



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	计科_1_班	组长	郝裕玮
学号	18329015	18325071	19335153		
学生	郝裕玮	张闯	马淙升		
实验分工					
郝裕玮	张闯	马淙升			
共同完成实验和实验报告	共同完成实验和实验报告	共同完成实验和实验报告			

【实验题目】配置 TCP 负载分配。

【实验目的】

配置网络地址变换，使用一个单地址实现两台 WEB 服务器负载平衡。

【实验内容】

1. 完成实验 9-4 (P314)，注意步骤 0 和步骤 6。
2. 在进行验证时如果不用 Web，而改用 Telnet 或远程桌面连接，同样能验证吗？
3. 请回答 P317 的实验思考。

【实验要求】

重要信息需给出截图，注意实验步骤的前后对比。

【实验记录】(如有实验拓扑请自行画出)

1. 完成实验 9-4 (P314)，注意步骤 0 和步骤 6。

【实验拓扑】

本实验的拓扑结构如图 9-12 所示。选择 192.168.1.0/24 作为私有地址，采用 NAT 技术处理和外部网络的连接。内部有 2 台 Web 服务器，IP 地址分别为 192.168.1.5 和 192.168.1.6，虚拟服务器地址为 50.1.1.10。

【实验设备】

路由器 2 台，交换机 1 台，计算机 1 台，Web 服务器 2 台。

【实验步骤】

分析: 根据要求，可在路由器上定义内网与外网端口，利用 TCP 负载均衡实现 2 台服务器负载均衡。为此，必须搭建好服务器端的 Web 应用服务，可以是 Windows Server 自带的 IIS 服务或 Apache 服务，也可以是其他 Web 服务器软件。否则验证时 sh ip nat translations、



debug ip nat 均无法显示预期的结果。

步骤 1:

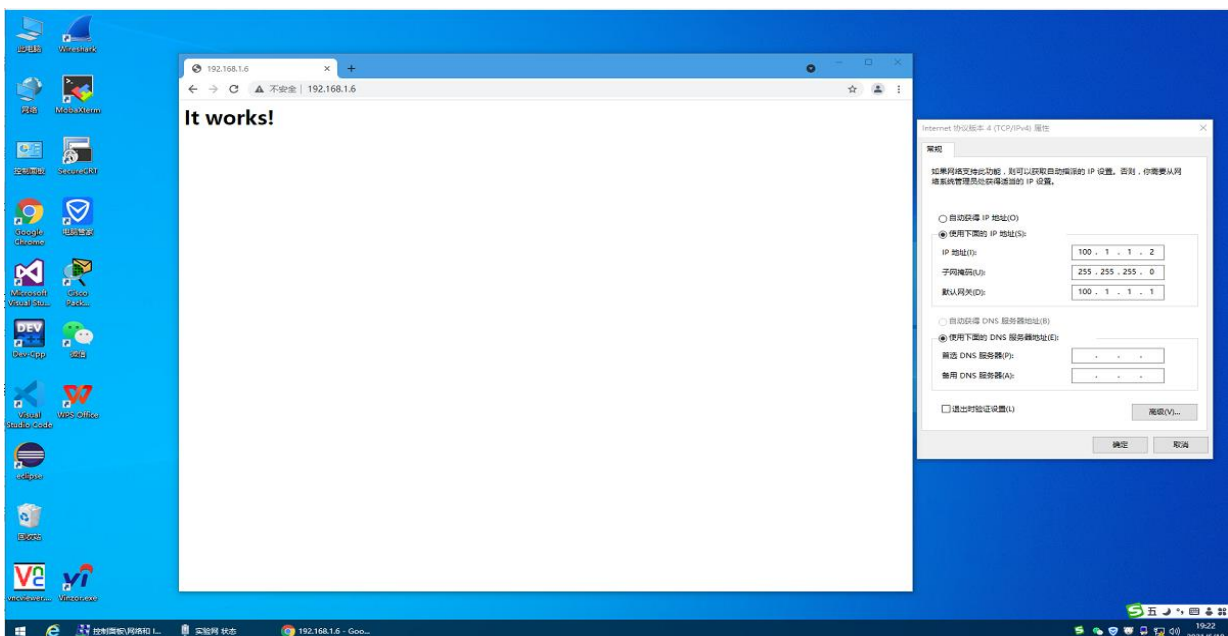
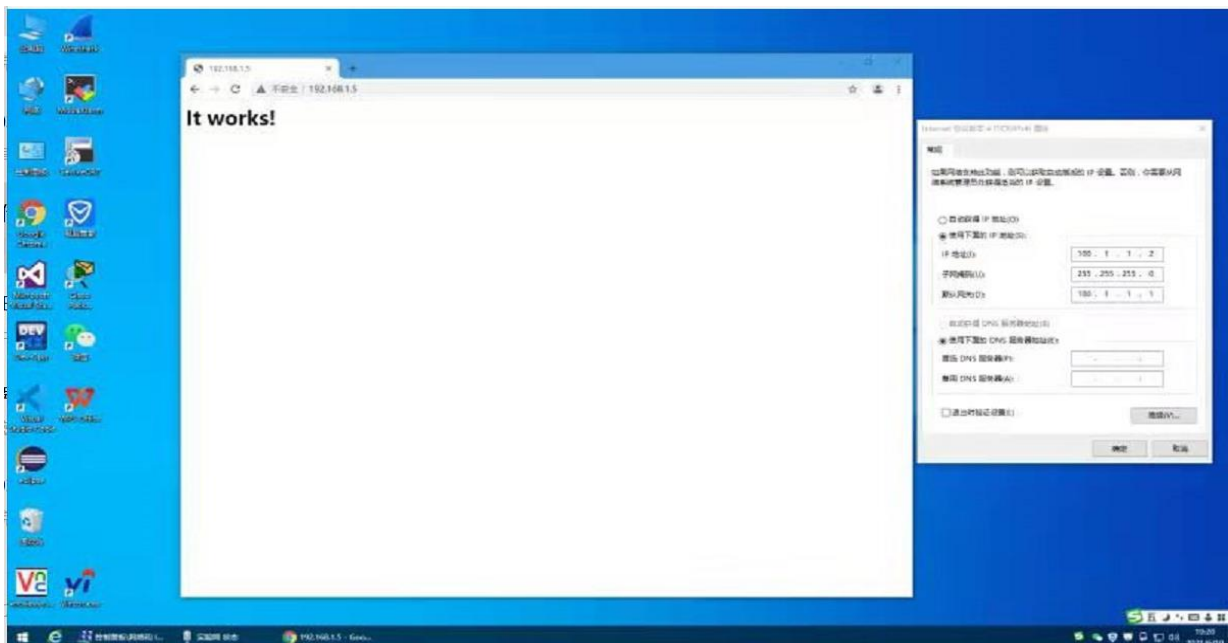
(1) 搭建 Web 服务器。

配置 Apache server 到官网下载 Apache HTTP server, 解压至电脑根目录下。打开 conf 文件夹, 打开 httpd.conf 文件, 打开 HTTP 服务 (查找 ServerName, 删去前面的注释), 查看端口, 即 listen 行, 默认端口为 80, 如有需要可以修改。

打开终端, 进入 Apache 下的 bin 目录, 执行 `httpd.exe -k install -n "Apache24"`, 安装 HTTP 服务。

最后运行 bin 下的 `ApacheMonitor.exe` 可执行文件, 即可运行 Web 服务器。

(2) 在完成步骤 2 后, 验证整个网络的连通性(必须确保连通)。





由上图易知网络连通性正常。

(3) 查看 NAT 表: #show ip nat translations (由于微信截图的时效性导致截图模糊, 但是该步显示结果为空, 所以影响不大)。

```
S-RS20-2(config)#show ip nat translation
Pro inside global      inside local      outside global
S-RS20-2(config)#
```

结果为空的原因: 尚未配置 NAT, 所以 NAT 表上的所有信息均为空。

步骤 2: 在路由器上配置 IP 地址和路由。

路由器 RG 的设置如下。

```
RG(config)#interface serial 2/0
RG(config-if) #ip address 200.1.1.2 255.255.255.252
RG(config)#interface gigabitethernet 0/1
RG(config-if) #ip address 192.168.1.1 255.255.255.0
RG(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0
```

请自行写出路由器 ISP 的设置。

由于微信截图的时效性导致截图模糊, 所以只好采用文字形式体现:

```
interface serial 2/0
ip address 200.1.1.1 255.255.255.252
exit
interface gi 0/1
ip address 100.1.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 serial 2/0
```

补充说明: 由于本次是微信截图且事后没有来得及保存原图, 导致很多图片较为模糊, 所以步骤 3-6 的对应代码图不再贴出, 在这里向助教表示歉意! 下次会选择用 U 盘保存截图, 不再出现这样的低级失误。

步骤 3: 通过一个虚拟主机许可声明定义一个扩展的 IP 访问列表。

```
RG(config)#access-list 150 permit ip any host 50.1.1.10
```

步骤 4: 为真实主机定义一个 IP NAT 池, 确保其为旋转式池。

```
RG (config) # ip nat pool webserver 192.168.1.5 192.168.1.6 prefix-length 24
type rotary
```

步骤 5: 定义访问列表与真实主机池之间的映射。

```
RG(config)#ip nat inside destination list 150 pool webserver
```

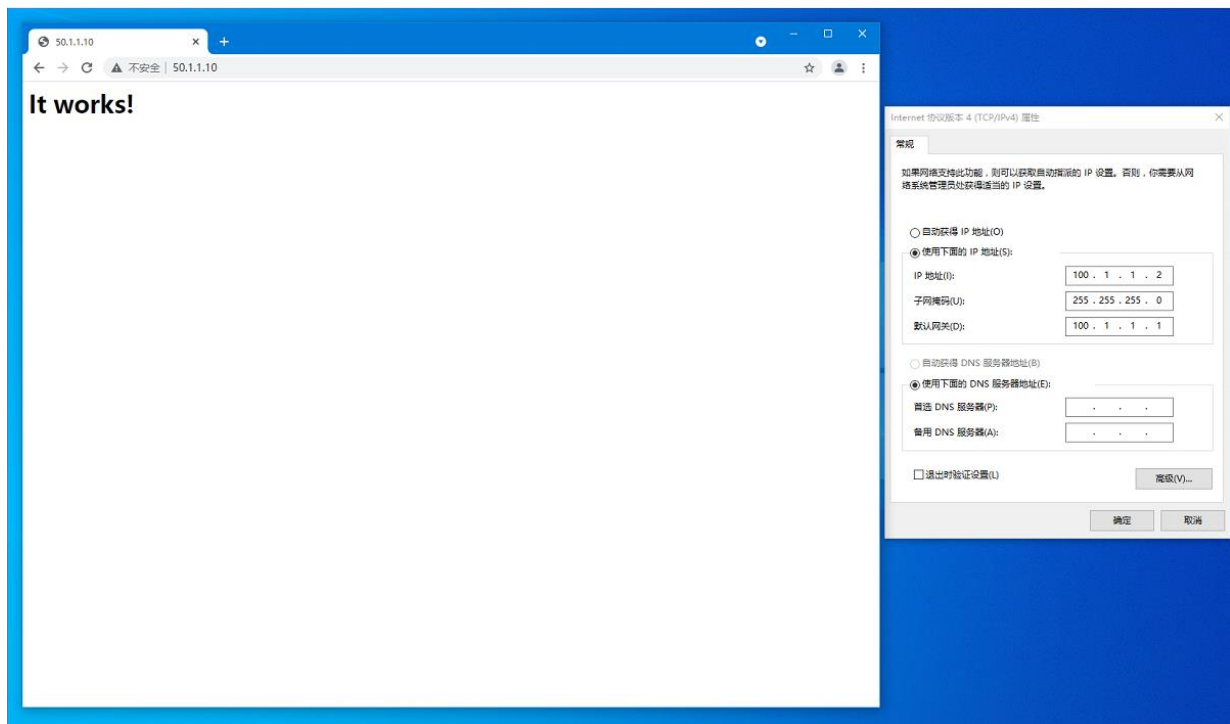
步骤 6: 指定一个内部端口和一个外部端口。

```
RG(config)#interface serial 2/0
RG(config-if)#ip nat outside
RG(config)#interface gigabitethernet 0/1
RG(config-if)#ip nat inside
```



步骤 7: 验证测试。

(1) 在主机 A 上用浏览器打开 `http://50.1.1.10`。



由上图可知，实验结果符合预期。

(2) 查看地址翻译的过程：`#debug ip nat`。

```
10-RSR20-2#debug ip nat
```

输入指令后无结果显示。

(3) 查看 NAT 表：`#show ip nat translations`;说明表中端口号有什么作用？

```
10-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 100.1.1.2:1742     100.1.1.2:1742   50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1734     100.1.1.2:1734   50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1736     100.1.1.2:1736   50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1741     100.1.1.2:1741   50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1743     100.1.1.2:1743   50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1744     100.1.1.2:1744   50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1735     100.1.1.2:1735   50.1.1.10:80      192.168.1.5:80
```

表中端口号作用: 当 NAT 路由器接收到该应答数据包后, 使用内部本地地址和端口号, 以及外部地址和端口号作为关键字在 NAT 表中进行查找。找到后把应答包中的源地址转换为虚拟主机地址(内部全局地址)进行替换(目的地址不变), 继续转发应答数据包, 直至外部网络用户收到应答数据包。

(4) 在 Web 服务器上捕获数据包, 查看发送过程中报文的 IP 地址转换情况, 并作出合理解释。

```
100.1.1.2      192.168.1.5      TCP      62 1598 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
192.168.1.5    100.1.1.2        TCP      62 80 → 1598 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM
100.1.1.2      192.168.1.5      HTTP     452 GET / HTTP/1.1
192.168.1.5    100.1.1.2        HTTP     920 HTTP/1.1 200 OK (text/html)
100.1.1.2      192.168.1.5      TCP      60 1598 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
100.1.1.2      192.168.1.5      TCP      60 1597 → 80 [ACK] Seq=797 Ack=1733 Win=64240 Len=0
```

具体解释: ①外部网络用户主机(IP 地址为 100.1.1.2)发起与虚拟主机(内部全局地址



50.1.1.10 的连接。此时数据包中的源地址为外部全局地址(100.1.1.2), 目的地址为虚拟主机地址(50.1.1.10)。

②当路由器接收到连接请求数据包时, 创建一个内部网络中真实主机(192.168.1.5)进行关联的新的 NAT 转换条目。

③NAT 路由器把连接请求数据包中的目的地址用真实主机的本地地址进行替换(源地址不变), 然后继续发送连接请求数据包。

④内部网络中真实主机(192.168.1.5)接收到该连接请求数据包, 并发出一个应答数据包。应答数据包中的源地址是内部真实主机本地地址(192.168.1.5), 目的地址为外部网络主机 B 的 IP 地址(100.1.1.2)。

⑤当 NAT 路由器接收到该应答数据包后, 使用内部本地地址和端口号, 以及外部地址和端口号作为关键字在 NAT 表中进行查找。找到后把应答包中的源地址转换为虚拟主机地址(内部全局地址)进行替换(目的地址不变), 继续转发应答数据包, 直至外部网络用户收到应答数据包。

NAT 路由器一直重复这样的转换过程, 只是下一次转换时虚拟主机所对应的内部主机本地地址可能不是 192.168.1.5, 也有可能是 192.168.1.6。显然这是一个动态 NAT 转换过程。

(5) 在 192.168.1.5 和 192.168.1.6 主机上建立用户名和口令。建立方法是右击“计算机”图标, 在弹出的快捷菜单中选择“管理”选项, 在“计算机管理”窗口中选择“本地用户和组”→“用户”选项, 右击后在弹出的快捷菜单中选择“新建用户”选项。分别采用 Telnet 和远程桌面连接(设置方法是右击“计算机”图标, 在弹出的快捷菜单中选择“属性”选项, 在“系统属性”对话框中选择“远程”, 选择“允许用户远程到此计算机”复选框)的方法代替(1), 重做(2)~(4)的内容。

建立的用户必须有属于管理员的权限(或直接用 administrator 用户登录)。

答: 该题可详见第 2 题, 且因为实验室电脑不是家庭版, 没有远程桌面连接, 所以最终只能进行 Telnet 实验。

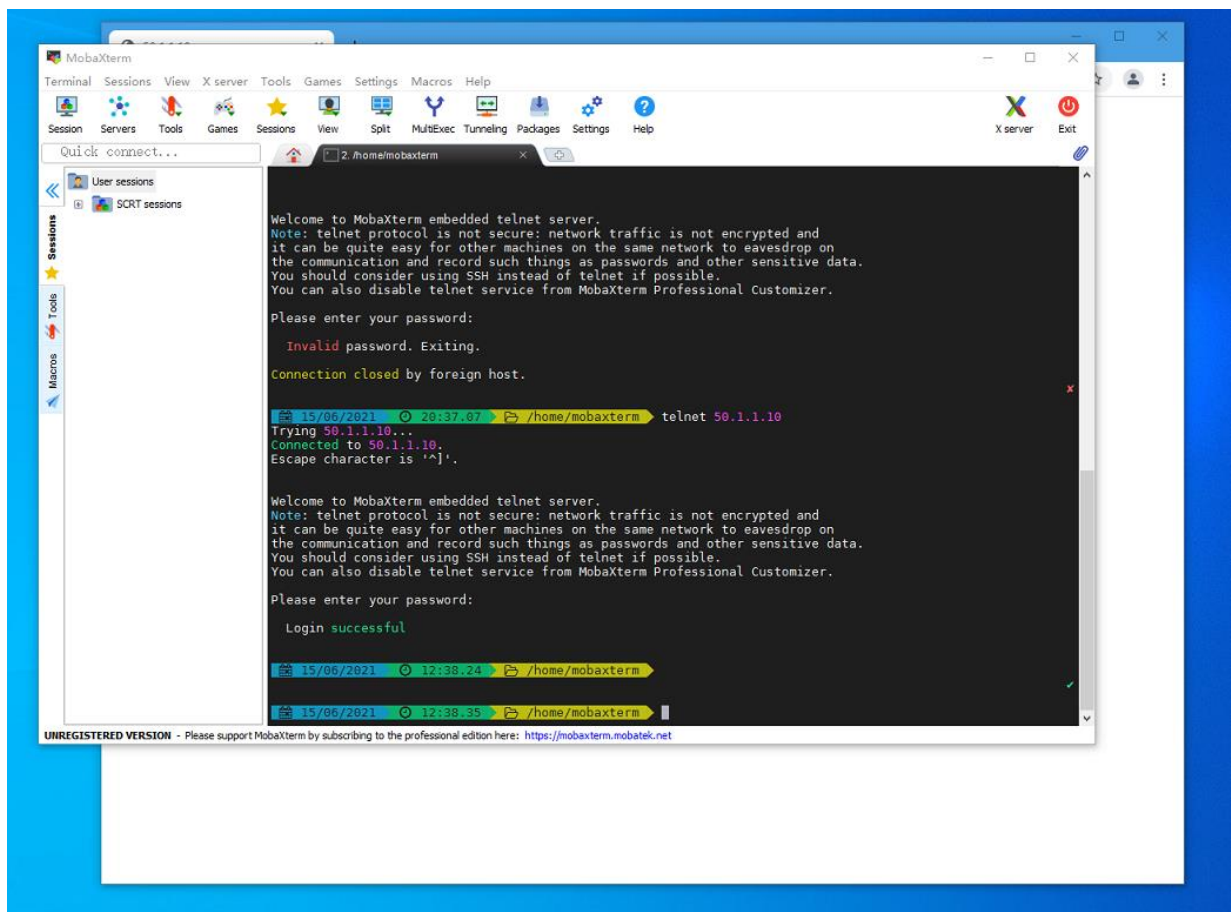


2.在进行验证时如果不用 Web，而改用 Telnet 或远程桌面连接，同样能验证吗？

由于沟通和操作原因，未能保存下完整的实验结果，针对本题我们进行口头阐述当时进行的实验步骤及其实验结果，给助教带来不便，非常抱歉！

因为配置无需更改，所以我们重新进行步骤 7 的（1）—（4）的验证：

（1）在主机 A 上输入命令 telnet 50.1.1.10:



由上图可知，实验结果符合预期。

（2）查看地址翻译的过程:#debug ip nat.

```
10-RSR20-2#debug ip nat
```

输入指令后无结果显示。

（3）查看 NAT 表:#show ip nat translations;说明表中端口号有什么作用？

由于操作失误，本题结果未能保存下来，但实际结果和 Web 的结果并无太大差异，只是端口号不再是 HTTP 默认的 80 端口。

表中端口号作用:当 NAT 路由器接收到该应答数据包后,使用内部本地地址和端口号,以及外部地址和端口号作为关键字在 NAT 表中进行查找。找到后把应答包中的源地址转换为虚拟主机地址(内部全局地址)进行替换(目的地址不变),继续转发应答数据包,直至



外部网络用户收到应答数据包。

(4) 在 Web 服务器上捕获数据包, 查看发送过程中报文的 IP 地址转换情况, 并作出合理解释。

在访问的同时进行抓包:

409 21.050213	50.1.1.10	100.1.1.2	TCP	70 23 → 1924 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PER
410 21.050204	100.1.1.2	50.1.1.10	TCP	54 1924 → 23 [ACK] Seq=1 Ack=1 Win=65536 Len=0
411 21.050045	100.1.1.2	50.1.1.10	TELNET	81 Telnet Data ...

由上图可知成功抓到 telnet 报文。

转换情况和解释可参考步骤 7 (4)。

3.请回答 P317 的实验思考。

(1) 实验时不能简单地从主机 A ping 50.1.1.10 的方式进行验证, 这是什么原因?

答: NAT TCP 负载均衡只适用于 TCP 连接, 对于非 TCP 连接请求, NAT 进程将不会对其进行转换。又因为 ping 发送的是 ICMP 包, 所以无法通过 ping 的方式来验证。

(2) TCP 负载均衡与访问量有关吗? 请设计有效方法, 该方法可以考察到负载均衡的效果, 并总结其规律性。

答: TCP 负载均衡与访问量无关。当我们利用 IP 地址为 100.1.1.2 的主机 A 反复访问 50.1.1.10 时, 观察 NAT 表, 观察到一直是访问的 192.168.1.5 这台主机, 从我们关掉 192.168.1.5 的服务器后, 主机 A 无法访问 50.1.1.10 这个现象也可以验证。在我们修改主机 A 的 IP 为 100.1.1.3 后, 观察 NAT 表可以看出访问的是 192.168.1.6 的服务器, 可以看出负载均衡成功实现, 但和访问量没有关系。经其他同学提出, 负载均衡是通过对 IP 地址哈希的方式实现的。

(3) 本实验采用的技术有什么现实意义?

答: ①当访问服务器的主机特别多时, 通过 NAT 构造虚拟服务器, 并运用轮转技术实现负载均衡, 可以分担服务器的压力, 保证服务器的性能;

②运用 NAT 技术, 外部主机不能直接访问到内部服务器, 一定程度上保证了服务器的安全性。

学号	学生	自评分
18329015	郝裕玮	95
18325071	张闯	95
19335153	马淙升	95