



警示

- 1.
2. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
3. 当次小组成员成绩只计学号、姓名登录在下表中的。
4. 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。
5. 实验报告文件以 PDF 格式提交。

院系	计算机学院	班 级	人工智能与大数据	组长	陈欣宇
学号	21307347	21307350	21307100		
学生	陈欣宇	高宇	陈华清		
实验分工					
陈欣宇	搭建其中一台 Web 服务器,配置路由器,共同完成实验及报告		陈华清	完成部分路由器配置和主机的配置,共同完成实验任务与报告	
高宇	完成部分路由器配置和一台 Web 服务器搭建,共同完成实验报告				

【实验题目】NAT 实验

【实验目的】理解 NAT 的功能、应用及配置方法。

【实验内容】

- (1) 完成实验教程第九章实验 9-4 的实验，回答实验提出的问题及实验思考。(P314)
- (2) 请提前了解 Web 应用服务的简易搭建方法。
- (3) (选做) 如果希望实现服务器(例如:TFTP, DHCP, BOOTP, DNS)在 UDP 的端口映射, 应该如何实现?请查阅网络资料, 并尝试实现。

【实验要求】

一些重要信息信息需给出截图，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,)

实验 9-4:

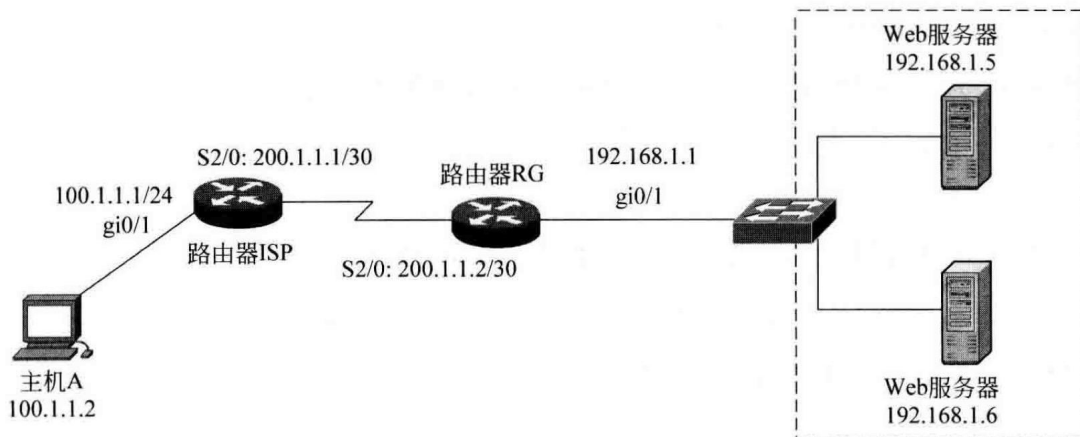
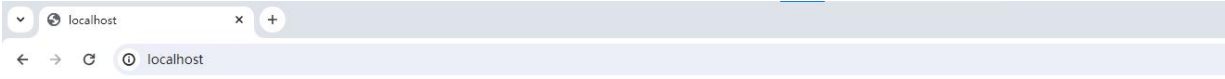


图 9-12 TCP 负载均衡实验拓扑

步骤 1:

(1) 搭建 Web 服务器: 参考 ACL 实验 WWW 服务器的搭建

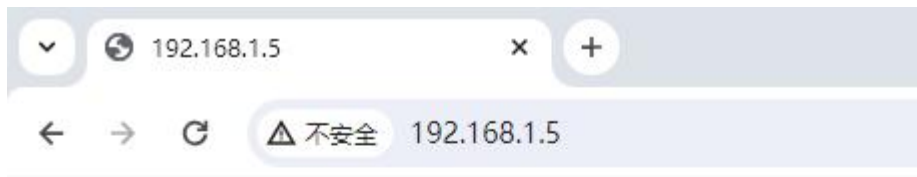
结果: 搭建成功



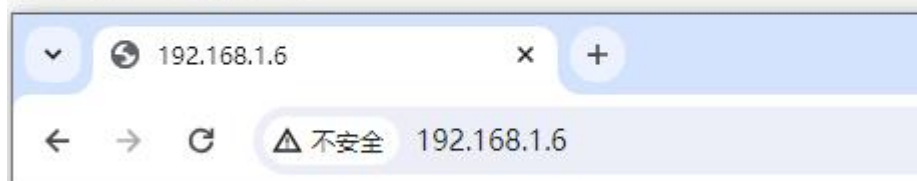
It works!



(2) 完成步骤 2 后，测试网络连通性(必须确保连通)
网络连通，PCA 能够访问两台服务器



It works!



It works!

(3) 查看 NAT 表: #show ip nat translations

```
26-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
```

未配置 NAT，表信息为空。

步骤 2: 在路由器上配置 IP 地址和路由

路由器 RG 设置:

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*  0.0.0.0/0 is directly connected, Serial 2/0
C   192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C   192.168.1.1/32 is local host.
C   200.1.1.0/30 is directly connected, Serial 2/0
C   200.1.1.2/32 is local host.
```



路由器 ISP 设置:

```
interface serial 2/0
ip address 200.1.1.1 255.255.255.252
interface gigabitethernet 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
```

```
26-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 0.0.0.0 to network 0.0.0.0
S*  0.0.0.0/0 is directly connected, Serial 2/0
C   100.1.1.0/24 is directly connected, GigabitEthernet 0/1
C   100.1.1.1/32 is local host.
C   200.1.1.0/30 is directly connected, Serial 2/0
C   200.1.1.1/32 is local host.
```

步骤 3: 通过虚拟主机许可申明定义一个扩展的 IP 访问列表

步骤 4: 为真实主机定义一个 iP NAT 池, 确保其为旋转式池

步骤 5: 定义访问列表与真实主机池之间的映射

步骤 6: 指定一个内部端口和一个外部端口

步骤 7: 验证测试

(1) 在主机 A 打开 <http://50.1.1.10>

可以访问 web 服务器 50.1.1.10

← → ↻ ⚠ 不安全 | 50.1.1.10

It works!

(2) 查看地址翻译过程: #debug ip nat

截图见第 (3) 问, 无 debug 信息

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

```
26-RSR20-2#debug ip nat
26-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 100.1.1.2:49486    100.1.1.2:49486  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:49484    100.1.1.2:49484  50.1.1.10:80      192.168.1.5:80
```

表中端口号用于端口多路复用, 使内部网络的所有主机均可共享一个合法外部 IP 地址, 最大限度节约 IP 地址资源, 同时可隐藏网络内部的所有主机, 有效避免来自 Internet 的攻击。

(4) 在 Web 服务器上捕获数据包, 查看发送过程中报文的 IP 地址转换过程, 并作出合理解释
主机上抓包:



*以太网 3

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
664	22.308396	100.1.1.2	50.1.1.10	HTTP	452	GET /favicon.ico HTTP/1.1
754	25.076437	50.1.1.10	100.1.1.2	HTTP	470	HTTP/1.1 404 Not Found (text/html)

在服务器上抓包：

http

No.	Time	Source	Destination	Protocol	Length	Info
32	10.255537	100.1.1.2	192.168.1.5	HTTP	452	GET /favicon.ico HTTP/1.1
33	10.258279	192.168.1.5	100.1.1.2	HTTP	466	HTTP/1.1 404 Not Found (text/html)

可见主机传过去访问地址为 50.1.1.10 在经过路由器后被改变为选择服务器的地址 192.18.1.5

(5) 在 192.168.1.5 和 192.168.1.6 主机上建立用户名和口令。分别采用 Telnet 和远程桌面连接的方法代替方法(1)，重做(2)~(4)的内容。

Telnet 连接：

```
04/12/2023 18:15.14 /home/mobaxterm telnet 50.1.1.10
Trying 50.1.1.10 ...
Connected to 50.1.1.10.
Escape character is '^]'.

Welcome to MobaXterm embedded telnet server.
Note: telnet protocol is not secure: network traffic is not encrypted and
it can be quite easy for other machines on the same network to eavesdrop on
the communication and record such things as passwords and other sensitive data.
You should consider using SSH instead of telnet if possible.
You can also disable telnet service from MobaXterm Professional Customizer.

Please enter your password:

Login successful
```

成功抓到 TELNET 数据包，此处只截取了部分服务器的包，实际分析仍经历了地址改变的过程

243	35.989322	100.1.1.2	192.168.1.5	TCP	64	54461 → 23 [ACK] Seq=1 Ack=1 Win=262656 Len=0
244	35.989985	192.168.1.5	100.1.1.2	TELNET	66	Telnet Data ...
245	35.998853	100.1.1.2	192.168.1.5	TELNET	85	Telnet Data ...
246	36.040929	192.168.1.5	100.1.1.2	TCP	54	23 → 54461 [ACK] Seq=13 Ack=28 Win=262656 Len=0

#show ip nat translations 如下：增加了访问 50.1.1.10 的 23 端口号，对应 telnet 连接

```
26-RSR20-2#debug ip nat
26-RSR20-2#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	100.1.1.2:54508	100.1.1.2:54508	50.1.1.10:80	192.168.1.5:80
tcp	100.1.1.2:54507	100.1.1.2:54507	50.1.1.10:80	192.168.1.5:80
tcp	100.1.1.2:54461	100.1.1.2:54461	50.1.1.10:23	192.168.1.5:23

远程桌面连接并在远程桌面进行抓包操作：抓取到 TLSv1.2 的包，同样只截取了一部分，实验中包传递过程同样发生了地址的转变。



50.1.1.10 - 远程桌面连接

正在捕获 以太网 3

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: ... <Ctrl-L>/>

No.	Time	Source	Destination	Protocol	Length	Info
7868	152.278758	192.168.1.5	100.1.1.2	TCP	54	3389 → 53144 [ACK]
7869	152.279565	192.168.1.5	172.16.5.2	TCP	66	[TCP Retransmission]
7870	152.294435	200.1.1.1	192.168.1.5	ICMP	74	Redirect
7871	152.301821	192.168.1.1	192.168.1.5	ICMP	74	Redirect
7872	152.314034	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data
7873	152.322189	200.1.1.1	192.168.1.5	ICMP	74	Redirect
7874	152.329689	192.168.1.1	192.168.1.5	ICMP	74	Redirect
7875	152.341741	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data
7876	152.341816	192.168.1.5	100.1.1.2	TCP	54	3389 → 53144 [ACK]
7877	152.364839	200.1.1.1	192.168.1.5	ICMP	74	Redirect
7878	152.372810	192.168.1.1	192.168.1.5	ICMP	74	Redirect
7879	152.385222	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data
7880	152.420831	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data
7881	152.420871	192.168.1.5	100.1.1.2	TCP	54	3389 → 53144 [ACK]
7882	152.447999	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data
7883	152.474535	100.1.1.2	192.168.1.5	TLSv1.2	101	Application Data
7884	152.474565	192.168.1.5	100.1.1.2	TCP	54	3389 → 53144 [ACK]
7885	152.510268	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data
7886	152.536739	100.1.1.2	192.168.1.5	TLSv1.2	101	Application Data
7887	152.536793	192.168.1.5	100.1.1.2	TCP	54	3389 → 53144 [ACK]
7888	152.564308	100.1.1.2	192.168.1.5	TLSv1.2	108	Application Data

> Frame 7439: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF{...}

#show ip nat translations 如下: 增加了 50.1.1.10 的 3389 端口号, 对应远程桌面连接

```
26-RSR20-2#debug ip nat
26-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 100.1.1.2:53193    100.1.1.2:53193  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:53194    100.1.1.2:53194  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:53144    100.1.1.2:53144  50.1.1.10:3389    192.168.1.5:3389
```

【实验思考】

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

NAT TCP 负载均衡只是用与 TCP 连接, 对于 ping 这种非 TCP 操作, 发送的是 ICMP 包, NAT 进程不会对其进行转换。

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

负载均衡与访问量无关:

尝试在主机 A 使用 `1..100 | ForEach-Object { Start-Process curl -ArgumentList "-s http://50.1.1.10/" -NoNewWindow }` 命令得到对服务器的多条并行访问。

#show ip nat translations 如下: 对于同一 ip 地址不同端口的访问, 始终访问到 192.168.1.5 一台服务器。轮询似乎不起作用

```
26-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 100.1.1.2:54642    100.1.1.2:54642  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54635    100.1.1.2:54635  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54633    100.1.1.2:54633  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54641    100.1.1.2:54641  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54508    100.1.1.2:54508  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54638    100.1.1.2:54638  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54507    100.1.1.2:54507  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54639    100.1.1.2:54639  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54640    100.1.1.2:54640  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54634    100.1.1.2:54634  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54636    100.1.1.2:54636  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:54637    100.1.1.2:54637  50.1.1.10:80      192.168.1.5:80
```

通过测试关闭 192.168.1.5 服务器之后, 主机访问 50.1.1.10, 结果变为无法访问, 查看 NAT 表依旧



计算机网络实验报告

映射到 192.168.1.5，但由于该服务器已经关闭，因此在另一台服务器打开情况下，仍旧无法访问。接下来通过尝试接入一台新主机，两台主机同时访问 50.1.1.10，查看 NAT 表，发现此时才将访问分到两个服务器上，两台主机分别访问两台服务器。实验结果表明单一 ip 地址下访问量增加并不会负载均衡，只有当多个 ip 对其进行访问的时候才会通过轮询将访问分配到不同服务器，达到负载均衡的效果。

（增加一台主机 100.1.1.3，发现访问了另一台服务器）

```
26-RSR20-2(config)#show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
tcp 100.1.1.2:65391     100.1.1.2:65391  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:65392     100.1.1.2:65392  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.3:51553     100.1.1.3:51553  50.1.1.10:80      192.168.1.6:80
tcp 100.1.1.2:65390     100.1.1.2:65390  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.3:51552     100.1.1.3:51552  50.1.1.10:80      192.168.1.6:80

tcp 100.1.1.2:50036     100.1.1.2:50036  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:50109     100.1.1.2:50109  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:49932     100.1.1.2:49932  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:1373      100.1.1.2:50010  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:49860     100.1.1.2:49860  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:49300     100.1.1.2:49300  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.2:50108     100.1.1.2:50108  50.1.1.10:80      192.168.1.5:80
tcp 100.1.1.3:51604     100.1.1.3:51604  50.1.1.10:80      192.168.1.6:80
```

(3) 本实验采用的技术有什么现实意义？

现实中访问服务器的主机特别多的情况下，通过 NAT 实现负载均衡，使用轮询方式，将大量的访问合理地分配到多台服务器上，减轻每台服务器的访问压力。且隐藏网络内部的服务器 IP，有效避免来自 Internet 的攻击。

学号	学生	自评分
21307347	陈欣宇	93
21307350	高宇	92
21307100	陈华清	92