023 年 11 月 30 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# 配置NAT

## 一、实验目的

1. 配置H3C路由器NAT功能，实现一对一静态NAT；

2. 熟悉NAT查看、监测和调试的相关命令；

3. 配置H3C路由器动态NAT的Basic NAT方式；

4. 配置H3C路由器动态NAT的NAPT方式；

5. 配置H3C路由器动态NAT的EASY IP方式；

6. 配置H3C路由器作为内部服务器；

7. 熟练使用FTP命令进行文件的上传和下载；

8. 熟悉FTP服务查看、监测和调试的相关命令。

## 二、实验要求

1. 1台具有24个以太网接口的路由器；

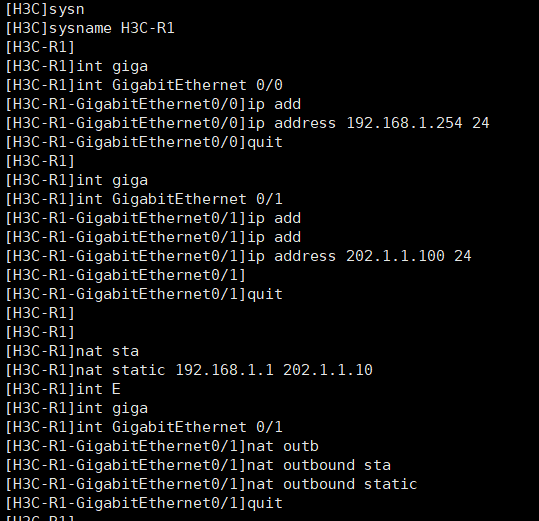
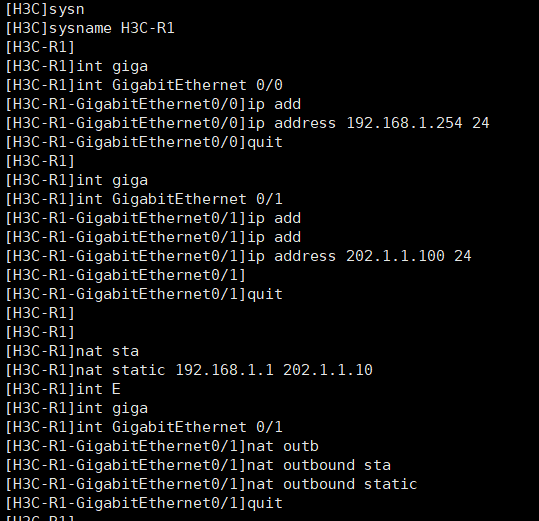
2. 2台装有Windows系列操作系统的PC（台式机或笔记本）；

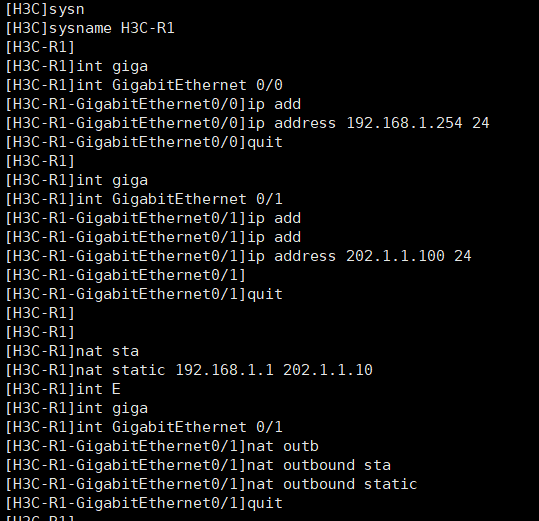
3. 2条双绞跳线（交叉线）；

## 三、实验步骤

1. 配置静态NAT

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）





nat static 192.168.1.1 202.1.1.10命令是配置静态NAT映射的命令，其含义如下：

192.168.1.1：指定私有IP地址，这是内部网络中的一个主机或设备的私有IP地址。

202.1.1.10：指定公共IP地址，这是为私有IP地址分配的公共IP地址。

此命令的目的是将内部网络中的192.168.1.1映射到公共网络中的202.1.1.10。在网络中，NAT用于将私有IP地址转换为公共IP地址，以便在互联网上进行通信。这种静态NAT映射是一对一的映射，意味着特定的私有IP地址将始终映射到相应的公共IP地址，不会动态变化。

nat outbound static是一个网络设备上用于配置静态NAT映射的命令。以下是这个命令的主要含义：

nat outbound static：表示配置一个静态NAT映射规则，用于处理从内部网络到外部网络的出站数据流。

Source：指定内部网络的源地址，即私有IP地址。这是要进行NAT处理的数据包的来源地址。

destination： 指定映射后的目标地址，即公共IP地址。这是指定内部网络中的源地址将映射到的外部网络的地址。

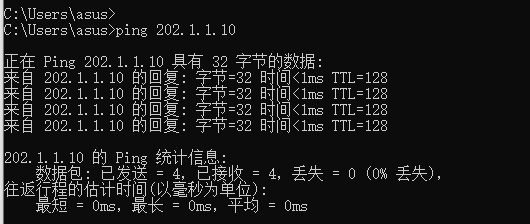
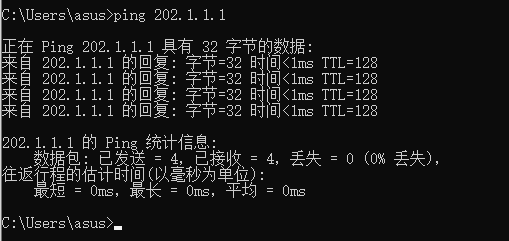
interface：指定出站数据流离开的接口。这是指定数据流离开网络的物理或逻辑接口。

mapping-type：指定映射类型，这里是静态映射。静态映射表示一对一的映射关系，其中一个特定的私有IP地址将被映射到相应的公共IP地址。这个映射是静态的，不会随时间或连接状态的变化而变化。

extendable：表示是否启用扩展，允许多个内部主机使用相同的公共IP地址进行出站通信。如果启用了扩展，多个内部主机可以共享一个公共IP地址。

2. 从PC上查看NAT是否成功

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）



发送ICMP报文： ping首先显示发送的ICMP报文的信息，通常包括报文大小、TTL（生存时间）等。

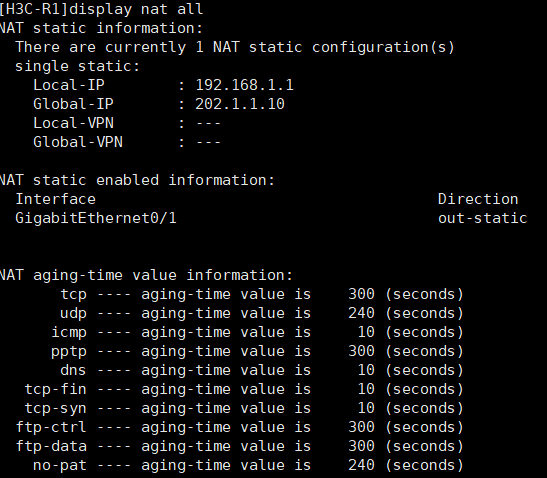
超时或响应信息：然后，ping命令会显示每个发送的ICMP报文是否收到响应。如果成功接收到目标主机的ICMP回显应答，通常显示回应时间（以毫秒为单位）。如果目标主机没有响应，通常显示超时消息。

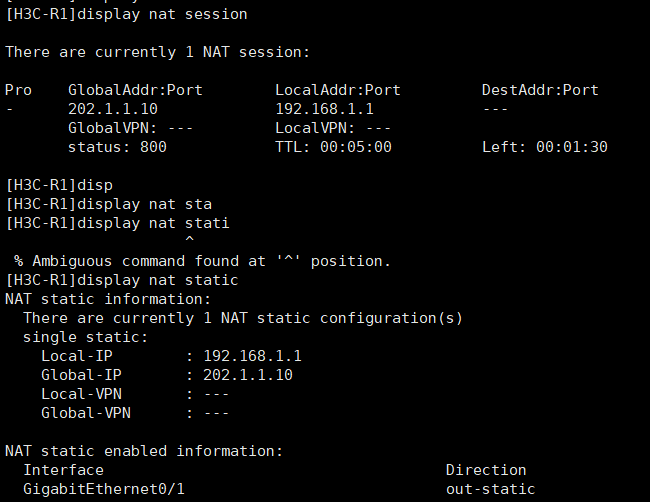
统计信息：在ping运行结束后，会显示有关传输的统计信息，例如发送的 ICMP 报文数量、接收到的 ICMP 回显应答数量、丢失的报文数量和往返时间的统计数据。

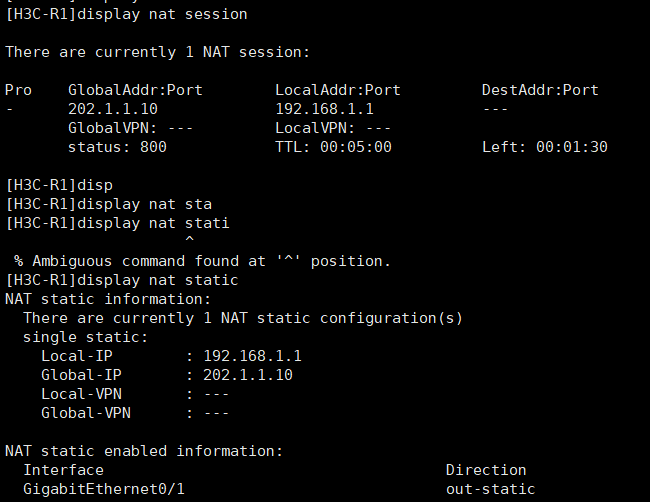
**从 Ping 的结果中可以看到，内网主机 PC1 已经能够成功访问外网主机 PC2: 外网主机PC2 同样能够成功访问内网主机 PC1。**

3. 在路由器上查看和调试NAT信息

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）







**display nat all：显示设备所有的 NAT 配置信息。**

**NAT static information:下面的输出表示 NAT 静态地址转换信息。也可以使用命令display nat static 得到类似的输出结果。**

输出表示存在1条 NAT静态地址转换关联信息。

single static: 表示一对一静态地址转换映射。

Local-IP:内网私有地址为 192.168.1.1。

Global-IP;外网公有地址为 202.1.1.10。

NAT static enabled information: 表示静态地址转换在 Ethernet0/1 接口的使能信息。

NAT aging-time value information: 表示各个协议的地址转换连接的有效时间信息。

**display nat session命令通常用于查看网络设备上当前的NAT会话信息。以下是一般情况下这个命令的主要含义：**

源地址（Source Address）：显示私有网络内部主机的原始IP地址。

源端口（Source Port）：显示内部主机使用的原始端口号。

目的地址（Destination Address）：显示外部目标服务器的IP地址。

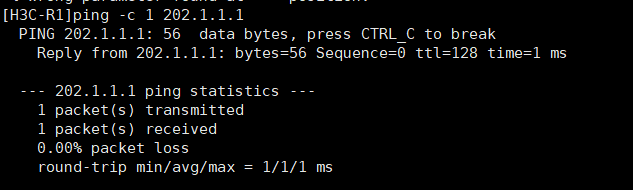
目的端口（Destination Port）：显示外部目标服务器的端口号。

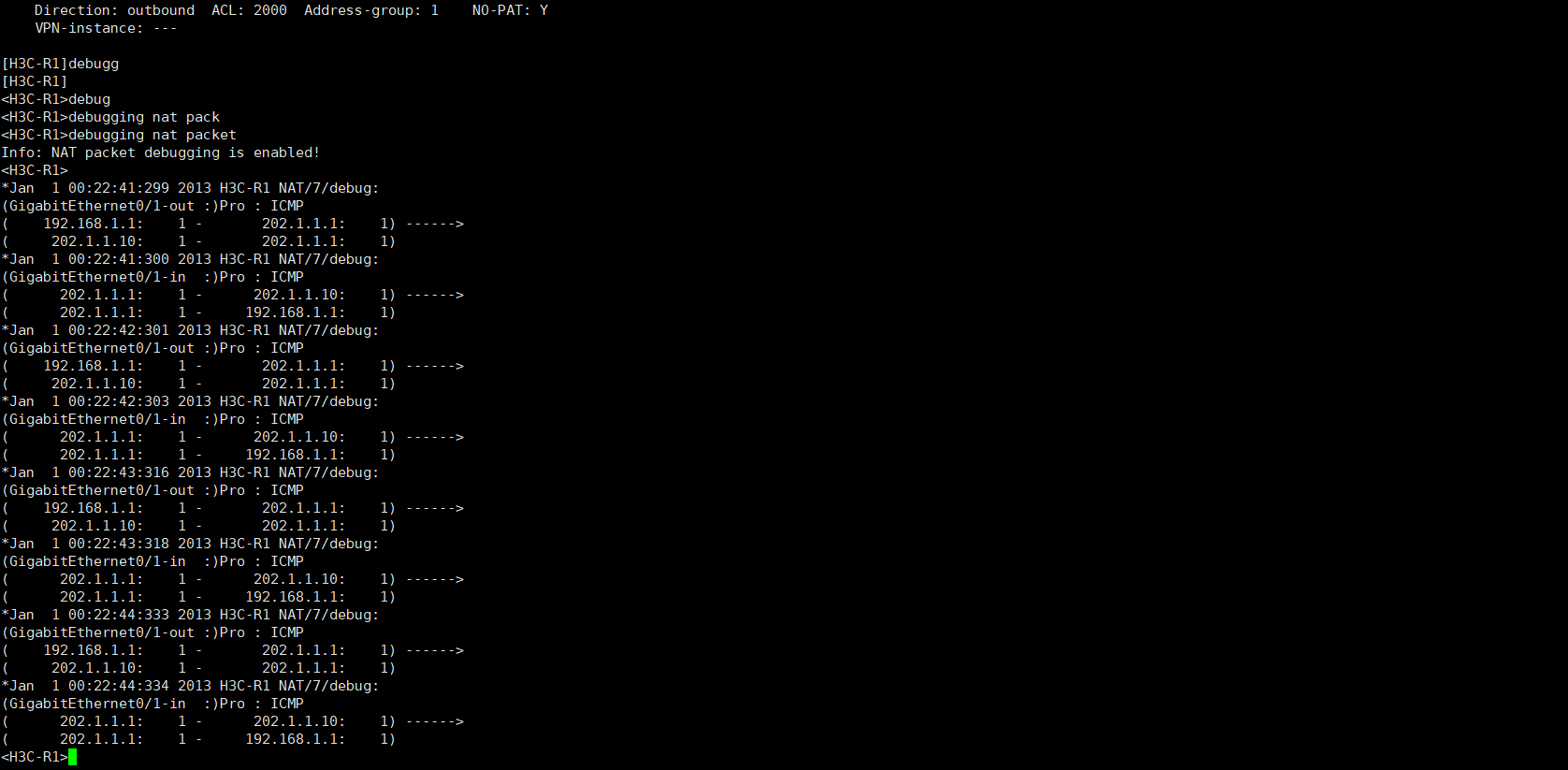
转换后的地址（Translated Address）：显示NAT后的公共IP地址。

转换后的端口（Translated Port）：显示NAT后的端口号。

协议（Protocol）：显示传输协议，如TCP或UDP。

状态（State）：显示NAT会话的当前状态，例如established（已建立）、unestablished（未建立）等。



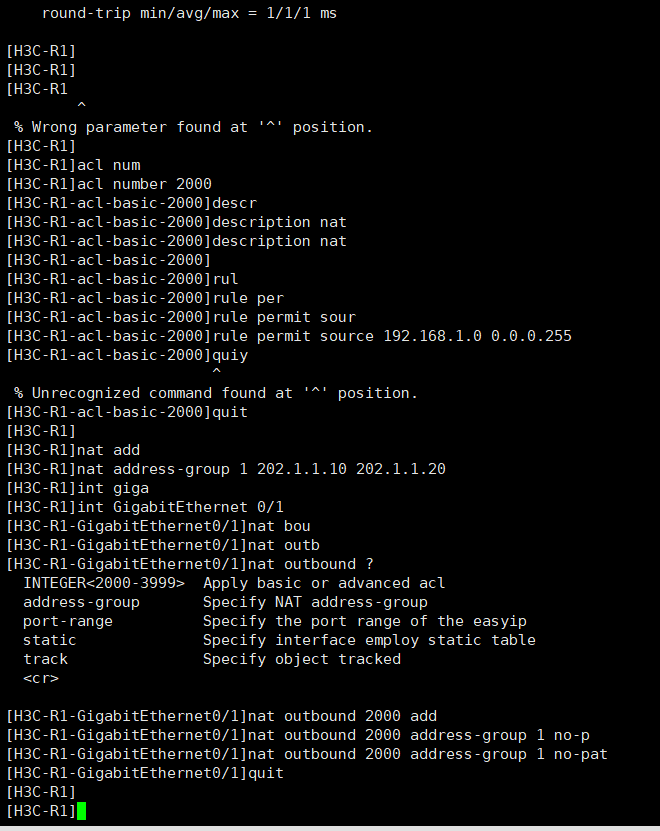


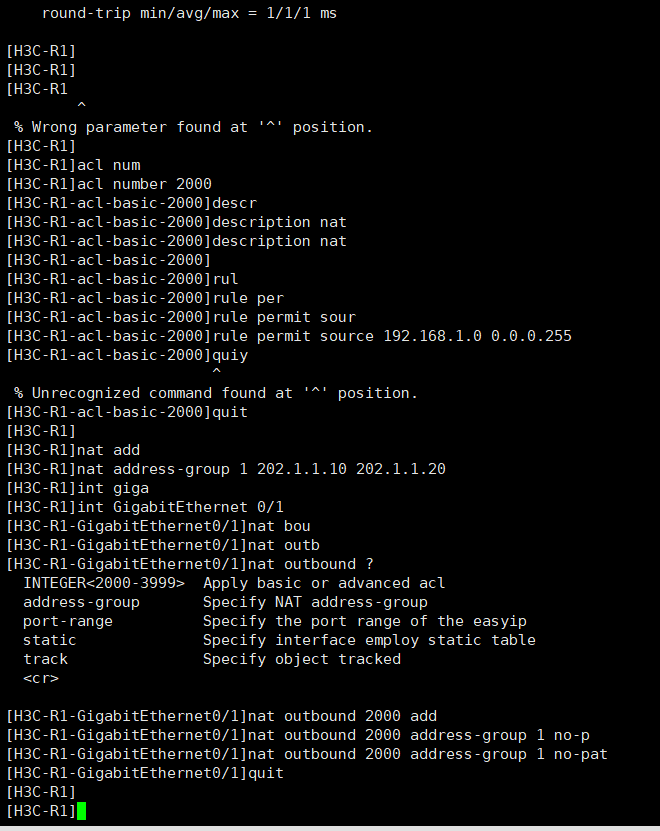
debugging nat packet 命令调试 NAT 报文在 H3C-R1 路由器的转换过程

可以看到从 PC1 上向 PC2 发送一个 Ping 报文。因为 Pro 字段显示ICMP，所以输出的192.168.1.1:1中的1表示通过的报文是ICMP报文。当报文通过H3C-R1路由器的 Ethernet0/1该口的出方向进行地址转换时，通过查找NAT地址表,把PC1发出报文的源地址192.168.1.1转换成 202.1.1.10，继续通过 Ethernet0/1接口向外发。当Ethernet0/1口的入方向收到去往 202.1.1.10 的目的地址时，通过查找 NAT 地址表，把目的地址 202.1.1.10 转换成192.168.1.1 后继续进行后续的路由转发。

4. 配置Basic NAT

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）





acl number 2000 创建序列号为2000的ipv4 acl，并进入相应视图。通常用于配置ACL（Access Control List）规则，其中number是ACL规则的编号。通过此命令，可以配置ACL规则，定义允许或禁止特定IP地址、协议、端口等特征的数据包通过网络设备。ACL规则通常用于网络安全和流量控制。

description nat 该命令的目的是为了提供对特定配置项的注释或说明。在description后面添加的nat被视为对nat的描述信息。

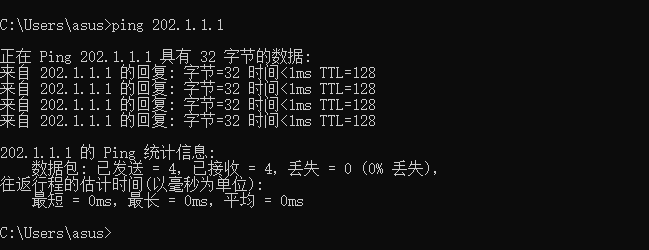
rule permit source 192.168.1.0 0.0.0.255 允许192.168.1.0网段的主机发送tcp报文，同时允许源地址为 192.168.1.0 到 192.168.1.255 范围内的所有IP地址的流量通过。

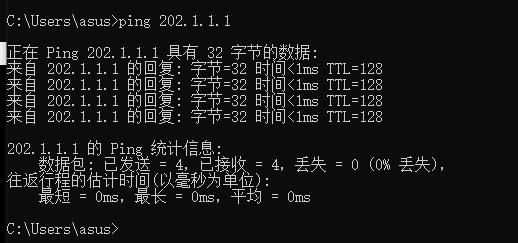
nat address-group 1 202.1.1.10 202.1.1.20 定义一个地址池，地址池索引号为1，地址池的开始IP地址为202.1.1.10，地址池的结束IP地址为202.1.1.20。NAT 地址组常常用于配置地址池，这些地址池用于将内部私有地址转换为公共地址。在这个指令中，地址组编号为1，包含了一个地址范围，可能被用作 NAT 转换的目标地址。当内部主机发送流量经过 NAT 设备时，其私有地址会被映射为地址组中的一个公共地址。

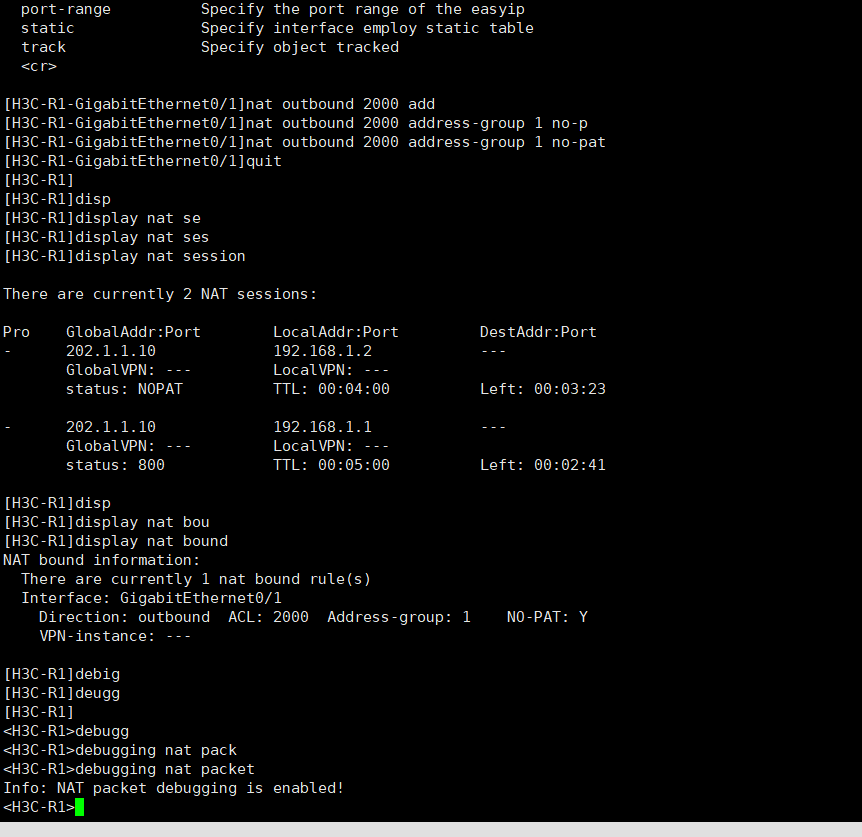
nat outbound 2000 address-group 1 no-pat 在出接口配置访问控制列表和地址池关联，不使用端口信息，实现NO-PAT功能。

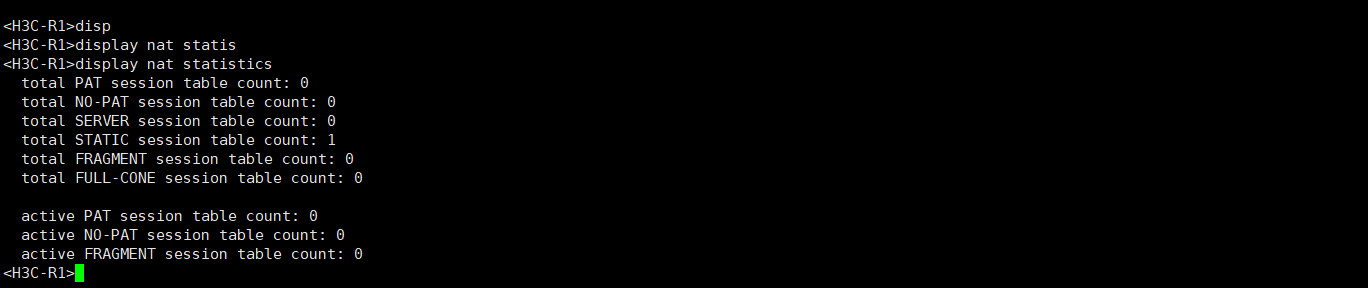
5. 查看Basic NAT输出及调试信息

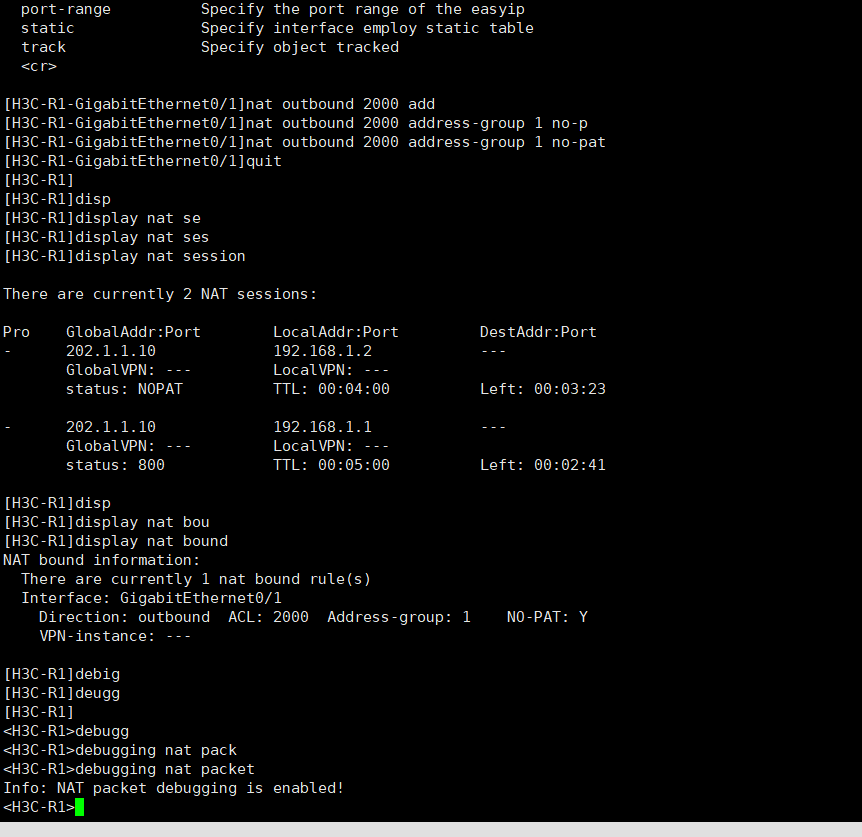
（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）











**display nat session命令通常用于查看网络设备上当前的NAT会话信息。以下是一般情况下这个命令的主要含义：**

源地址（Source Address）：显示私有网络内部主机的原始IP地址。

源端口（Source Port）：显示内部主机使用的原始端口号。

目的地址（Destination Address）：显示外部目标服务器的IP地址。

目的端口（Destination Port）：显示外部目标服务器的端口号。

转换后的地址（Translated Address）：显示NAT后的公共IP地址。

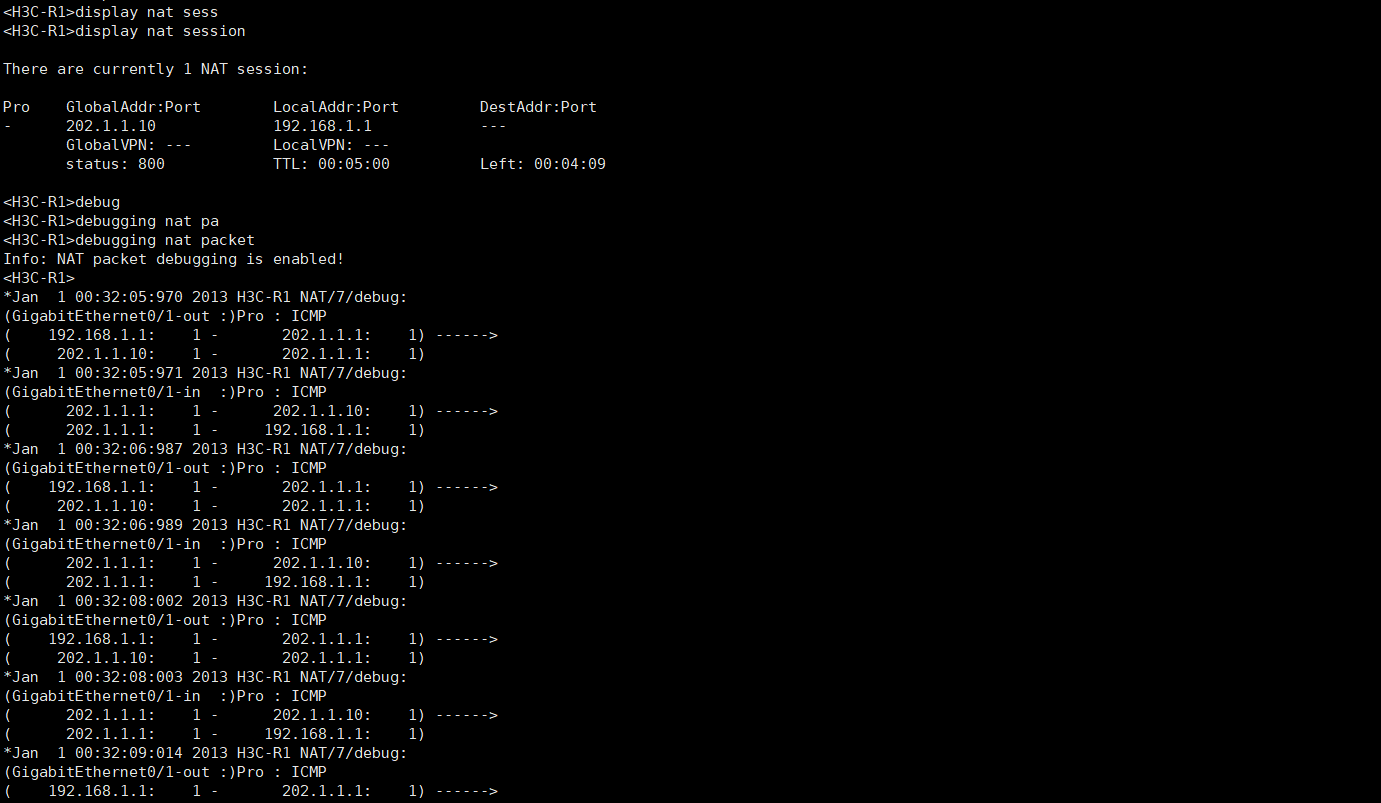
转换后的端口（Translated Port）：显示NAT后的端口号。

协议（Protocol）：显示传输协议，如TCP或UDP。

状态（State）：显示NAT会话的当前状态，例如established（已建立）、unestablished（未建立）等。

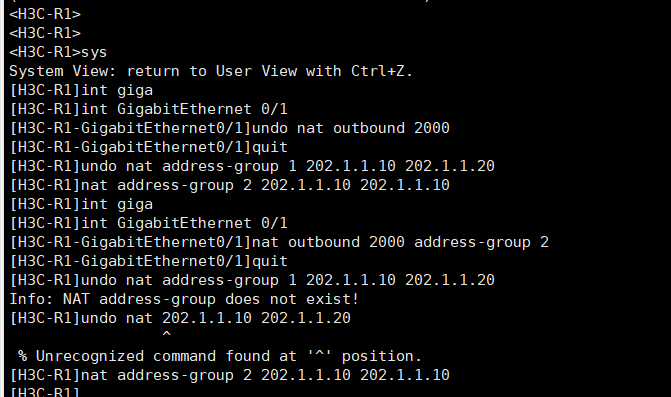
**display nat statistic :**通常用于查看 NAT的统计信息，包括有关 NAT 活动的一些关键信息。

display nat bound这个命令通常用于查看当前 NAT绑定表的内容。这个命令的输出通常包含了已建立的 NAT 绑定的详细信息。



6. 配置NAPT

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）



undo nat outbound 2000 address-group 1 no-pat 解除ACL和地址池的绑定关系。

undo: 撤销配置。

nat outbound 2000: 指定NAT出站方向的编号（这里是编号 2000）。

address-group 1: 取消与地址组1的关联。

no-pat: 取消 PAT配置，即取消对端口的转换。

这个命令的效果是取消与 ACL编号为 2000、关联了的地址组1并启用了 PAT的NAT配置。

undo nat address-group 1 202.1.1.10 202.1.1.20 命令删除配置的地址池。

undo: 撤销配置。

nat: 进入NAT配置模式。

address-group 1:指定地址组编号为 1。

202.1.1.10 202.1.1.20: 删除配置的地址池范围。

这个命令的效果是取消与地址组 1 相关的地址池范围的配置。

nat outbound 2000 address-group 2 在出接口配置访问控制列表和地址池关联，并使用TCP/UDP端口信息实现多对一地址转换。

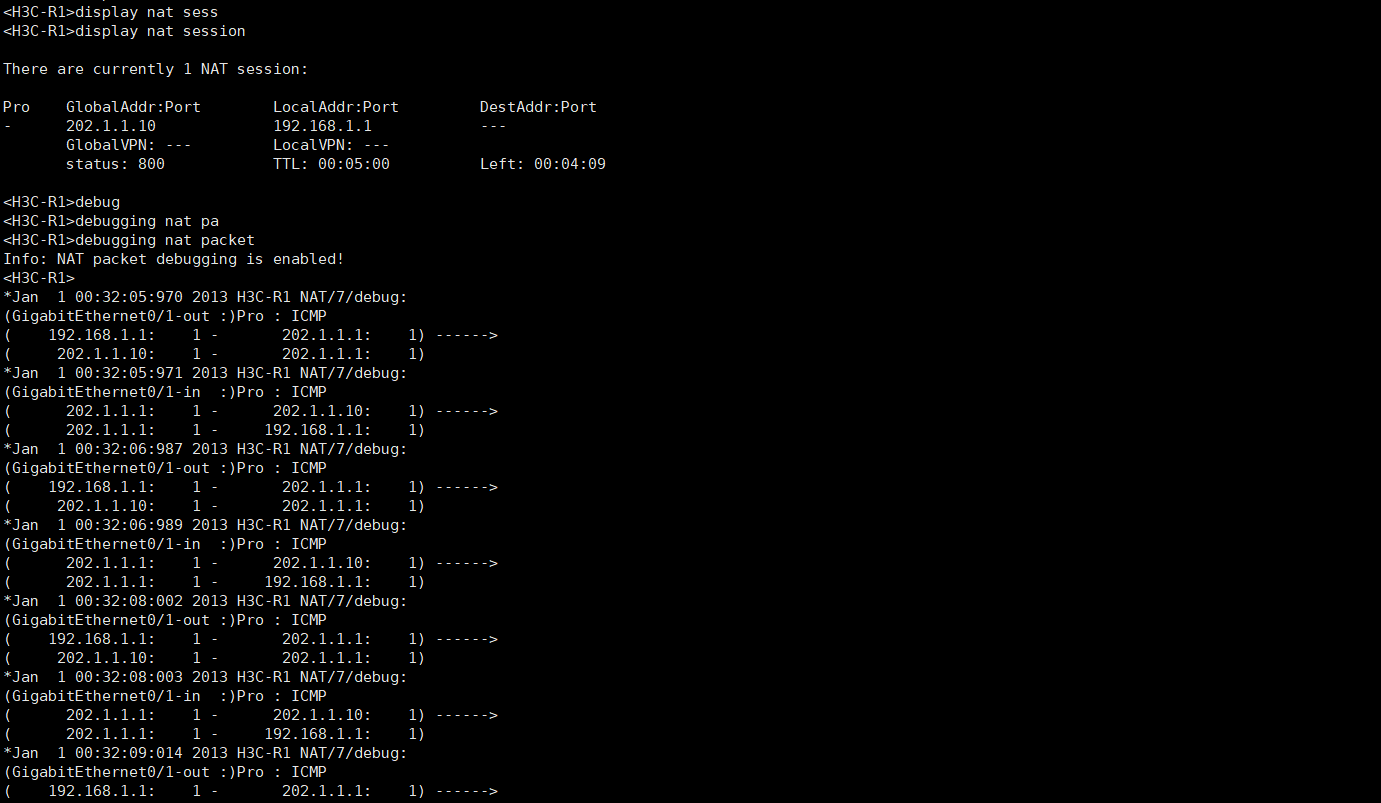
nat outbound 2000: 指定NAT出站方向的编号为 2000。

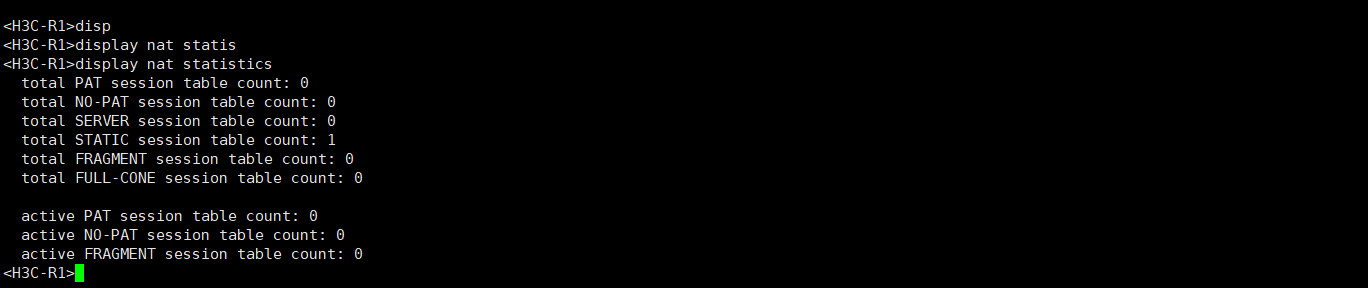
address-group 2: 关联地址组编号为 2。

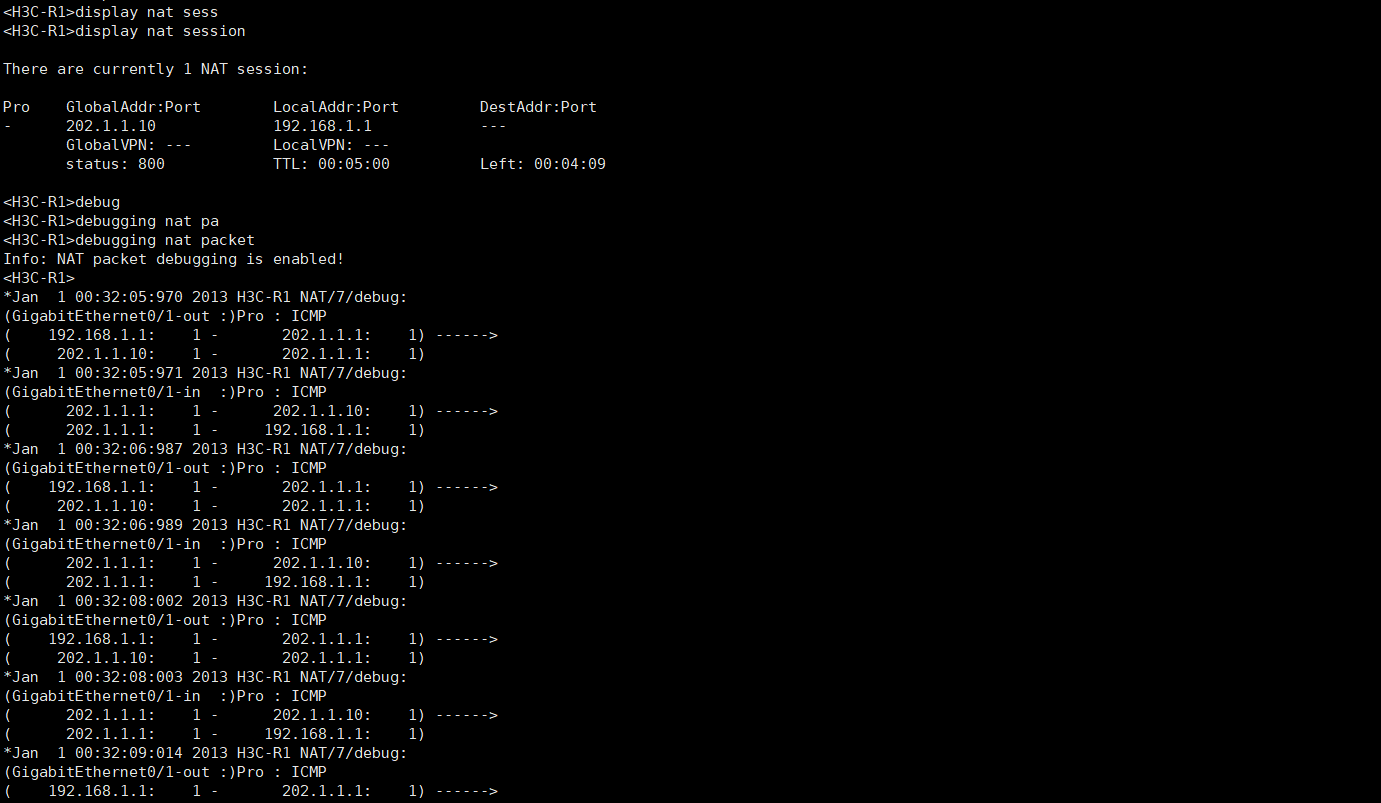
这个命令的效果是将NAT出站方向编号为 2000 的配置与地址组编号为 2 关联，进而实现多对一地址转换。

7. 查看NAPT输出及调试信息

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）







**display nat session命令通常用于查看网络设备上当前的NAT会话信息。以下是一般情况下这个命令的主要含义：**

源地址（Source Address）：显示私有网络内部主机的原始IP地址。

源端口（Source Port）：显示内部主机使用的原始端口号。

目的地址（Destination Address）：显示外部目标服务器的IP地址。

目的端口（Destination Port）：显示外部目标服务器的端口号。

转换后的地址（Translated Address）：显示NAT后的公共IP地址。

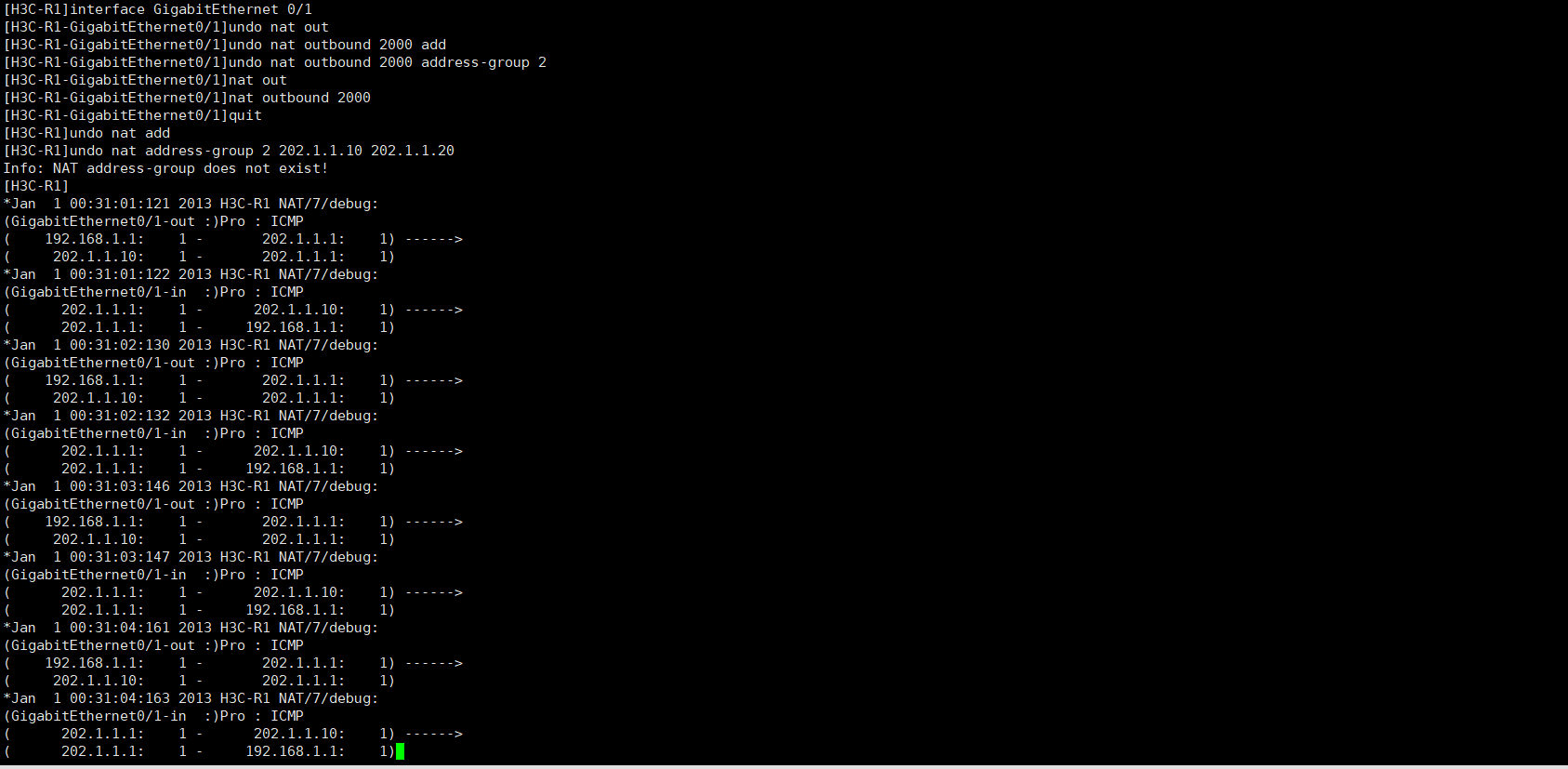
转换后的端口（Translated Port）：显示NAT后的端口号。

协议（Protocol）：显示传输协议，如TCP或UDP。

状态（State）：显示NAT会话的当前状态，例如established（已建立）、unestablished（未建立）等。

8. 配置Easy NAT

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）

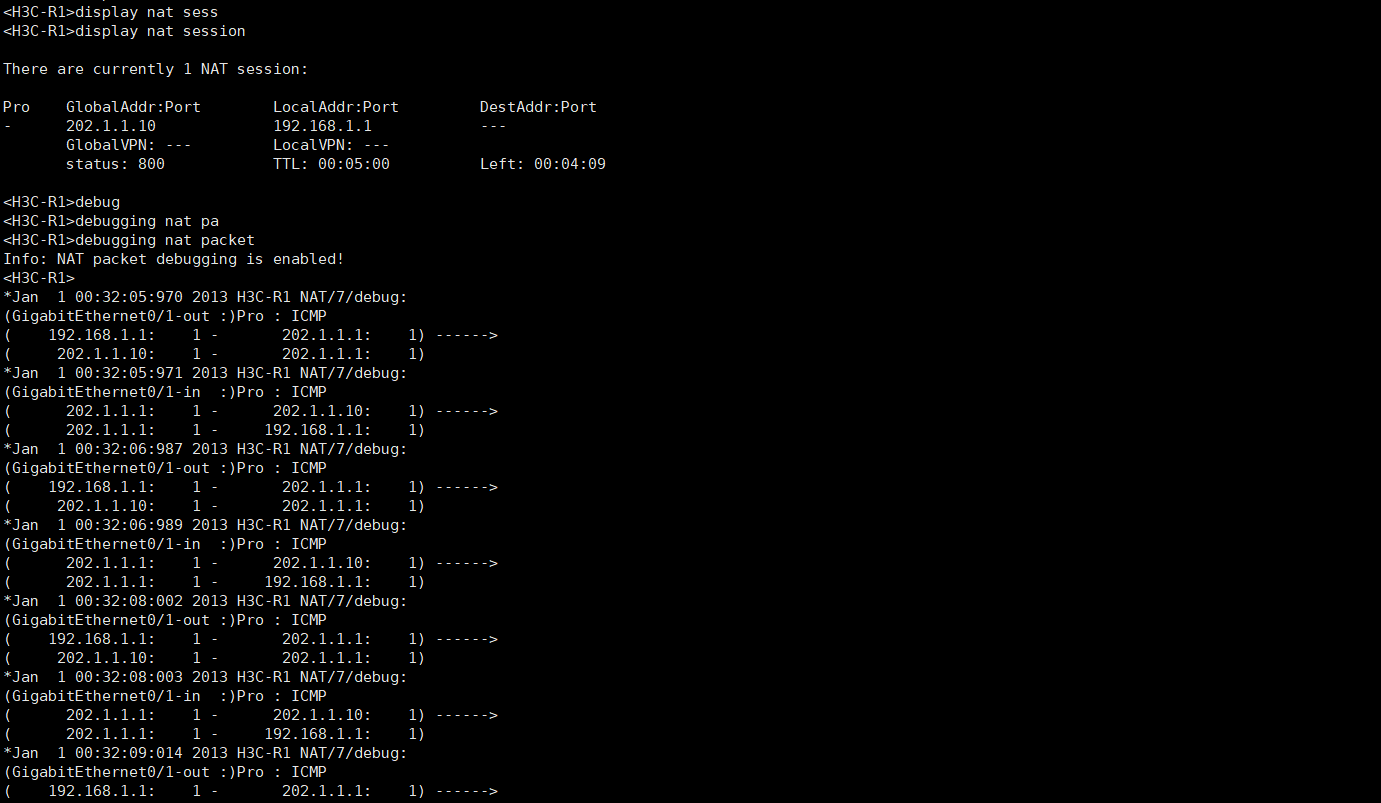


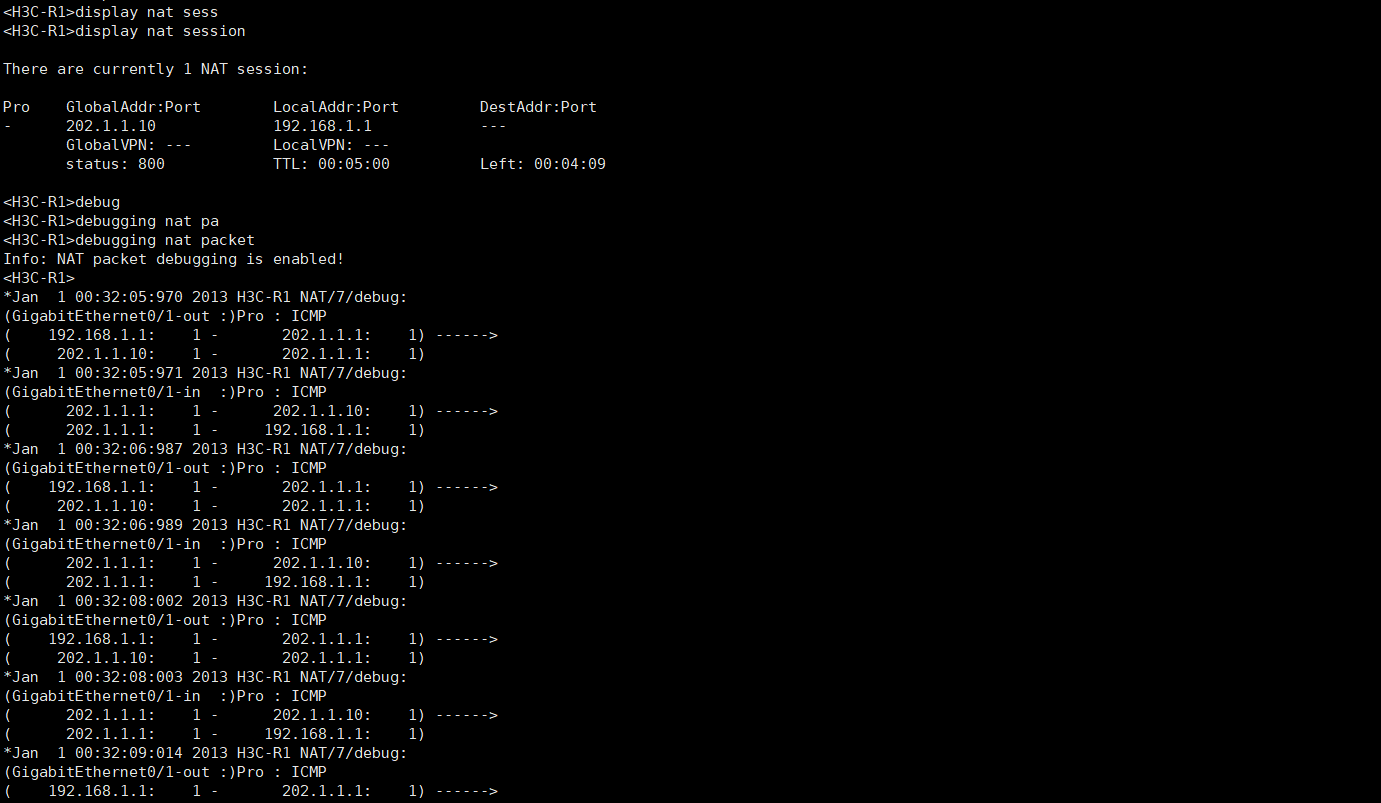
nat outbound 2000 用于配置 NAT的出站方向，其中 2000 是指定的出站方向的编号。这个命令通常涉及将内部私有网络中的内部地址映射到外部公共网络的地址。

在这个配置模式下，你可以执行其他相关的配置，比如关联地址组、指定转换类型（静态、动态、PAT 等）、配置 ACL（Access Control List）规则等，以定义具体的 NAT 转换行为。这种配置通常用于实现网络地址转换，将内部私有地址映射到一个或多个外部公共地址，以便在私有网络和公共网络之间实现通信。

9．查看Easy NAT输出及调试信息

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）





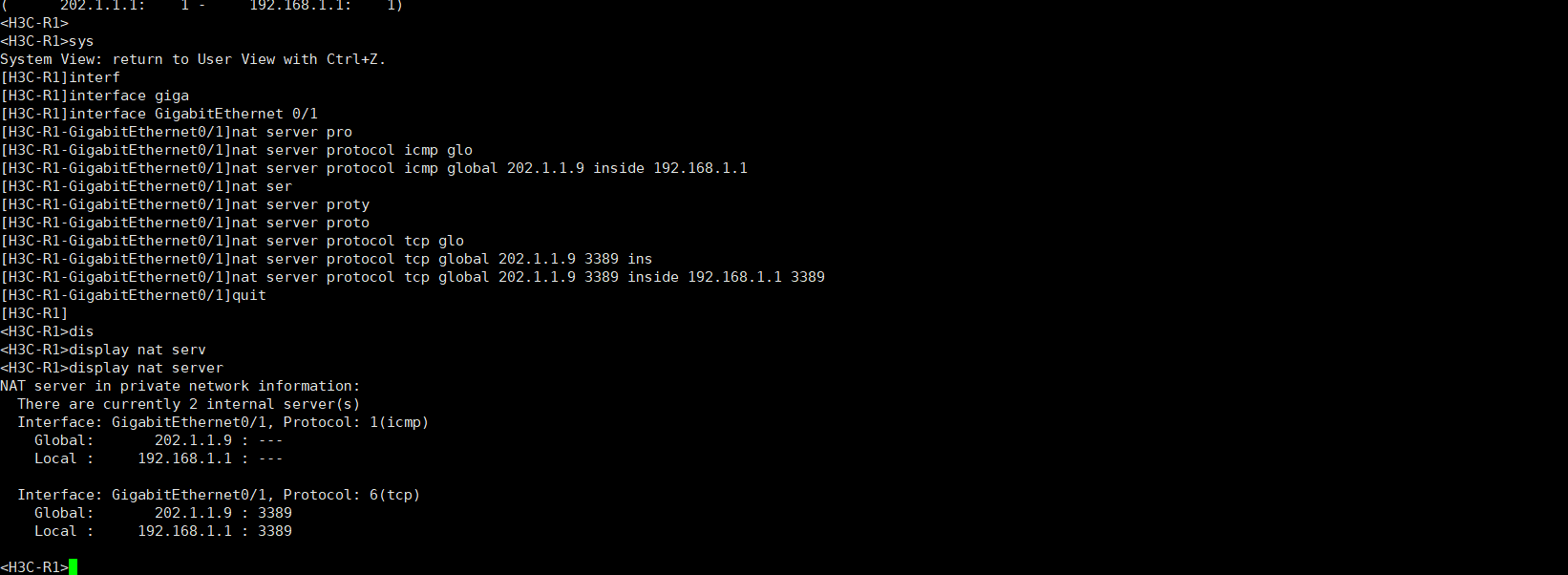
NAT 设备 H3C-R1 收到私有网络侧主机 PC1 发送的访间公有网络侧 PC2 的报文。当PC1 以地址 192.168.1.1 测试到 PC2 的连通性时，利用 NAT 设备 H3C-R1 的公有网络侧接口的“公网IP地址 202.1.1.100+端口号 12288”，建立与私有网络侧报文“源IP地址192.168.1.1+源口号 2560”间的 NAPT 转换表，并依据正向NAPT表项的结果将报文转换后向公有网络侧发送。NAT 设备收到公有网络侧的回应报文后，根据其“目的IP地址 192.168.1.1十目的端口号 2560”查找反向 NAPT 表项，并依据查表结果将报文转接后向私有网络侧发送。

同样，当 PC1 以地址 192.168.1.2 测试到 PC2 的连通性时，利用 NAT 设备 H3C-R1 的公有网络侧接口的“公网 IP 地址 202.1.1.100+端口号 12289”，建立与私有网络侧报文“源 IP地址 192.168.1.2十源端口号 2816”间的 NAPT 转换表项(正反向)并依据查找正向 NAPT表项的结果将报文转换后向公有网络侧发送。NAT 设备收到公有网络侧的回应报文后，根据其“目的 IP 地址192.168.1.2+目的端口号 2816”查找反向 NAPT 表项，并依据查表结果

将报文转换后向私有网络侧发送。

10.配置内部服务器

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）



nat server protocol icmp：这条命令的含义是将外部网络对于公共IP地址 202.1.1.9 的 ICMP流量映射到内部服务器的私有IP地址 192.168.1.1 上。

nat server protocol icmp指定了映射的协议为 ICMP，这是用于在网络中传递控制消息的协议，通常用于诊断和错误报告。

global 202.1.1.9表示映射的外部地址，即公共IP地址，这是外部网络访问的目标地址。

inside 192.168.1.1表示映射的内部服务器地址，即内部网络上的目标服务器的私有IP地址。

该命令的效果是，当外部网络发起 ICMP 请求到公共IP地址 202.1.1.9 时，NAT设备会将这个请求映射到内部服务器的 IP 地址 192.168.1.1 上，实现了对 ICMP 流量的转发。这样，内部服务器就能够接收并响应来自外部网络的 ICMP 请求。

nat server protocol tcp global 202.1.1.9 3389 inside192.168.1.1 3389：这个命令的含义是将外部网络（global）中的 TCP 流量映射到内部服务器（inside）的具体地址和端口。

nat server protocol tcp：指定要进行映射的协议为 TCP。TCP是一种面向连接的协议，提供可靠的、有序的、面向字节流的数据传输。

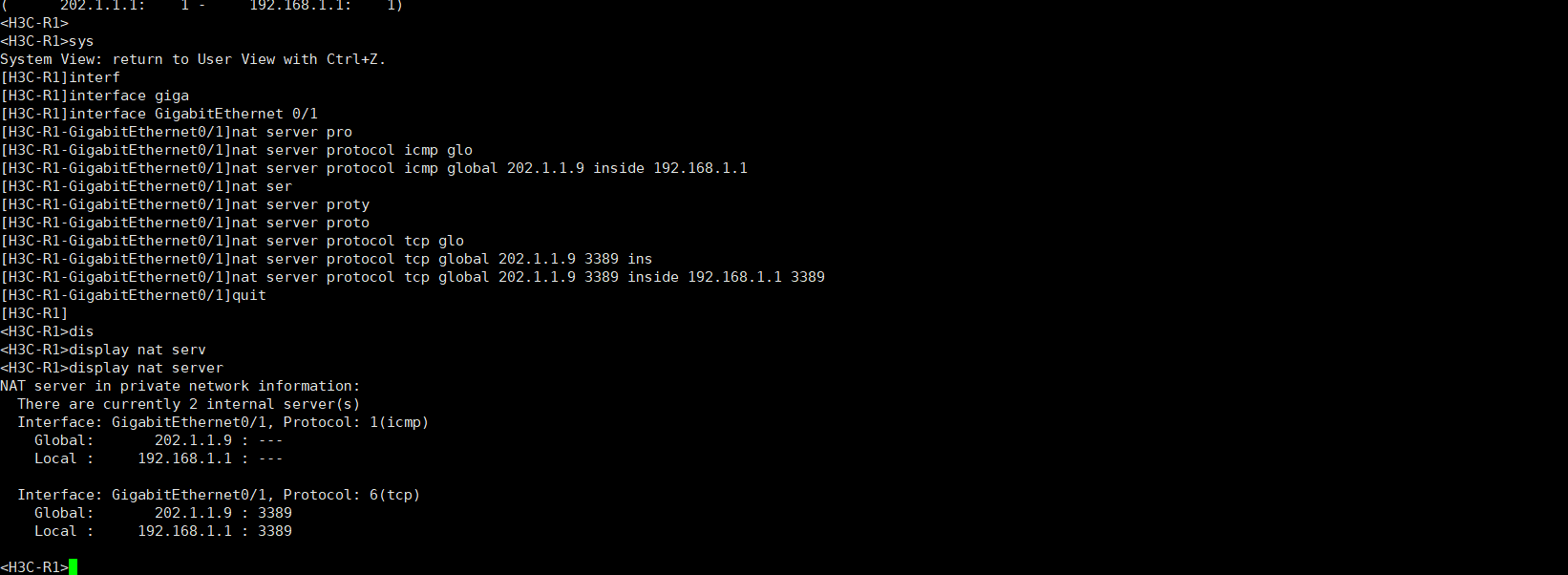
global 202.1.1.9 3389：指定映射的全局地址和端口，即外部网络上的公共IP地址为 202.1.1.9，端口为 3389。

inside 192.168.1.1 3389：指定映射到内部服务器的私有IP地址和端口，即内部网络中的服务器地址为 192.168.1.1，端口为 3389。

这个命令的效果是，当外部网络中有 TCP 流量发送到公共IP地址 202.1.1.9 的端口 3389 时（通常用于远程桌面连接），NAT会将这些 TCP 流量映射到内部网络中的 IP 地址 192.168.1.1 的端口 3389 上，确保 TCP 连接能够正确地到达内部服务器的远程桌面服务。

11. 查看内部服务器输出及调试信息

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）



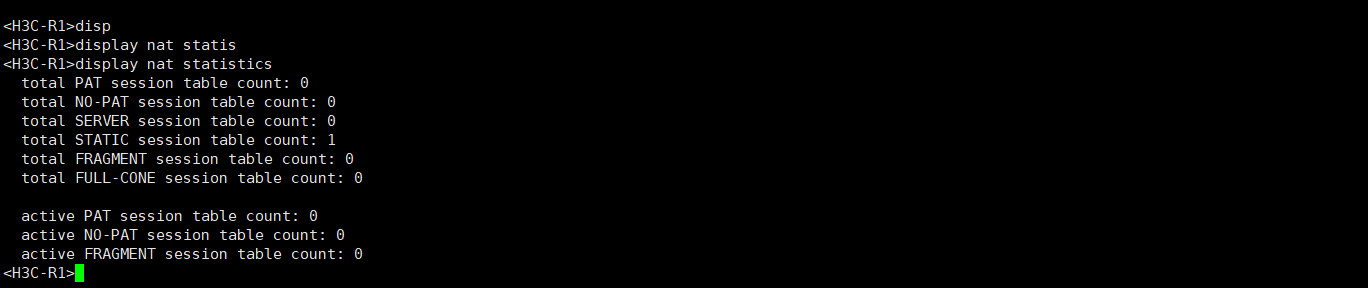
display nat server 命令显示内部服务器的信息。

There are currently 2 internal server(s): 表示存在2 条内部服务器信息。Interface:表示内部服务器所在的接口，可以看到内部服务器应用在 H3C-RI 上的Ethernet0/1。

Protocol: 表示内部服务器的协议类型。可以看到 2 条内部服务器表项使用的协议分别是ICMP 和TCP。

[global]:表示服务器外网地址/口号

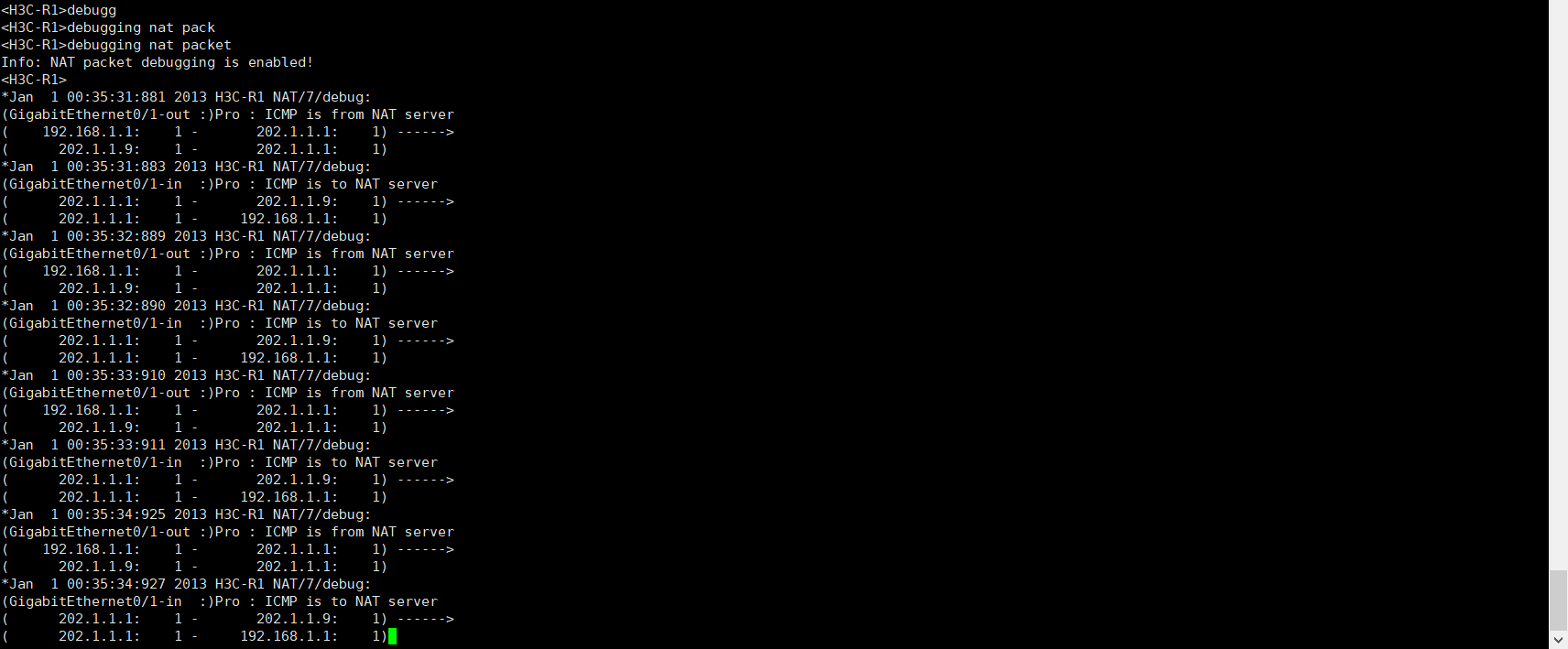
[local]: 显示服务器内网地址/端口号。



display nat statistics 命令显示地址转换的统计信息。

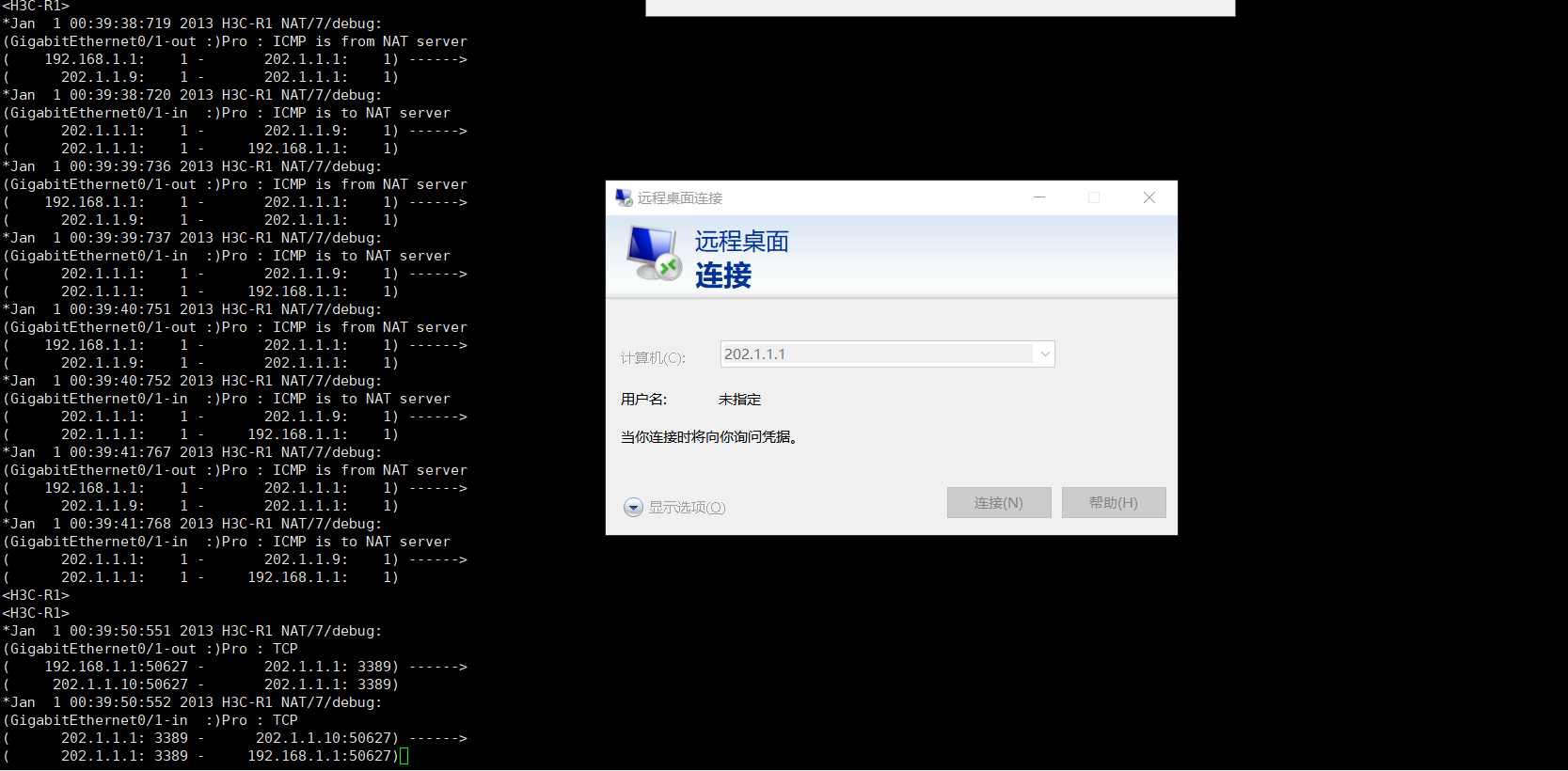
可以看到 SERVER 的转换表条目为2.因为在 NAT 设备上建立了 2 条内部服务器地址转换的记录。

可以使用 Ping 命令从 PC2 访 PCI 来测试连通性，模拟从公网主机访问私网主机换的记录信息。启用 NAT 功能的 H3C-R1 路由器上会输出调试信息。



debugging nat packet 命令调试 NAT 报文信息

从NAT 试报文输出中，可以看到 C2 通过 Ping 命令访问 PC1 来测试连通性时，路器上的报文转换过程。



五、实验结果及分析

1. 整个实验过程中遇到什么问题（有截图最好），如何解决的？通过该实验有何收获？

在实验中主机之间进行ping的时候ping不通，后来发现是没有关闭防火墙导致的。

NAT是一种常见的网络技术，进行NAT配置的实验给我带来了以下一些收获：

1. 地址转换理解：通过配置NAT，理解了内部私有地址如何映射到外部公共地址，以便在私有网络和公共网络之间进行通信。

2. 端口地址转换：学会了如何使用PAT将多个内部地址映射到一个公共地址，并使用端口信息来区分不同的连接。3. ACL规则配置：了解了如何配置ACL规则，以定义哪些流量需要进行地址转换。ACL在NAT中用于控制允许或拒绝哪些数据包进行地址转换。

4.NAT统计信息查看：学习了如何查看NAT统计信息，以监控NAT转换的效果，包括转换的数据包数量和连接数等。

5.动态NAT和静态NAT的应用：了解了动态NAT和静态NAT的区别以及它们在不同场景中的应用。静态NAT常用于将一个内部地址映射到一个外部地址，而动态NAT则允许内部主机动态地映射到外部地址。

6. 安全性考虑：学习了NAT如何提供一定程度的网络安全性，因为内部地址对外部网络是不可见的，从而提高了网络的安全性。

总体而言，NAT的实验使我能够深入了解网络中地址转换的原理和实际应用，为构建更灵活、安全的网络提供了实用的技能。