

计算机网络实验报告

警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4. 实验报告文件以 PDF 格式提交。

| | | | | | |
|------|-----------------|------|--------|-----------------|----|
| 院系 | 计算机学院 | 班 级 | 1 班+保密 | 组长 | 马岱 |
| 学号 | <u>22336180</u> | | | <u>22336090</u> | |
| 姓名 | <u>马岱</u> | | | <u>黄集瑞</u> | |
| 实验分工 | | | | | |
| 姓名 | | 分工 | | 在本次中的占比 | |
| 马岱 | | 合作完成 | | 50% | |
| 黄集瑞 | | 合作完成 | | 50% | |

【实验内容】

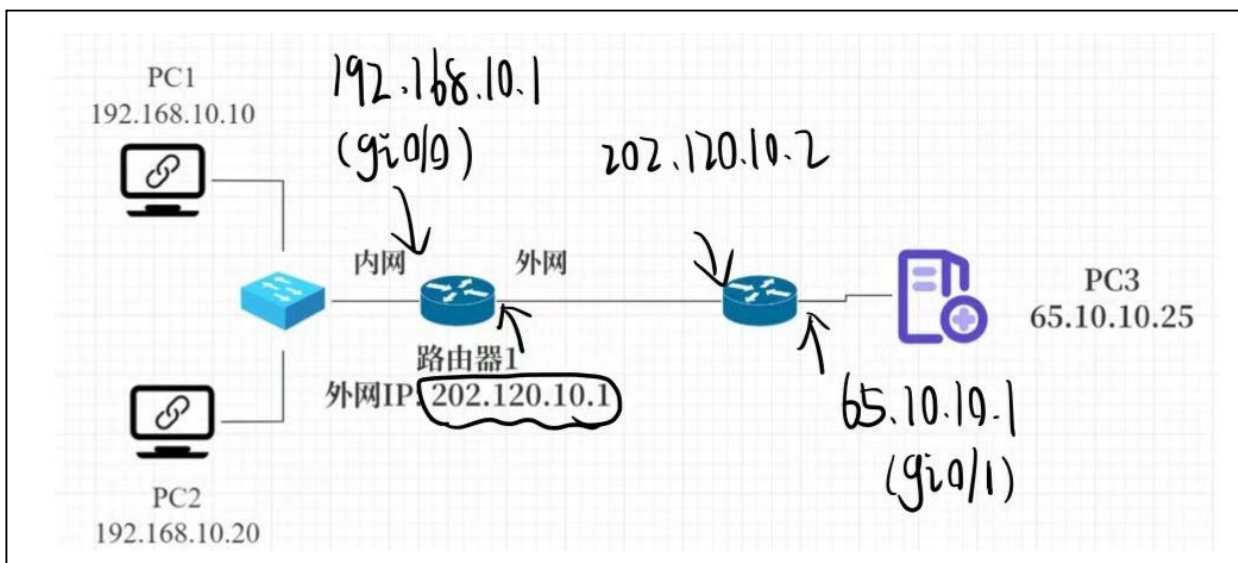
按上图的网络拓扑搭建网络，实验要求如下：

- (1) PC1, PC2, PC3 的 IP 如图所示，未标明的接口请自行设定 IP 地址；
- (2) 路由器 1 为 NAT 路由器，所有从内网访问外网的数据包共享路由器 1 的外网 IP 地址；
- (3) PC1、PC2 均可 ping 通 PC3；
- (4) 允许 PC1 访问 PC3 上的 Web 服务，禁止 PC2 访问 PC3 上的 Web 服务；
- (5) 在 PC3 上运行 Wireshark 进行抓包，分析数据包的源 IP 地址和目的 IP 地址。

请完成以上要求，并截图记录以下信息：

- (1) 在 PC1 和 PC2 上分别 ping PC3；
- (2) 在 PC1 和 PC2 的浏览器中输入 PC3 的 IP 地址，记录网页载入情况；
- (3) 在 PC3 Wireshark trace 中源 IP 地址和目的 IP 地址是否符合预期。

【实验拓扑】



Attention!!! 由于我们原本所在组 16 组的路由器 2 损坏，因此我们已经征得老师同意使用第 17 组的路由器来完成实验，所以截图显示的是 17 组的组号。

计算机网络实验报告

【实验记录】

- 步骤一：
 - (1) 按照拓扑图上的标示，配置 PC1、PC2 以及 PC3 的 IP 地址、子网掩码、网关，具体配置如下：

编辑 IP 设置

手动

IPv4

开

IP 地址

192.168.10.10

子网前缀长度

24

网关

192.168.10.1

首选 DNS

备用 DNS

保存

取消

编辑 IP 设置

手动

IPv4

开

IP 地址

192.168.10.20

子网前缀长度

24

网关

192.168.10.1

首选 DNS

备用 DNS

保存

取消

编辑 IP 设置

手动

IPv4

开

IP 地址

65.10.10.25

子网前缀长度

24

网关

65.10.10.1

首选 DNS

备用 DNS

保存

取消

我们根据上面的拓扑图，分别将 PC1、PC2 和 PC3 的 IP 地址配置成 192.168.10.10、192.168.10.20 以及 63.10.10.25；同时将网关分别设置成第一跳路由器的 IP 地址为 192.168.10.1 以及 63.10.10.1

- (2) 按照拓扑图上的标示，分别配置路由器 1 和路由器 2 的端口 IP 地址

路由器 2:

```
17-RSR20-2(config)#interface serial 2/0
17-RSR20-2(config-if-Serial 2/0)#ip address 202.120.10.2 255.255.255.0
17-RSR20-2(config-if-Serial 2/0)#no shutdown
17-RSR20-2(config-if-Serial 2/0)#exit
17-RSR20-2(config)#interface gigabitethernet 0/1
17-RSR20-2(config-if-GigabitEthernet 0/1)#ip address 65.10.10.1 255.255.255.0
17-RSR20-2(config-if-GigabitEthernet 0/1)#no shutdown
17-RSR20-2(config-if-GigabitEthernet 0/1)#exit
```

观察对应结果:

```
17-RSR20-2(config)#show ip interface brief
Interface              IP-Address(Pri)      IP-Address(Sec)      Status
Serial 2/0              202.120.10.2/24      no address            up
Serial 3/0              no address           no address            down
GigabitEthernet 0/0     no address           no address            down
GigabitEthernet 0/1     65.10.10.1/24       no address            up
VLAN 1                  no address           no address            down
```

可以看到，以上配置都按照我们所期望的进行配置。

计算机网络实验报告

路由器 1:

```
Password:
17-RSR20-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
17-RSR20-1(config)#interface gigabitethernet 0/0
17-RSR20-1(config-if-GigabitEthernet 0/0)#ip address 192.168.10.1 255.255.255.0
17-RSR20-1(config-if-GigabitEthernet 0/0)#ip nat inside
17-RSR20-1(config-if-GigabitEthernet 0/0)#exit
17-RSR20-1(config)#interface serial 2/0
17-RSR20-1(config-if-Serial 2/0)#ip address 202.120.10.1 255.255.255.0
17-RSR20-1(config-if-Serial 2/0)#ip nat outside
17-RSR20-1(config-if-Serial 2/0)#exit
```

可以看到在路由器 1 处我们不仅仅是配置了端口的 ip 地址，同时也使用了 ip nat inside 以及 ip nat outside 指令，分别在内部和外部接口上指定了 NAT，以作用于我们之后实现端口的静态转换。

```
17-RSR20-1(config)#show ip interface brief
Interface                               IP-Address(Pri)    IP-Address(Sec)    Status
-----
Serial 2/0                               202.120.10.1/24    no address          up
SIC-3G-WCDMA 3/0                         no address          no address          up
GigabitEthernet 0/0                     192.168.10.1/24    no address          up
GigabitEthernet 0/1                       no address          no address          down
VLAN 1                                   no address          no address          up
```

```
17-RSR20-1(config)#show ip route
```

```
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
C    192.168.10.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.10.1/32 is local host.
C    202.120.10.0/24 is directly connected, Serial 2/0
C    202.120.10.1/32 is local host.
```

可以看到以上配置都按照我们所期望的来配置。

(3) 配置端口静态地址转换并且配置 ACL 来实现题目的要求

```
C    202.120.10.1/32 is local host.
17-RSR20-1(config)#$ list 100 interface serial 2/0 overload
17-RSR20-1(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0
17-RSR20-1(config)#$it tcp 192.168.10.10 0.0.0.255 host 65.10.10.25 eq www
17-RSR20-1(config)#$ tcp 192.168.10.20 0.0.0.255 host 65.10.10.25 eq www
17-RSR20-1(config)#access-list 100 permit ip any any
17-RSR20-1(config)#interface gigabitethernet 0/0
17-RSR20-1(config-if-GigabitEthernet 0/0)#ip access-group 100 in
17-RSR20-1(config-if-GigabitEthernet 0/0)#show access-list

ip access-list extended 100
 10 permit tcp 192.168.10.0 0.0.0.255 host 65.10.10.25 eq www
 20 deny tcp 192.168.10.0 0.0.0.255 host 65.10.10.25 eq www
 30 permit ip any any
17-RSR20-1(config-if-GigabitEthernet 0/0)#
```

计算机网络实验报告

如图所示，我们将匹配访问控制列表的 100 的内部地址进行 NAT 转换，将内部地址都转换成 serial 2/0 接口的 IP 地址；同时，我们使用了 overload，启用了这个参数之后，我们可以实现多个不同的内部设备之间的连接，使得多个内部设备共享同一个公共 IP 地址来进行对外部的访问。而将这些带入到我们的实验就是 PC1 以及 PC2 共享路由器 1 的外部 IP 地址 202.120.10.1，这样就完成了静态地址转换。

此外，我们设置的 ACL 100，作用只是为了限制 PC2 不能访问 PC3 的 web 服务，而其他服务是不受限制的（也就是 ping 是可以 ping 通的）。注意这里必须使用大于 99 的 ACL，最开始使用了 ACL 1，一直报错表示无效命令，后来经过上网查询我们了解到标准的 ACL 号是从 1-99 和 1300-1999，而我们需要使用扩展的 ACL，所以必须使用大于 99 的 ACL 号。

接下来，让我们通过 PC1 ping PC2，并立刻查看此时的端口地址的转换：

```
17-RSR20-1(config)#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
udp 202.120.10.1:38800 192.168.10.10:38800 10.8.4.4:53        10.8.4.4:53
udp 202.120.10.1:38800 192.168.10.10:38800 10.8.8.8:53        10.8.8.8:53
17-RSR20-1(config)#
```

可以看到内部 PC 的 ip 地址都被转换到了 202.120.10.1

● 步骤二：

接下来，我们来验证个主机之间的连通性

PC1:

```
C:\Users\D502>ping -S 192.168.10.10 65.10.10.25
```

正在 Ping 65.10.10.25 从 192.168.10.10 具有 32 字节的数据：

来自 65.10.10.25 的回复: 字节=32 时间=36ms TTL=126

来自 65.10.10.25 的回复: 字节=32 时间=36ms TTL=126

来自 65.10.10.25 的回复: 字节=32 时间=36ms TTL=126

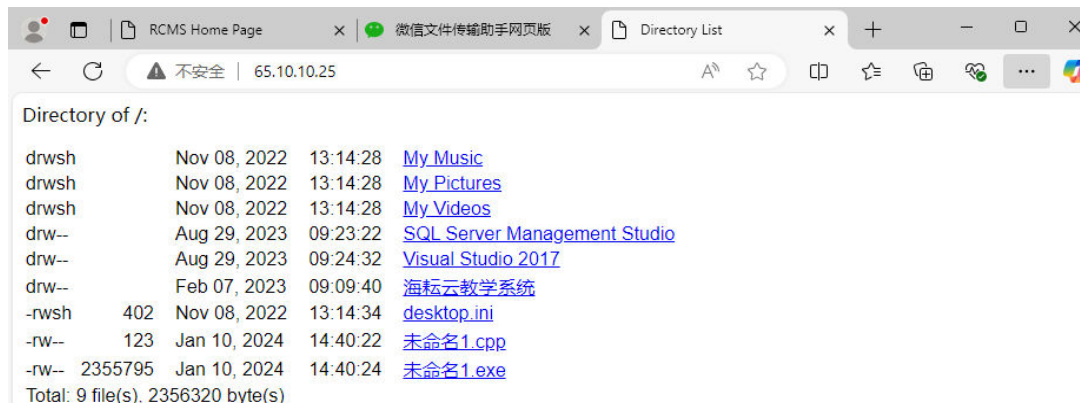
来自 65.10.10.25 的回复: 字节=32 时间=38ms TTL=126

65.10.10.25 的 Ping 统计信息：

数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，

往返行程的估计时间(以毫秒为单位)：

最短 = 36ms，最长 = 38ms，平均 = 36ms



可以看到 PC1 不仅可以 ping 通 PC3，并且可以访问其的 web 服务器

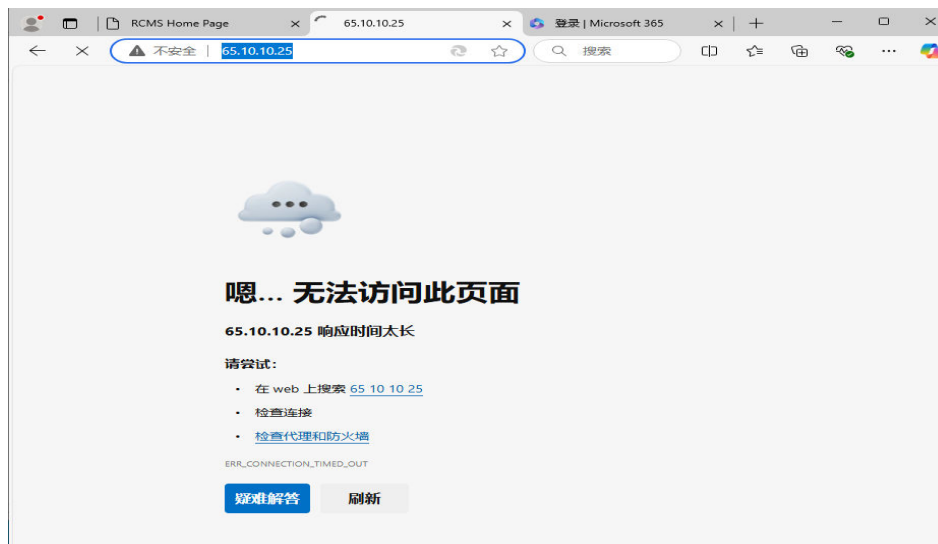
计算机网络实验报告

PC2:

```
C:\Users\D502>ping -S 192.168.10.20 65.10.10.25

正在 Ping 65.10.10.25 从 192.168.10.20 具有 32 字节的数据:
来自 65.10.10.25 的回复: 字节=32 时间=36ms TTL=126
来自 65.10.10.25 的回复: 字节=32 时间=35ms TTL=126
来自 65.10.10.25 的回复: 字节=32 时间=39ms TTL=126
来自 65.10.10.25 的回复: 字节=32 时间=38ms TTL=126

65.10.10.25 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 35ms, 最长 = 39ms, 平均 = 37ms
```



可以看到 PC2 可以 ping 通 PC3，但是却不能访问其的 web 服务器

抓包:

| Source | Destination | Protocol | Length | Info |
|--------------|--------------|----------|--------|---|
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0001, seq=45/11520, ttl=126 (reply in 119) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=45/11520, ttl=128 (request in 118) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0001, seq=46/11776, ttl=126 (reply in 129) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=46/11776, ttl=128 (request in 128) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0001, seq=47/12032, ttl=126 (reply in 133) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=47/12032, ttl=128 (request in 132) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0001, seq=48/12288, ttl=126 (reply in 180) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=48/12288, ttl=128 (request in 179) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0302, seq=53/13568, ttl=126 (reply in 403) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0302, seq=53/13568, ttl=128 (request in 402) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0302, seq=54/13824, ttl=126 (reply in 405) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0302, seq=54/13824, ttl=128 (request in 404) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0302, seq=55/14080, ttl=126 (reply in 438) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0302, seq=55/14080, ttl=128 (request in 437) |
| 202.120.10.1 | 65.10.10.25 | ICMP | 78 | Echo (ping) request id=0x0302, seq=56/14336, ttl=126 (reply in 476) |
| 65.10.10.25 | 202.120.10.1 | ICMP | 74 | Echo (ping) reply id=0x0302, seq=56/14336, ttl=128 (request in 475) |

可以看到，我们成功实现了对应的地址转换，并且源 ip 地址就是我们转换的端口 202.120.10.1，然后目的 ip 地址就是 65.10.10.25

计算机网络实验报告

【遇到的问题】

- (1) 由于是期末考试,老师没有给我们机会来提前预习实验的内容,导致我们没有做好充足的准备,在加上其他的大大小小的问题,让我们的心态有点崩溃,总体做实验的时候太着急,导致犯了很多小错误。
- (2) 我们本次实验还遇到了之前没有遇到的过的硬件问题,连接路由器的线一直接触不良,导致有时候可以输入指令有时候又不可以输入指令,最严重的时候是无法登陆实验界面,导致我们做实验停滞了很久,在助教的帮助下我们一直扶着那根路由线才勉强做完了所有实验。
- (3) 基础知识掌握不牢,因为一开始以为是简单的静态端口地址转换,但是经过冷静思考并且通过查阅实验书教材后才发现原来是要利用端口静态地址转换,需要使用 overload 指令来同时转换多个内部设备的 IP 地址。端口转化 (PAT, Port Address Translation) 通常用于在 网络地址转换 (NAT) 中让多个内网设备共享一个公共 IP 地址访问外网。静态 NAT 是将内网中的每个 IP 地址都映射到一个唯一的外网 IP 地址上。每个内网设备都需要一个独立的外网 IP 地址。如果内网设备较多,使用静态 NAT 会需要大量的公共 IP 地址。例如,如果你的内网有 100 台设备,那么就需要 100 个公共 IP 地址来进行静态 NAT 转换。而动态 NAT 允许内网中的多个 IP 地址共享一组外网 IP 地址。通过 NAT 转换,内网设备会被分配一个公共 IP 地址,但是这个公共 IP 地址是动态分配的,不是固定的。端口转化 (PAT) 解决了静态和动态 NAT 的这些问题,允许多个内网设备共享一个外网 IP 地址进行通信。通过端口转化,多个内网设备可以共享一个公共 IP 地址来访问外网。具体做法是:每个内网设备通过外网 IP 地址发起连接时,路由器会给每个流量分配一个不同的端口号。例如,内网的 192.168.10.10 和 192.168.10.20 可以都通过外网的 202.120.10.1 发起连接,但是它们使用不同的端口号,比如端口 10001 和端口 10002,来区分不同的流量。
- (4) 由于标准的 ACL 号是从 1-99 和 1300-1999,而我们需要使用扩展的 ACL,所以必须使用大于 99 的 ACL 号。