**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 学号

同作者

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；

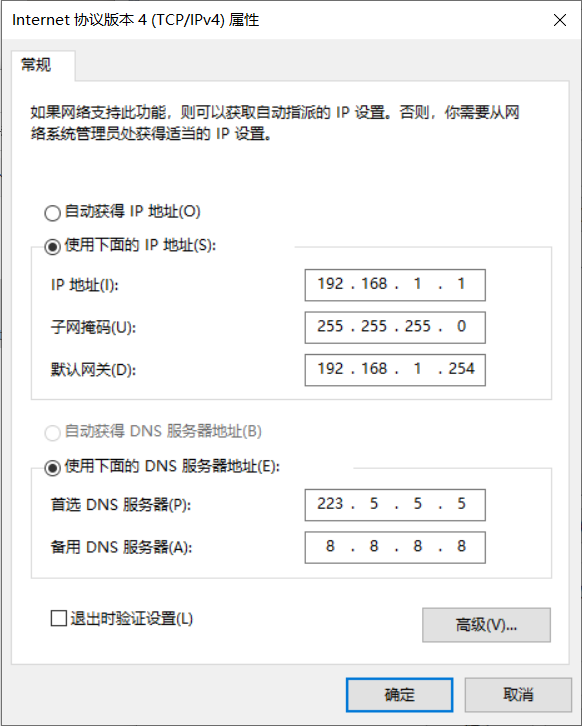
2. 2台装有Windows系列操作系统的PC（台式机或笔记本）；

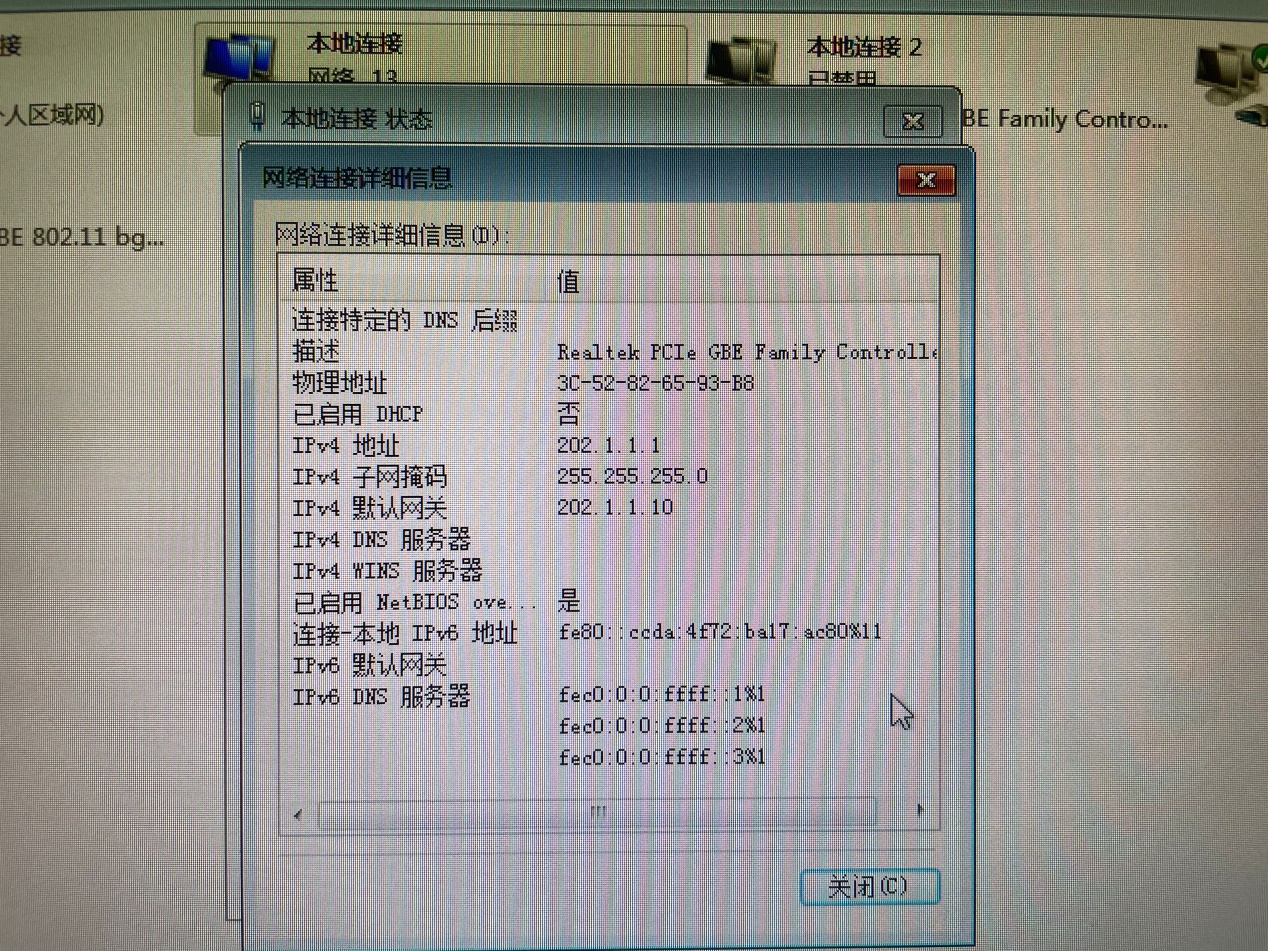
3. 2条双绞跳线（交叉线）；

## 三、实验步骤

1. 配置静态NAT

（1）首先配置PC1和PC2的IP地址，并根据表1中的H3C路由器的接口IP地址配置默认网关。

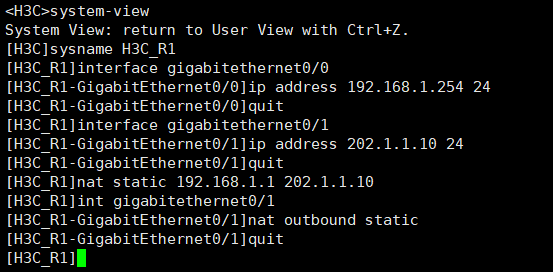




（2）之后配置H3C-R1的静态NAT。

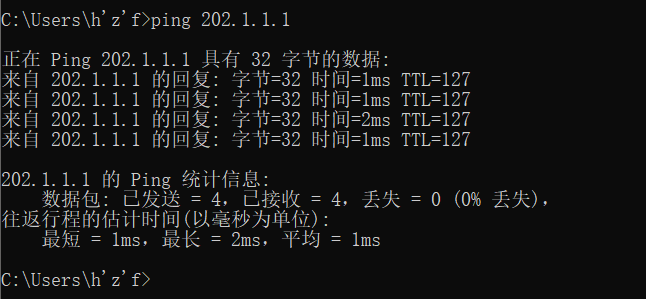
首先配置R1的接口地址，根据表1，E0/0为192.168.1.254/24,E0/1为202.1.1.10/24。

之后配置静态NAT，其中 为配置一对一的静态地址转换映射，设置了内网IP（192.168.1.1）和外网IP（202.1.1.10）的转换映射。然后进入E0/1的接口视图，并使用 命令，使配置的NAT静态转换在E0/1接口上生效。

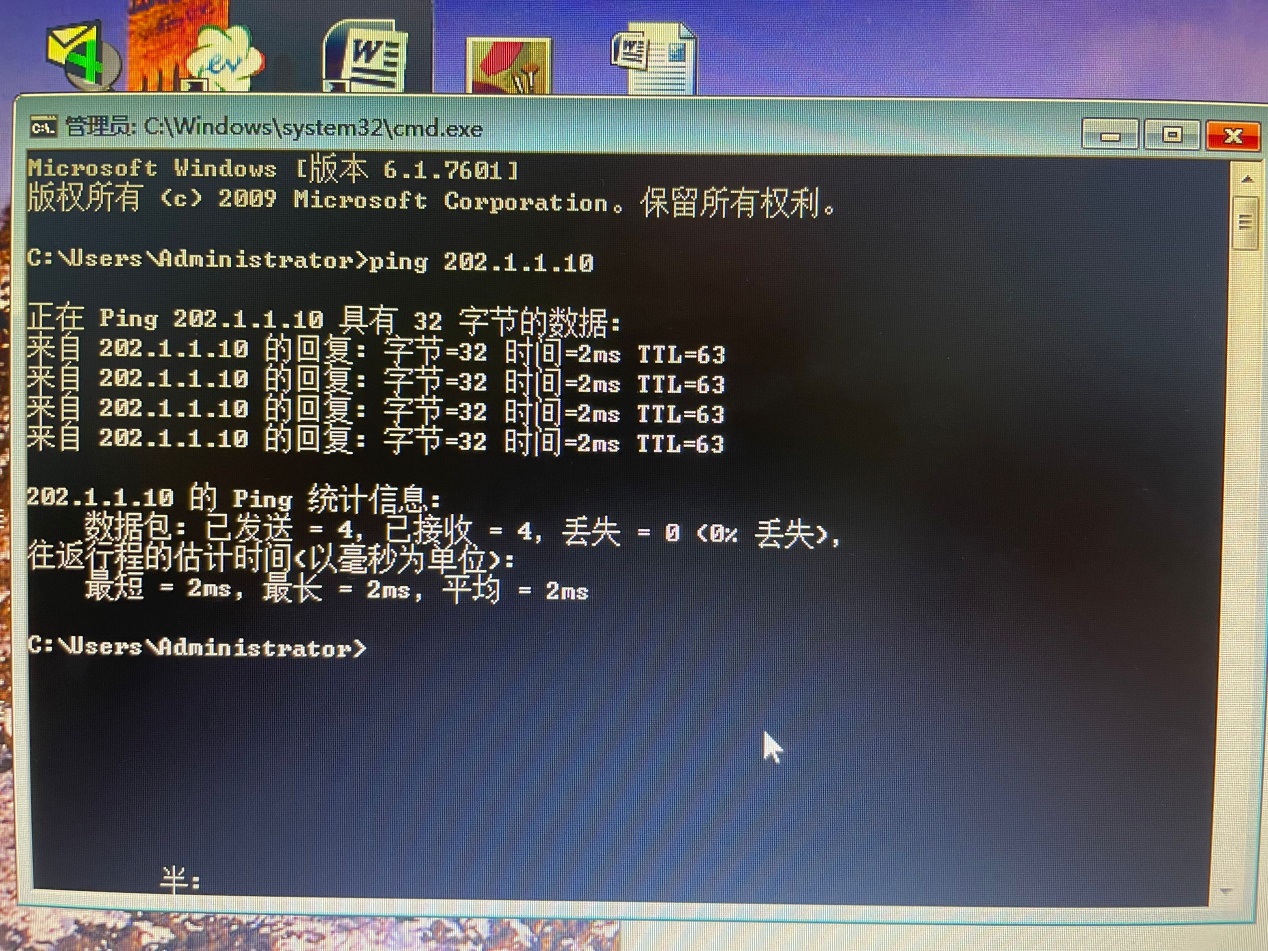


2. 从PC上查看NAT是否成功

（1）完成配置以后，首先测试内网主机访问外网主机，在PC1中，使用ping命令访问PC2，查看NAT是否成功。由ping结果可知，PC1到PC2连通性正常。



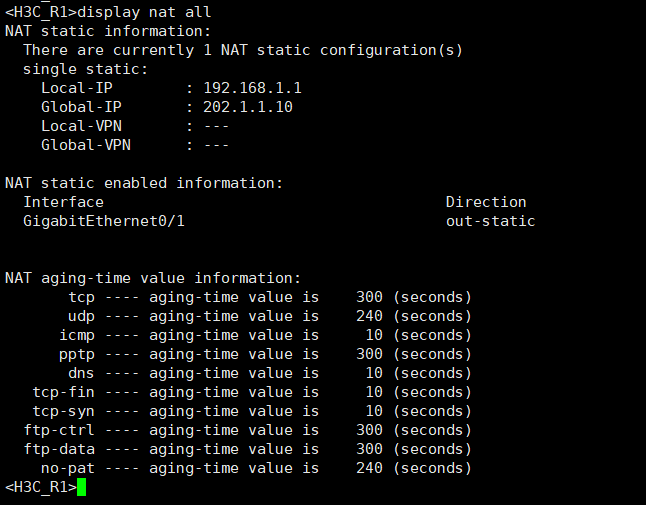
（2）之后测试外网主机访问内网主机，在PC2中，使用ping命令访问PC1，查看NAT是否成功。由ping结果可知，PC2到PC1连通性正常。



3. 在路由器上查看和调试NAT信息

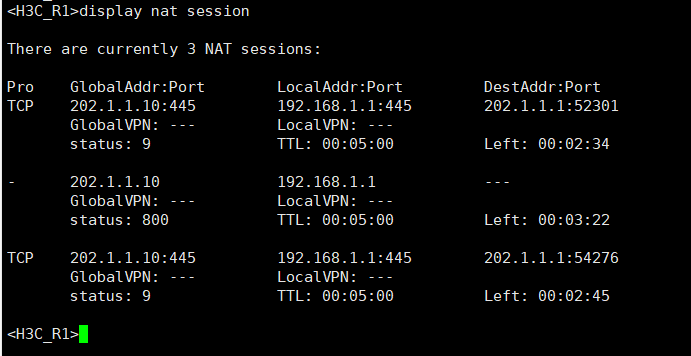
（1）在使用ping命令测试NAT地址转换后，立即通过display命令查看NAT配置及状态信息。具体信息如下图所示。

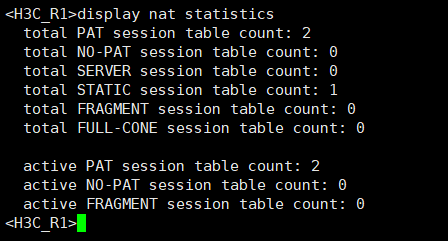
首先查看NAT信息，其中 命令可以显示所有的NAT配置信息，可以看到有一条NAT静态地址转换关联信息，Local-IP（192.168.1.1）与Global-IP（202.1.1.10）即为我之前配置的静态转换映射，并在我们配置的E0/1接口上。



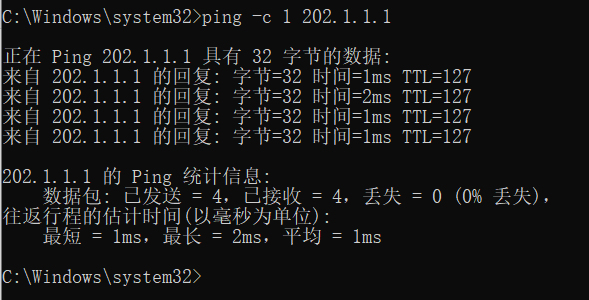
（2）之后使用 命令，查看当前NAT转换表项信息。可以看到静态NAT的GlobalAddr:port（外部地址和端口）为202.1.1.10:0，由于不区分应用，端口为0；LocalAddr:Port（内部源地址和源端口）为192.168.1.1:0，由于不区分应用，端口为0。TTL为NAT表项的生命周期，其中输出为00:05:00，即300s；Left为NAT表项的剩余存活时间，其中输出为00:03:22，即202s。

根据 命令的结果，可以发现有1个静态NAT转换表。

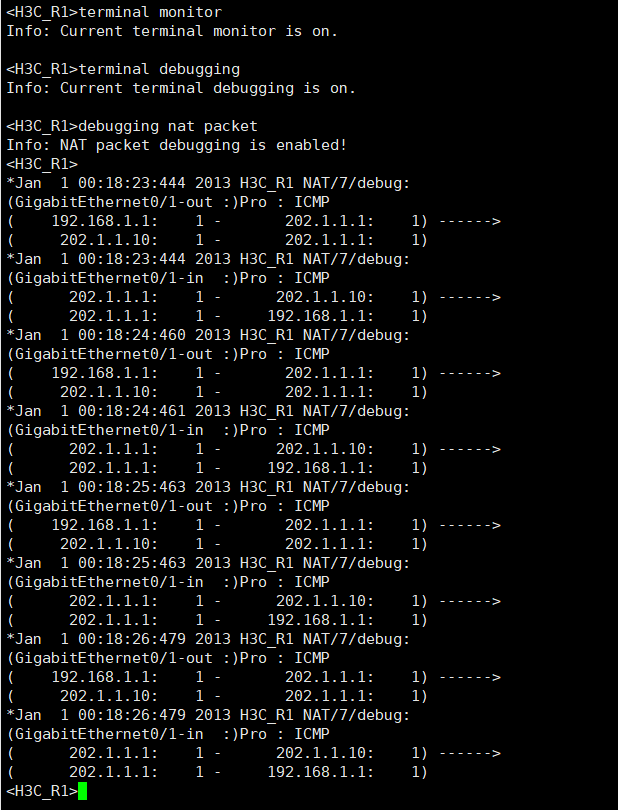




（3）打开R1的nat packet调试后，使用 发送一个ping包，查看调试信息。



查看调试信息。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R1的E0/1接口的出方向进行地址转换时，通过查找NAT地址表，把PC1发出的报文的源地址192.168.1.1转换成202.1.1.10，继续通过E0/1接口向外发送。当E0/1接口的入方向收到了去往202.1.1.10的目的地址时，通过NAT地址表，把202.1.1.10转换成192.168.1.1后继续进行后续的路由转发。



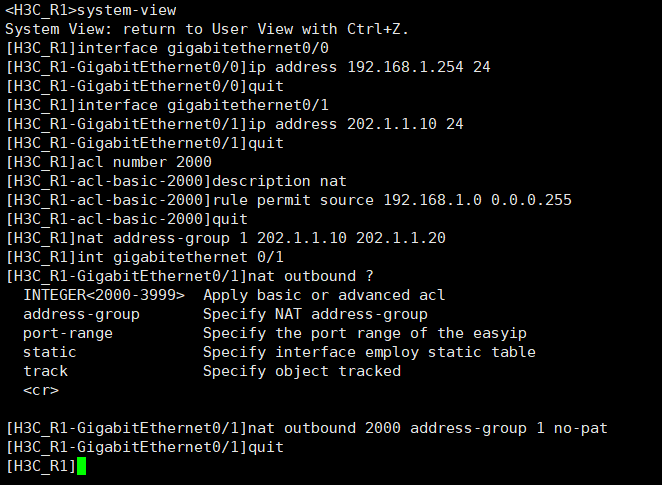
4. 配置Basic NAT

配置动态NAT，此处在R1上允许192.168.1.0/24网段访问外网，并配置公有地址池为202.1.1.10——202.1.1.20。

首先配置R1的接口地址，之后在R1上配置ACL，用来判断哪些数据包的地址应该被转换。此处的 即规定了只允许源IP为192.168.1.0——192.168.1.255之间的地址转换。

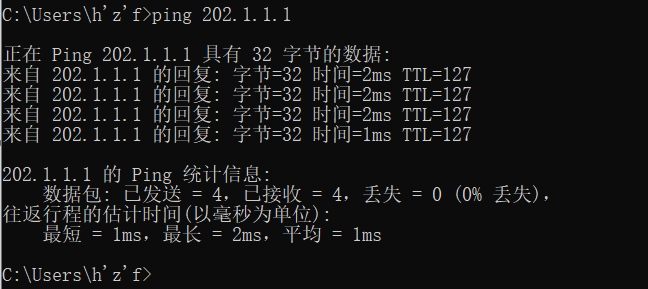
之后配置用于地址转换的公网地址池。 命令即配置了一个地址池，索引号为1，地址范围为202.1.1.10——202.1.1.20。

最后连接外网的接口上配置地址转换。使用 在E0/1上，将出接口配置访问控制列表和地址池1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

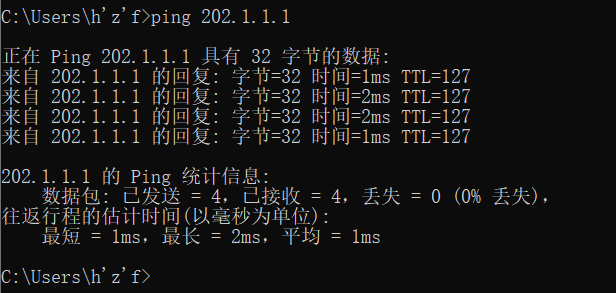
（1）完成配置后，首先测试内网主机访问外网主机，在PC1中访问PC2，测试连通性，发现连通性正常，内网主机已经能够成功访问外网主机。



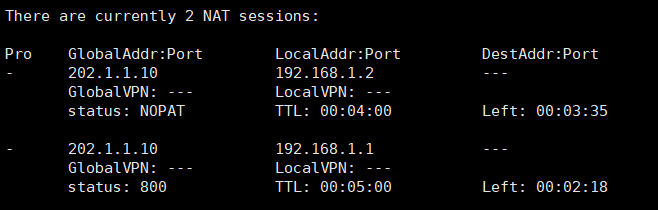
（2）之后更改内网主机PC的IP地址为192.168.1.2。

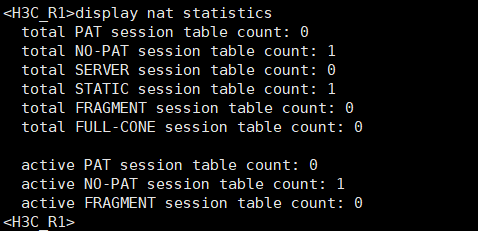


（3）在PC1的命令行下，再次使用ping访问PC2，同样，内网主机可以访问外网主机。

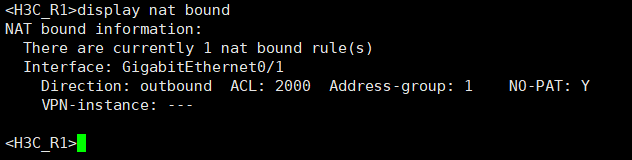


（4）之后使用display命令查看Basic NAT的状态输出。可以看到，由于当前活跃的只有1台本地PC（此时IP为192.168.1.2），且2600路由器只有两个端口，但是实验是在2台活跃本地PC的条件下进行测试的，因此此时显示的2个NAT转换表，只有1个状态为NOPAT，且GlobalAddr都为202.1.1.10，而非书中的202.1.1.10和202.1.1.11。

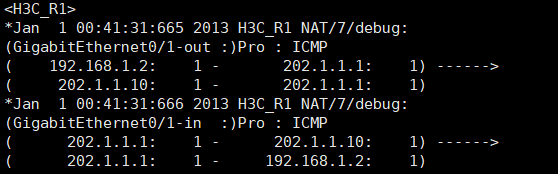




（5）但是对于nat bound的display，可以看到对于我们之前设置的地址池规则，状态正常，ACL为设置的2000，并采用编号为1的地址池（192.168.1.0——192.168.1.255），NO-PAT状态也为Y。

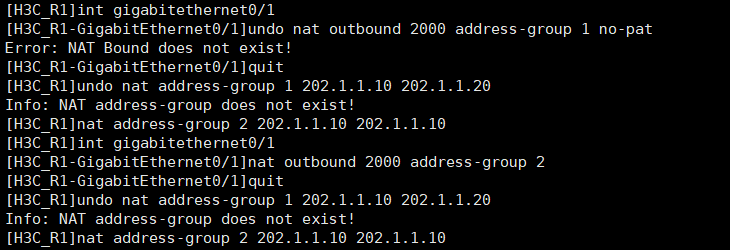


（6）在ping连通测试的nat packet调试中，Pro字段显示ICMP，所以输出的192.168.1.2:1中的1表示通过的报文是ICMP报文。当报文通过R1的E0/1接口的出方向进行地址转换时，通过查找NAT地址表，把PC1发出的报文的源地址192.168.1.2转换成202.1.1.10，继续通过E0/1接口向外发送。当E0/1接口的入方向收到了去往202.1.1.10的目的地址时，通过NAT地址表，把202.1.1.10转换成192.168.1.2后继续进行后续的路由转发。



6. 配置NAPT

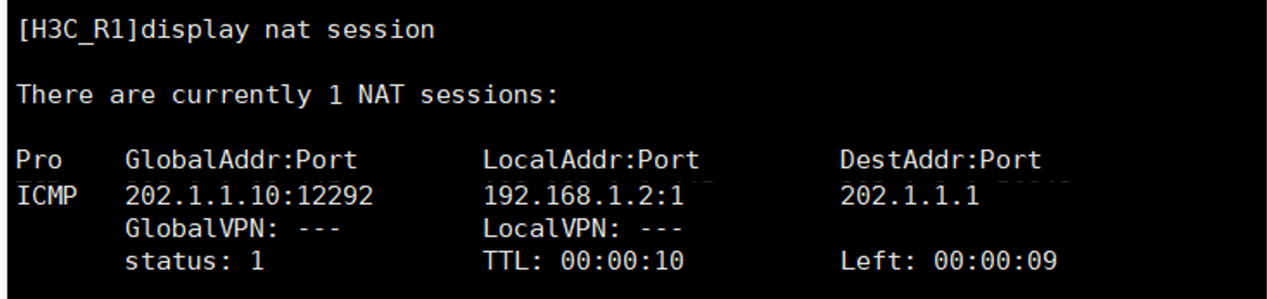
在上面配置Basic NAT的基础上改编配置，完成NAPT的配置，首先弃用之前的地址池1，并重新设置地址池2（202.1.1.10-202.1.1.10），并在E0/1端口的出接口配置访问控制列表和地址池2相关联。

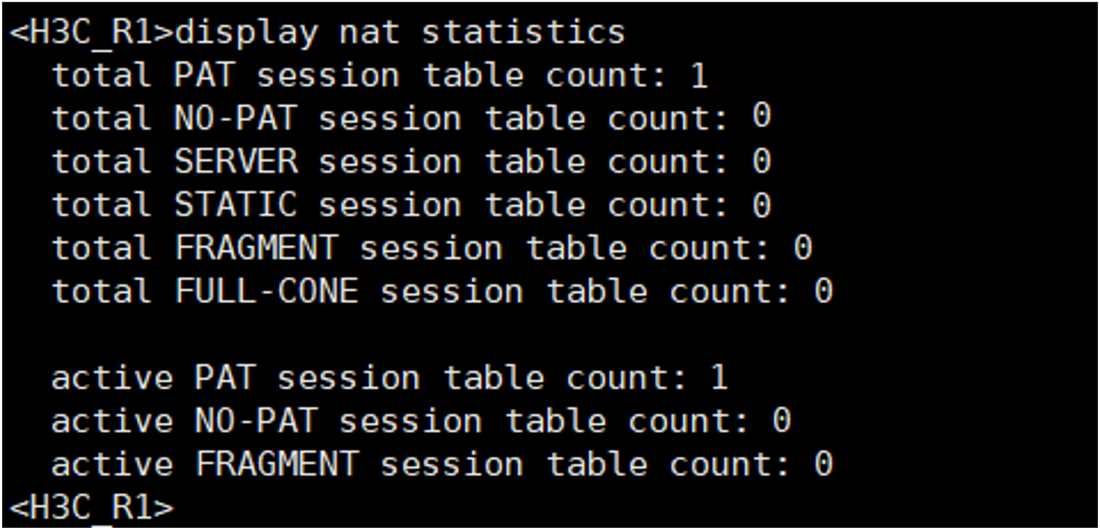


7. 查看NAPT输出及调试信息

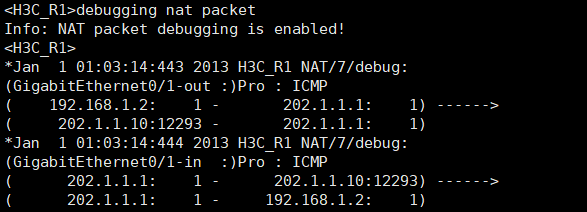
配置完成后，使用ping命令进行测试，之后使用display命令查看NAPT的状态输出。

对于 命令，由于ping发出的是ICMP协议，因此Pro为ICMP。NAPT能够同时映射IP地址和端口号，因此测试PC1到PC2连通性时，NAT设备R1从地址池选取一个空闲的“公网IP+端口号”，建立与私有网络侧报文“源IP地址+源端口号”间的NAPT转换表项。



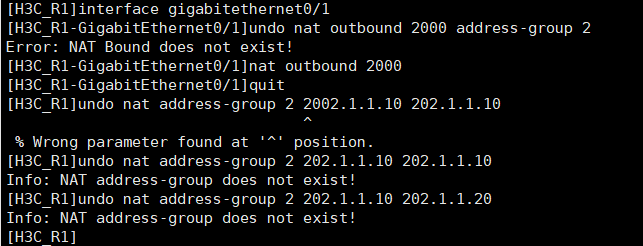


对于nat packet的debugging，当PC1以地址192.168.1.2测试到PC2的连通性时，NAT设备R1从地址池1中选取空闲的“公网IP202.1.1.10 + 端口号12293”，建立与私有网络侧报文“源IP地址192.168.1.2 + 端口号1”间的NAPT转换表项，并依据查找正向NAPT表项的结果将报文转换后向共有网络侧发送。NAT设备收到共有网络侧的回应报文后，根据其“目的地址192.168.1.2 + 目的端口号1”查找反向NAPT表项，并依据查表结果将报文转换后向私有网络侧发送。



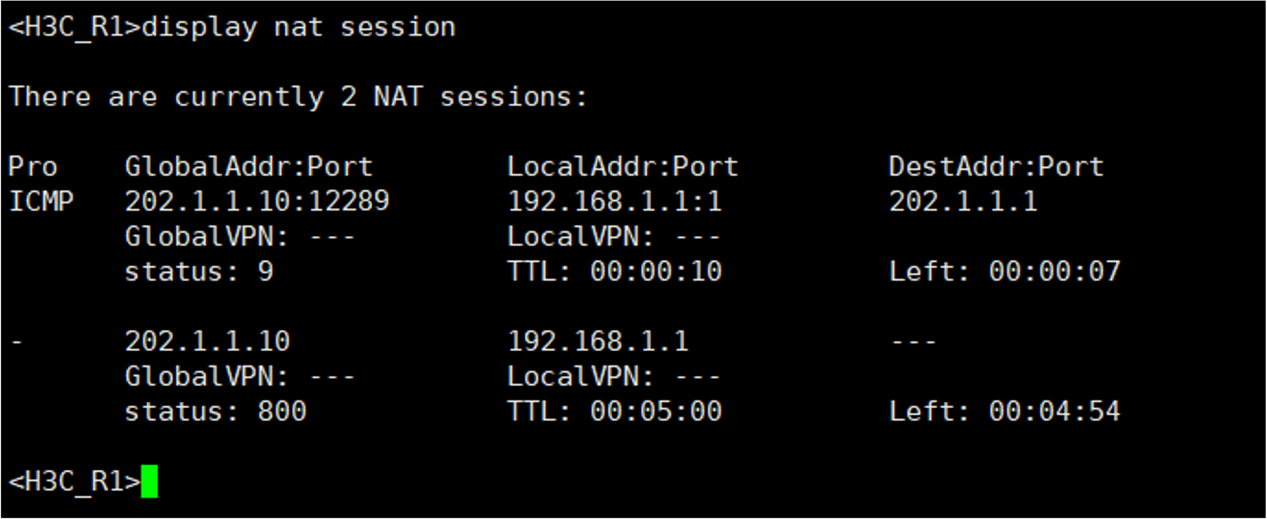
8. 配置Easy NAT

在配置NAPT的基础上改变配置，完成Easy NAT的配置，弃用地址池2，并使用 命令，在E0/1出接口配置访问控制列表，表示直接使用该接口的IP地址作为转换的地址，实现Easy IP功能。Easy NAT方式直接使用NAT设备接口的公网IP地址作为转换后的源地址进行地址转换，这样可以动态获取出接口地址，也可以通过ACL来控制哪些内部地址可以进行地址转换。

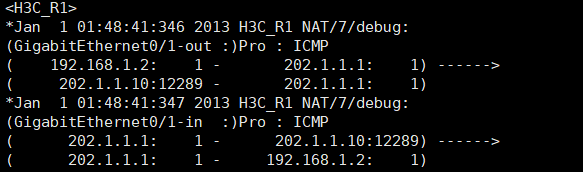


9．查看Easy NAT输出及调试信息

配置完成后，使用ping命令测试，然后使用display命令查看Easy NAT的状态输出。Easy NAT方式页能够同时映射IP地址和端口号，因此当测试PC1到PC2连通性时，NAT设备R1能够使用NAT设备上公网接口的IP地址，即“公网IP + 端口号”建立与私有网络侧报文“源IP地址 + 端口号”间的Easy NAT转变表项。



对于nat packet的debugging，当PC1以地址192.168.1.2测试到PC2的连通性时，NAT设备R1从地址池1中选取空闲的“公网IP202.1.1.10 + 端口号12289”，建立与私有网络侧报文“源IP地址192.168.1.2 + 端口号1”间的NAPT转换表项，并依据查找正向NAPT表项的结果将报文转换后向共有网络侧发送。NAT设备收到共有网络侧的回应报文后，根据其“目的地址192.168.1.2 + 目的端口号1”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。

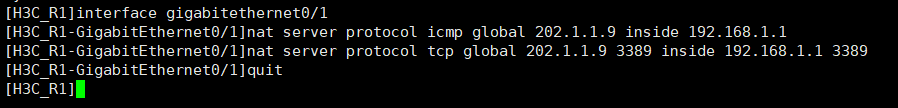


10.配置内部服务器

此处配置H3C路由器作为NAT的内部服务器，实现公网主机访问局域网私网服务器主机。由于各个接口的地址和之前的配置相同，因此不做重新配置，此处直接从配置内部服务器开始配置。

即为定义一个内部服务器映射表，用户可以通过global-address定义的地址和global-port定义的端口来访问地址和端口分别为local-address和local-port的内部服务器。

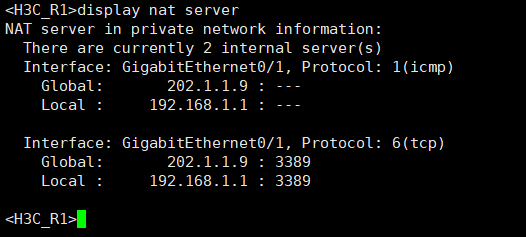
下面的命令即使用icmp协议和tcp协议，分别定义了202.1.1.9的全局地址访问私有地址192.168.1.1的映射表。

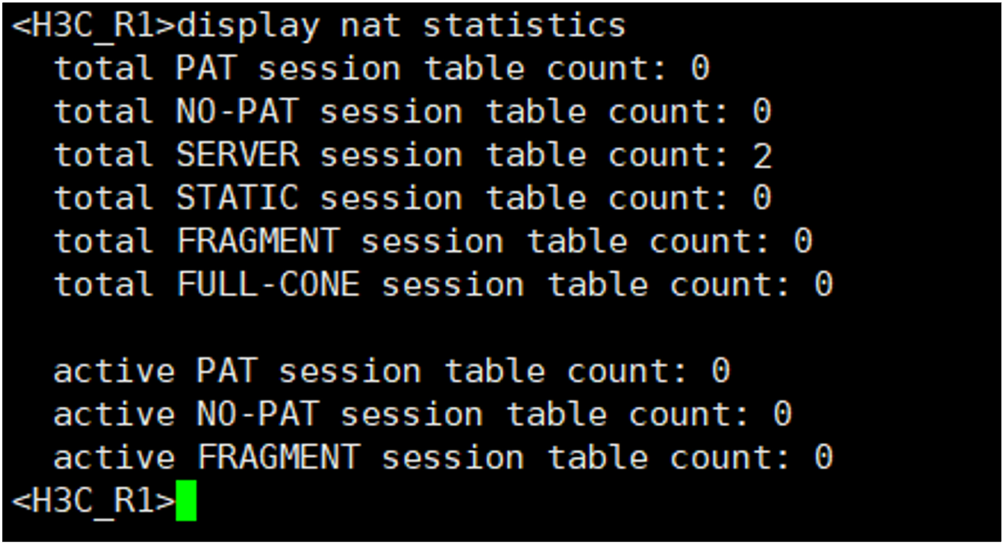


11. 查看内部服务器输出及调试信息

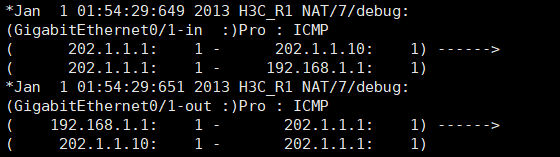
（1）配置完成后，使用display命令查看设备上配置的内部服务器状态信息。可以看到，存在2条内部服务器信息，均为之前我们设置的protocol、global-ip、global-port、local-ip、local-port。

关于地址转换的统计信息中，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信息。





（2）之后使用ping命令从PC2访问PC1来测试连通性，模拟从公网主机访问私网主机，可以看到以下调试信息。Pro字段显示ICMP，所以输出的202.1.1.1:1中的1表示通过的报文是ICMP报文。当报文通过R1的E0/1接口的出方向进行地址转换时，通过查找NAT地址表，把PC2发出的报文的源地址202.1.1.1转换成202.1.1.10，继续通过E0/1接口向外发送。当E0/1接口的入方向收到了去往192.168.1.1的目的地址时，通过NAT地址表，把202.1.1.10转换成192.168.1.1后继续进行后续的路由转发。



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？

在配置Basic NAT、NAPT、Easy NAT时，由于没有和书上相同的实验结果，即display中记录的本地PC端的IP地址：192.168.1.1和192.168.1.2两个IP地址在书中的实例中同时出现（我的实验中只出现了1个，且是当前配置的本机IP），因此产生了许多对实验现象的困惑。经过和老师的讨论，发现可能是设备型号的问题，没有同时active的192.168.1.1和192.168.1.2两个IP端设备，而只有1个本地PC端，因此H3C-R1没有对不活跃的IP进行记录导致的，但根据辅导资料中的实验理论，仍然可以对现有的现象进行分析，不影响实验的进行和实验结果的验证。