



警

- 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。

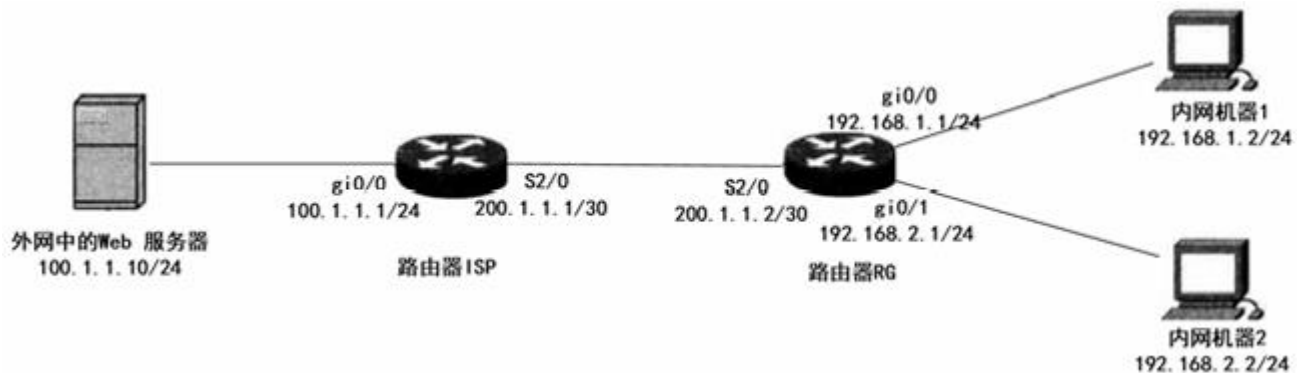
院系	计算机学院	班 级	计科 2 班	组长	林隽哲
学号	21312450	22365043	22302056		
学生	林隽哲	江颢怡	刘彦凤		

NAT 实验

【实验内容】

- (1) 阅读教材 9.1-9.4 章节，即 P304-312，理解并掌握地址转换、静态转换、动态转换和端口地址转换原理和相关配置方法。
- (2) 搭建实验拓扑：按拓扑图正确配置所有机器的 IP 地址、子网掩码、网关。搭建实验拓扑：正确配置 2 台路由器（路由器 ISP 和路由器 RG）的端口。
- (3) 安装 Web 服务器：在外网中的服务器机器上，正确安装 Web 服务器并启动它，使用本机的浏览器访问 `http://localhost:80/` 测试其安装的正确性。
- (4) 配置 NAT，并测试 NAT 转换。

(2) ①实验拓扑搭建如下：



模拟了某一 ISP 为家庭内部网络提供外网连接服务的拓扑。外部网络包括一台 Web 服务器，家庭内部网络包含 2 个子网，分别为 192.168.1.0/24 和 192.168.2.0/24。路由器 ISP 为家庭内网仅提供一个广域网 IP 地址 200.1.1.2/30。现在我们需要在路由器 RG 上配置 NAT 实现内网和外网的连接。

②配置路由器 ISP 和路由器 RG 的端口

路由器 RG 的配置 以及用 `show ip interface brief` 检查路由器的端口 IP 配置情况



```
11-RSR20-1(config)#interface serial 2/0
11-RSR20-1(config-if-Serial 2/0)#ip address 200.1.1.2 255.255.255.0
11-RSR20-1(config-if-Serial 2/0)#interface gigabitethernet 0/1
11-RSR20-1(config-if-GigabitEthernet 0/1)#2.168.1.1 255.255.255.0
11-RSR20-1(config-if-GigabitEthernet 0/1)#abitethernet 0/0
11-RSR20-1(config-if-GigabitEthernet 0/0)#exit
11-RSR20-1(config)#interface gigabitethernet 0/1
11-RSR20-1(config-if-GigabitEthernet 0/1)#2.168.2.1 255.255.255.0
11-RSR20-1(config-if-GigabitEthernet 0/1)#interface gigabitethernet 0/0
11-RSR20-1(config-if-GigabitEthernet 0/0)#2.168.1.1 255.255.255.0
11-RSR20-1(config-if-GigabitEthernet 0/0)#interface serial 2/0
11-RSR20-1(config-if-Serial 2/0)#ip address 200.1.1.2 255.255.255.252
11-RSR20-1(config-if-Serial 2/0)#exit
11-RSR20-1(config)#show ip interface brief
```

Interface	IP-Address(Pri)	IP-Address(Sec)	Status	Pr
Serial 2/0	200.1.1.2/30	no address	up	up
SIC-3G-WCDMA 3/0	no address	no address	up	dc
GigabitEthernet 0/0	192.168.1.1/24	no address	up	up
GigabitEthernet 0/1	192.168.2.1/24	no address	up	up
VLAN 1	no address	no address	up	dc

路由器配置接口 IP 的命令同上 这里省略了 只展示最后配置好的效果

```
11-RSR20-2(config)#show ip interface brief
```

Interface	IP-Address(Pri)	IP-Address(Sec)	Status	Protocol
Serial 2/0	200.1.1.1/30	no address	up	up
Serial 3/0	no address	no address	down	down
GigabitEthernet 0/0	100.1.1.1/24	no address	up	up
GigabitEthernet 0/1	no address	no address	down	down
VLAN 1	no address	no address	up	down

③配置所有机器的 IP 地址、子网掩码、网关

配置内网机器的 IP

Internet 协议版本 4 (TCP/IPv4) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址(O)

☒ 使用下面的 IP 地址(S):

IP 地址(I):

子网掩码(U):

默认网关(D):

☐ 自动获得 DNS 服务器地址(B)

☒ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

备用 DNS 服务器(A):

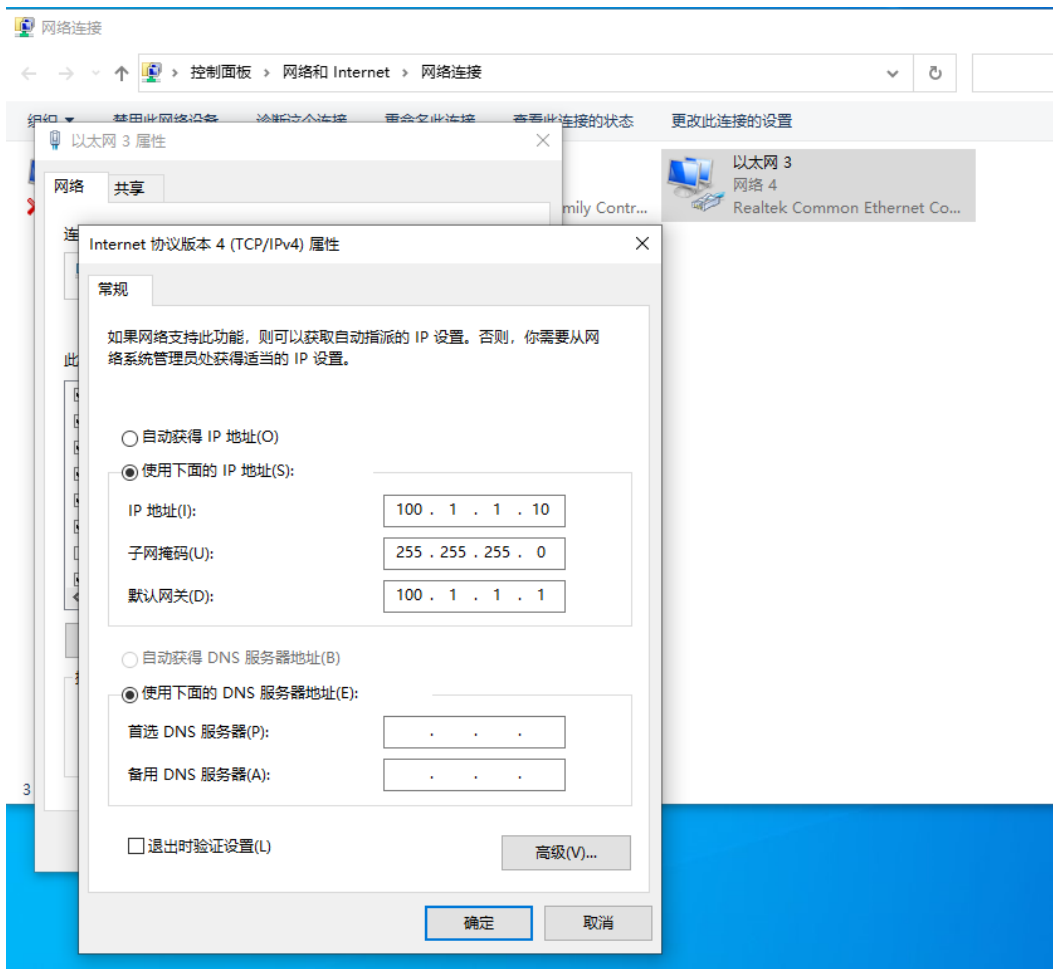
☐ 退出时验证设置(L)

高级(V)...

确定 取消



配置服务器的 IP



(3)安装 Web 服务器:

在外网中的服务器机器上，正确安装 Web 服务器并启动它，使用本机的浏览器访问 <http://localhost:80/> 测试其安装的正确性。

在服务器机器上成功安装并启动



RCMS Home Page x Test Page for Apache Installati x +

127.0.0.1

AN APACHE HAUS DISTRIBUTION

Test Page for Apache Installation

Apache/2.4 OpenSSL

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the web server administrator:



You may now add content to the directory `/htdocs`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, replace the existing `/htdocs/index.html` with one of your own.

If you are new to the Apache server software:


The Apache documentation has not been included with this distribution. You can always view the [documentation](http://documentation.apache.org) at apache.org

You are free to use the powered by Apache image below on an Apache-powered web server. There are a few variations in the `/icons` folder.

This distribution comes with an embedded lua interpreter module. This [script written](#) in lua can be used to test `mod_lua`'s functioning properly.



The Apache Haus is not affiliated with, or endorsed by, the Apache Software Foundation. Apache HTTP Server, Apache, and the Apache feather logo are trademarks of The Apache Software Foundation.



(4)配置 RG 的 NAT，并测试 NAT 转换。

配置步骤：

- (1) 创建访问控制列表，允许内网地址访问外部网络



```
RG Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

```
RG Router(config)# access-list 2 permit 192.168.2.0 0.0.0.255
```

(2) 将内部接口标记为内部接口、将外部接口标记为外部接口

```
RG Router(config)# interface gigabitethernet 0/0
```

```
RG Router(config-if)# ip nat inside
```

```
RG Router(config)# interface gigabitethernet 0/1
```

```
RG Router(config-if)# ip nat inside
```

```
RG Router(config)# interface serial 2/0
```

```
RG Router(config-if)# ip nat outside
```

(3) 配置 NAT 转换规则，将内网 IP 地址分别转换为外部 IP 地址。

```
RG Router(config)# ip nat inside source list 1 interface serial 2/0 overload
```

```
RG Router(config)# ip nat inside source list 2 interface serial 2/0 overload
```

(4) 配置静态路由或默认路由，令路由器 RG 可以转发到其他外网的数据包

```
RG Router(config)# ip route 0.0.0.0 0.0.0.0 serial 2/0
```

配置展示：

配置 RG 的 NAT

```
11-RSR20-1(config)#interface gigabitethernet 0/0
11-RSR20-1(config-if-GigabitEthernet 0/0)#ip nat inside
11-RSR20-1(config-if-GigabitEthernet 0/0)#exit
11-RSR20-1(config)#interface gigabitethernet 0/1
11-RSR20-1(config-if-GigabitEthernet 0/1)#ip nat inside
11-RSR20-1(config-if-GigabitEthernet 0/1)#exit
11-RSR20-1(config)#interface serial 2/0
11-RSR20-1(config-if-Serial 2/0)#ip nat outside
11-RSR20-1(config-if-Serial 2/0)#exit
11-RSR20-1(config)#ip nat inside source list 1 interface serial 2/0 overload
11-RSR20-1(config)#ip nat inside source list 2 interface serial 2/0 overload
11-RSR20-1(config)#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
```

- 配置中的 overload 关键字表明 NAT 将使用端口号来区分来自不同内网主机的会话。
 - 在这种情况下，多个内网主机的私有 IP 地址可以共享同一个公有 IP 地址（由接口 serial 2/0 提供的 IP），但每个会话会通过唯一的源端口号加以区分。
- 所以此时实验用的 NAT 转换类型是端口地址转换

(5) 实验结果展示

用内网机器成功 ping 通外网的 web 服务器



```
PS C:\Users\D502> ping 100.1.1.10

正在 Ping 100.1.1.10 具有 32 字节的数据:
来自 100.1.1.10 的回复: 字节=32 时间=38ms TTL=126
来自 100.1.1.10 的回复: 字节=32 时间=38ms TTL=126

100.1.1.10 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 38ms, 最长 = 38ms, 平均 = 38ms
Control-C
PS C:\Users\D502>
```

且用 show ip nat translations 可以查看是如何进行 NAT 地址转化的: 可以看到来自 192.168.1.2 的流量变成了 global 的 200.1.1.2 的流量

```
11-RSR20-1(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0
11-RSR20-1(config)#show ip nat translations
Pro Inside global      Inside local    Outside local   Outside global
tcp 200.1.1.2:52736    192.168.1.2:52736 100.1.1.10:80   100.1.1.10:80
tcp 200.1.1.2:52741    192.168.1.2:52741 172.16.26.3:7680 172.16.26.3:7680
tcp 200.1.1.2:52742    192.168.1.2:52742 172.16.4.1:7680 172.16.4.1:7680
tcp 200.1.1.2:52743    192.168.1.2:52743 172.16.7.1:7680 172.16.7.1:7680
tcp 200.1.1.2:52744    192.168.1.2:52744 172.16.15.2:7680 172.16.15.2:7680
```

成功在内网机器上 (192.168.1.2) 访问服务器的主页

Test Page for Apache Installation

Apache/2.4 OpenSSL

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the web server administrator:

You may now add content to the directory /htdocs. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, replace the existing /htdocs/index.html with one of your own.

If you are new to the Apache server software:

The Apache documentation has not been included with this distribution. You can always view the [documentation](http://documentation.apache.org) at apache.org

You are free to use the powered by Apache image below on an Apache-powered web server. There are a few variations in the /icons folder.

This distribution comes with an embedded lua interpreter module. This [script written](#) in lua can be used to test mod_lua's functioning properly.

t 协议版本 4 (TCP/IPv4) 属性

网络支持此功能, 则可以获取自动分配的 IP 设置。否则, 你需要从网
统管理员处获得适当的 IP 设置。

自动获得 IP 地址(O)
使用下面的 IP 地址(S):

地址(I): 192 . 168 . 1 . 2

子网掩码(U): 255 . 255 . 255 . 0

默认网关(D): 192 . 168 . 1 . 1

自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): . . .

备用 DNS 服务器(A): . . .

☐ 退出时验证设置(L) 高级(V)...

确定 取消



反过来想用外网的 web 服务器 ping 通内网机器 不成功 因为只在路由器 RG 配置了左向的流量 右向的流量没有办法进行 NAT 转换

```
C:\Users\D502>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

用 Wireshark 抓包的结果 可以看到双方通过 TCP 成功建立连接 且应用层协议是 HTTP 因为使用网页访问了 web 服务器 以及也有使用 ping 验证连通性的 ICMP 数据包

ip.src==192.168.1.2 &&ip.dst==100.1.1.10						
No.	Time	Source	Destination	Protocol	Length	Info
2	2.624190	192.168.1.2	100.1.1.10	TCP	66	52749 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
3	2.628627	192.168.1.2	100.1.1.10	TCP	66	52750 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
5	2.851435	192.168.1.2	100.1.1.10	TCP	54	52749 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
6	2.851850	192.168.1.2	100.1.1.10	HTTP	592	GET / HTTP/1.1
8	2.859057	192.168.1.2	100.1.1.10	TCP	54	52750 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
10	3.170298	192.168.1.2	100.1.1.10	TCP	54	52749 → 80 [ACK] Seq=539 Ack=291 Win=262400 Len=0
12	8.048231	192.168.1.2	100.1.1.10	TCP	54	52749 → 80 [ACK] Seq=539 Ack=292 Win=262400 Len=0
36	25.724589	192.168.1.2	100.1.1.10	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128
39	26.744857	192.168.1.2	100.1.1.10	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128
41	27.758767	192.168.1.2	100.1.1.10	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128
43	28.769927	192.168.1.2	100.1.1.10	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128
53	47.861633	192.168.1.2	100.1.1.10	TCP	55	[TCP Keep-Alive] 52750 → 80 [ACK] Seq=0 Ack=1 Win=262656
56	53.053320	192.168.1.2	100.1.1.10	TCP	55	[TCP Keep-Alive] 52749 → 80 [ACK] Seq=538 Ack=292 Win=2

(6) 实验总结与反思

实验总结--NAT 原理:

1.地址转换 (NAT, Network Address Translation) 是一种将私有网络地址转换为公有网络地址的技术,用于解决 IPv4 地址不足和网络安全问题。

出站通信: 当内网设备访问外网时, NAT 将私有 IP 转换为公有 IP, 并记录地址映射 (通常包括源端口号)。

入站通信: 当外网设备向 NAT 映射的公有地址发送数据时, NAT 将其转换为对应的私有 IP 地址。

2. NAT 的主要类型

本次实验用到的是静态地址转换。

2.1 静态地址转换 (Static NAT)

原理:

- 静态 NAT 实现一对一的地址映射, 每个私有 IP 地址固定对应一个公有 IP 地址。



```
# 将内网地址 192.168.1.10 静态映射到公有地址 203.0.113.10
ip nat inside source static 192.168.1.10 203.0.113.10

# 指定 NAT 的内外接口
interface GigabitEthernet0/0
  ip nat inside
interface GigabitEthernet0/1
  ip nat outside
```

2.2 动态地址转换 (Dynamic NAT)

原理:

- 动态 NAT 实现多对多的地址转换，使用一个公网地址池动态分配地址。
- 当内网主机需要访问外网时，从地址池中分配一个未使用的公有地址。

```
# 定义公网地址池
ip nat pool PUBLIC_POOL 203.0.113.1 203.0.113.10 netmask 255.255.255.0

# 配置内网到公网的地址转换规则
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 pool PUBLIC_POOL

# 指定 NAT 的内外接口
interface GigabitEthernet0/0
  ip nat inside
interface GigabitEthernet0/1
  ip nat outside
```

2.3 端口地址转换 (PAT, Port Address Translation)

原理:

- PAT 是动态 NAT 的扩展，实现多对一的地址转换。
- 多个内网主机可以通过同一个公有 IP 地址访问外网，利用端口号区分不同的会话。










```
# 配置 PAT，使用接口的公有地址
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface GigabitEthernet0/1 overload

# 指定 NAT 的内外接口
interface GigabitEthernet0/0
ip nat inside
interface GigabitEthernet0/1
ip nat outside
```

实验反思

1. 在没有退出某个路由器或者交换机时不能直接把校园网卡拔掉 因为之后进入的时候就会一直显示占用状态 解决措施就只能一键清 所有相关配置在敲一遍 如下图这次试验路由器 1 (11-RSR20-1) 就因为这个疏忽导致卡死。

欢迎来到中山大学东校区网络实验室

实验注意事项：每个图标分别对应不同的异步口， 表示二层交换机、 表示三层交换机、 表示核心交换机、 表示路由器、 表示防火墙、 表示不可识别的设备（没有配置）、 表示该线路已被禁止使用。点击某个图标，便可以弹出telnet客户端。如果异步口已被反向telnet占用或者被禁止使用，则文字变灰，不显示为超链接，不可点击。



2. 刚开始配置完后在内网机器上我们想要 ping 通服务器却失败了 于是借助中间节点一路 ping 过去 检查到底是哪个中间环节出了问题



```
Windows PowerShell
PS C:\Users\D502> ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=5ms TTL=64

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 5ms, 最长 = 9ms, 平均 = 7ms
Control-C
PS C:\Users\D502> ping 200.1.1.2

正在 Ping 200.1.1.2 具有 32 字节的数据:
来自 200.1.1.2 的回复: 字节=32 时间=5ms TTL=64
来自 200.1.1.2 的回复: 字节=32 时间=4ms TTL=64
来自 200.1.1.2 的回复: 字节=32 时间=4ms TTL=64

200.1.1.2 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 4ms, 最长 = 5ms, 平均 = 4ms
Control-C
PS C:\Users\D502> ping 200.1.1.1

正在 Ping 200.1.1.1 具有 32 字节的数据:
来自 200.1.1.1 的回复: 字节=32 时间=39ms TTL=63
来自 200.1.1.1 的回复: 字节=32 时间=44ms TTL=63

200.1.1.1 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 39ms, 最长 = 44ms, 平均 = 41ms
Control-C
PS C:\Users\D502> ping 100.1.1.1

正在 Ping 100.1.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 无法访问目标网。
来自 192.168.1.1 的回复: 无法访问目标网。

100.1.1.1 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
Control-C
PS C:\Users\D502>
```

最后发现是 ISP 路由器的两个接口之间流量无法传递 然后发现 ISP 路由器配置有点问题 因为默认是拒绝所有流量的 后正确配置成功 ping 通

学号	学生	自评分
21312450	林隽哲	100
22365043	江颢怡	100
22302056	刘彦凤	100