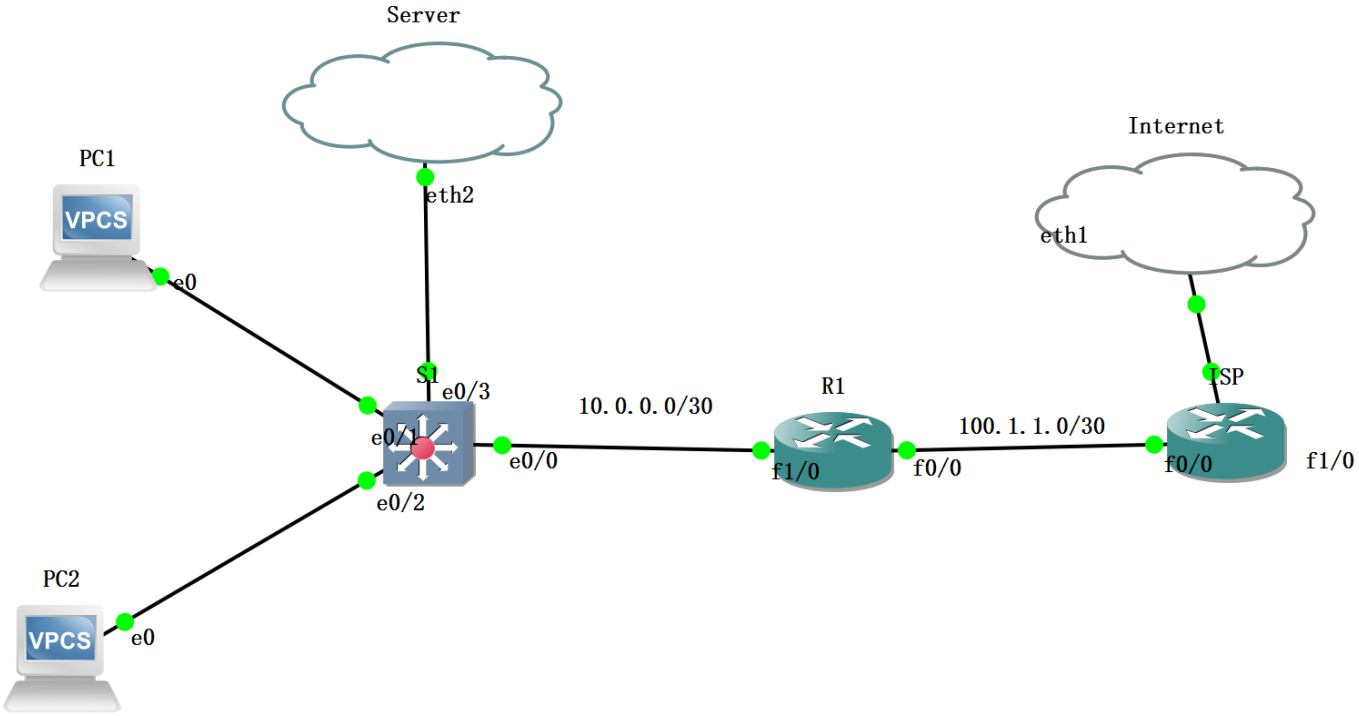
实践4 接入部分设计

[任务目标]

> 掌握默认路由重分布。
> 掌握动态NAPT
> 掌握静态NAPT
> 掌握使用NAT隐藏外部主机真实地址

[任务内容]

> - 一个企业网接入ISP部分设计拓扑如图所示。S1是核心层交换机，R1是接入ISP的边界路由器，企业网内部采用OSPF路由。要求
>   (1)在R1上设置默认路由重分布，使得内网的三层交换机的默认路由最终指向R1方向。
>   (2)在R1上配置动态NAPT使得内网10.0.2.0/24能访问外网。
>   (3)在R1上配置静态NAPT，使得外网的主机能访问内网的服务器。静态NAPT映射如下：
>   10.0.1.1:80->100.1.1.1:80
>   10.0.1.2:20->100.1.1.1:20
>   10.0.1.2:21->100.1.1.1:21
>   (4)在R1上使用NAT隐藏外部主机真实地址。外部真实主机到内部地址的映射为：
>   100.1.2.1->10.1.1.1



[操作人员]

年级 专业

学号 姓名

[任务记录]

R1

```
R1(config)#int f0/0
R1(config-if)#ip add 100.1.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#int f0/1
R1(config-if)#ip add 10.0.0.2 255.255.255.252
R1(config-if)#no shut
```

isp

```
R2(config)#int f0/0
R2(config-if)#ip add 100.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#int f0/1
R2(config-if)#ip add 100.1.2.254 255.255.255.0
R2(config-if)#no shut
```

S1

```
S1#conf t
S1(config)#int e0/0
S1(config-if)#no shut
S1(config-if)#no switchport
S1(config-if)#ip add 10.0.0.1 255.255.255.252

S1(config)#int e0/1
S1(config-if)#no switchport
S1(config-if)#ip add 10.0.2.254 255.255.255.0

S1(config)#int e0/2
S1(config-if)#no switchport
S1(config-if)#ip add 10.0.3.254 255.255.255.0

S1(config)#int vlan 1
S1(config-if)#ip add 10.0.1.254 255.255.255.0
S1(config-if)#no shut
```

PC1

```
pc1> ip 10.0.2.1 255.255.255.0 10.0.2.254
pc1> ping 10.0.2.254
```

PC2

```
pc2> ip 10.0.3.1 255.255.255.0 10.0.3.254
pc2> ping 10.0.3.254
```

S1

```
S1(config-if)#exit
S1(config)#no ip cef
```

去看视频 39.00

- 新建web服务器

- 新建FTP服务器
  - 接口VMnet3
- 配置默认路由重分布

  R1

```
conf t
ip route 0.0.0.0 0.0.0.0 100.1.1.2
router ospf 1
net 10.0.0.0 0.0.0.3 area 0
default-information originate always
```

S1

```
router ospf 1
net 0.0.0.0 255.255.255.255 area 0
end
sh ip route
```

- 动态NAPT配置
- 在R1上配置动态NAPT使得内网 `10.0.2.0/24` 能访问外网。

复用接口地址的动态NAPT

- 在全局设置模式下，定义一个标准的access-list规则以允许哪些内部本地地址可以进行动态地址转换。

  access-list 标号 permit 源地址 通配符

  其中标号为1－99之间的整数
- 在全局设置模式下，设置在内部的本地地址与内部合法IP地址间建立复用动态地址转换。

  ip nat inside source list <ACL编号> interface <接口类型与编号> overload

R1

```
conf t
access-list 1 permit 10.0.2.0 0.0.0.255
ip nat inside source list 1 interface f0/0 overload
int f0/1
ip nat inside
int f0/0
ip nat outside
end
sh ip nat translation
```

- 静态NAPT

> 在R1上配置静态NAPT，使得外网的主机能访问内网的服务器。静态NAPT映射如下：
> 10.0.1.1:80->100.1.1.1:80
> 10.0.1.2:20->100.1.1.1:20(ftp)
> 10.0.1.2:21->100.1.1.1:21(ftp)

R1

```
conf t
ip nat inside source static tcp 10.0.1.1 80 100.1.1.1 80
ip nat inside source static tcp 10.0.1.2 20 100.1.1.1 20
ip nat inside source static tcp 10.0.1.2 21 100.1.1.1 21
end
sh ip int b
show ip nat translation
```

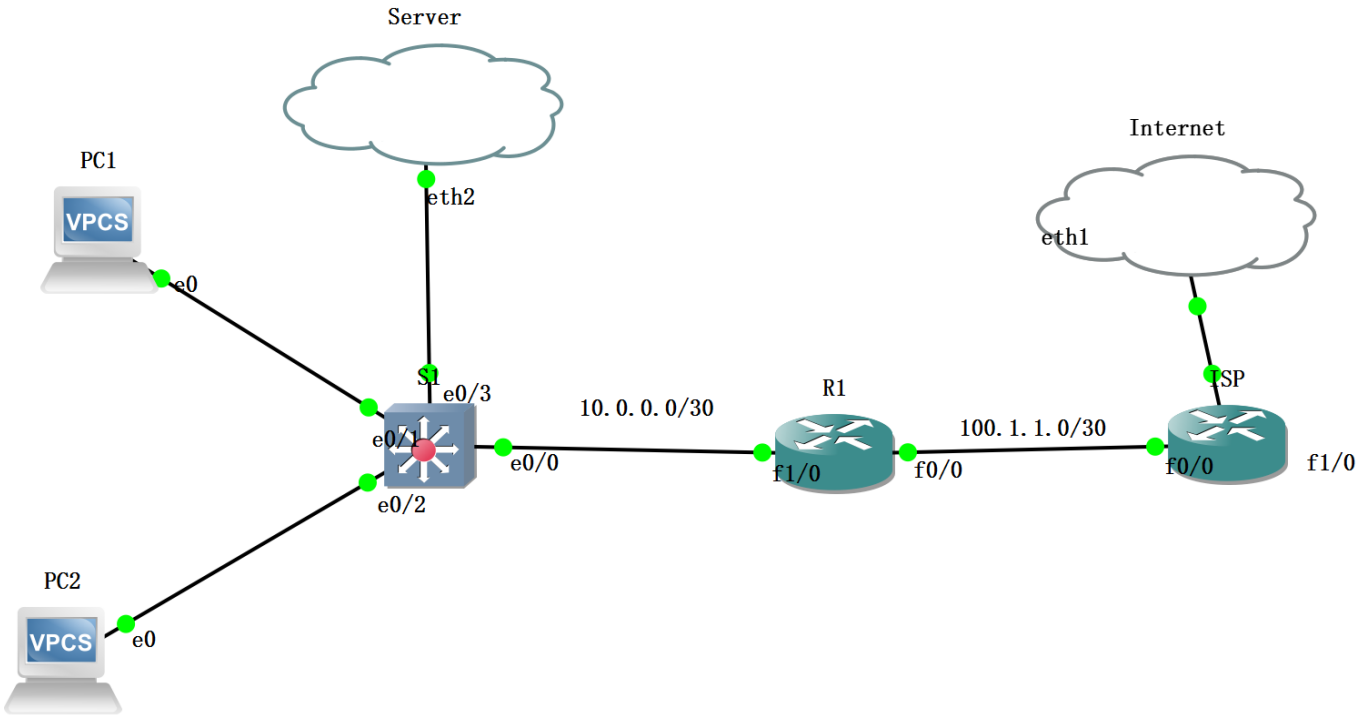
```
R1#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.1:20       10.0.1.2:20        ---                ---
tcp 100.1.1.1:21       10.0.1.2:21        ---                ---
tcp 100.1.1.1:80       10.0.1.1:80        ---                ---
```

R1

```
ip nat outside source static 100.1.2.1 10.1.1.1 add-route
```

- 隐藏外部主机真实地址

1. GNS3拓扑搭建



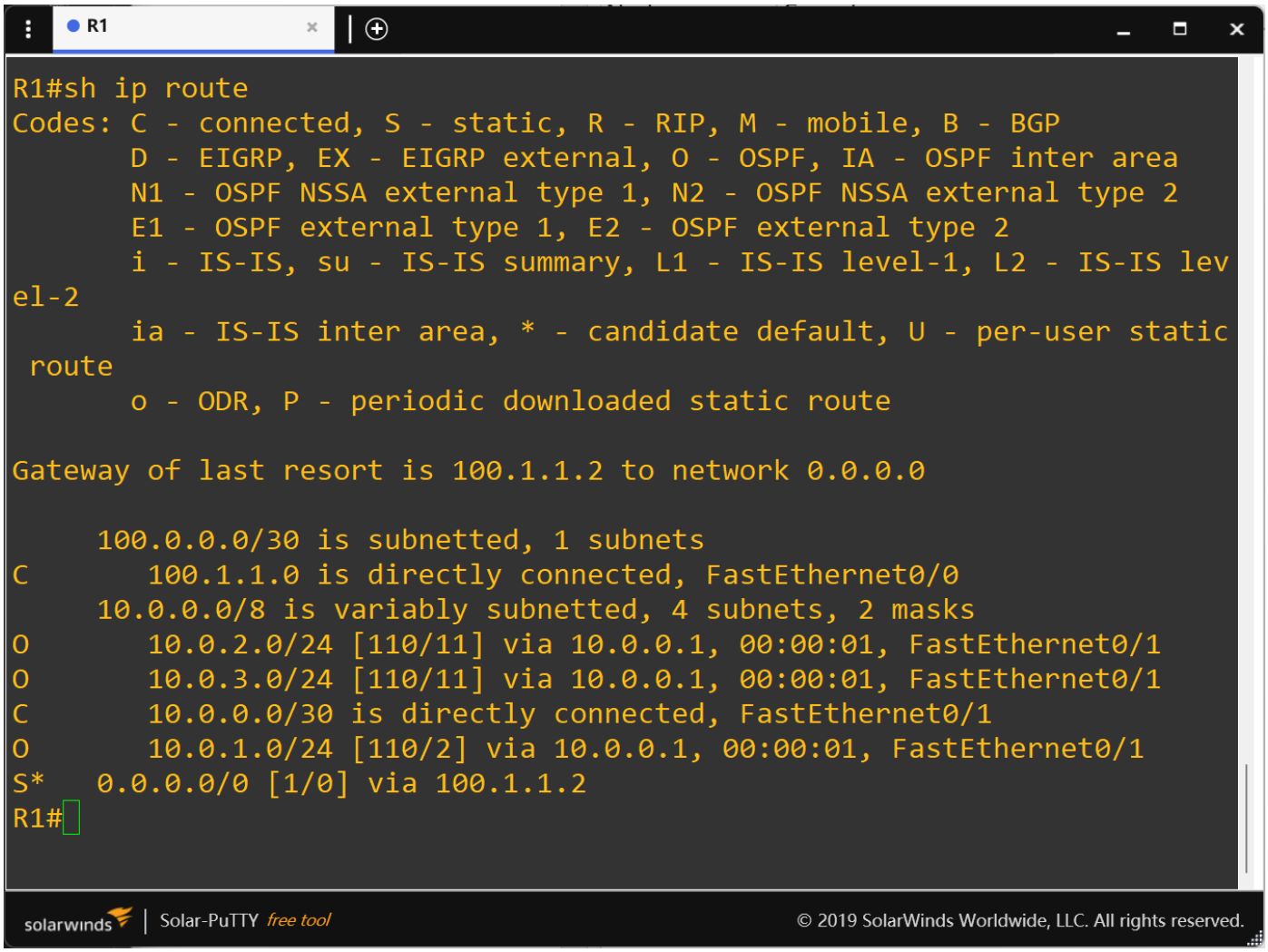
2. 配置接口IP与路由

```
PC1> ip 10.0.2.1 255.255.255.0 10.0.2.254
Checking for duplicate address...
PC1 : 10.0.2.1 255.255.255.0 gateway 10.0.2.254

PC1> pc1> ping 10.0.2.254
Bad command: "pc1> ping 10.0.2.254". Use ? for help.

PC1>  ping 10.0.2.254

84 bytes from 10.0.2.254 icmp_seq=1 ttl=255 time=0.109 ms
84 bytes from 10.0.2.254 icmp_seq=2 ttl=255 time=0.260 ms
84 bytes from 10.0.2.254 icmp_seq=3 ttl=255 time=0.300 ms
84 bytes from 10.0.2.254 icmp_seq=4 ttl=255 time=0.205 ms
84 bytes from 10.0.2.254 icmp_seq=5 ttl=255 time=0.210 ms

PC1>
```

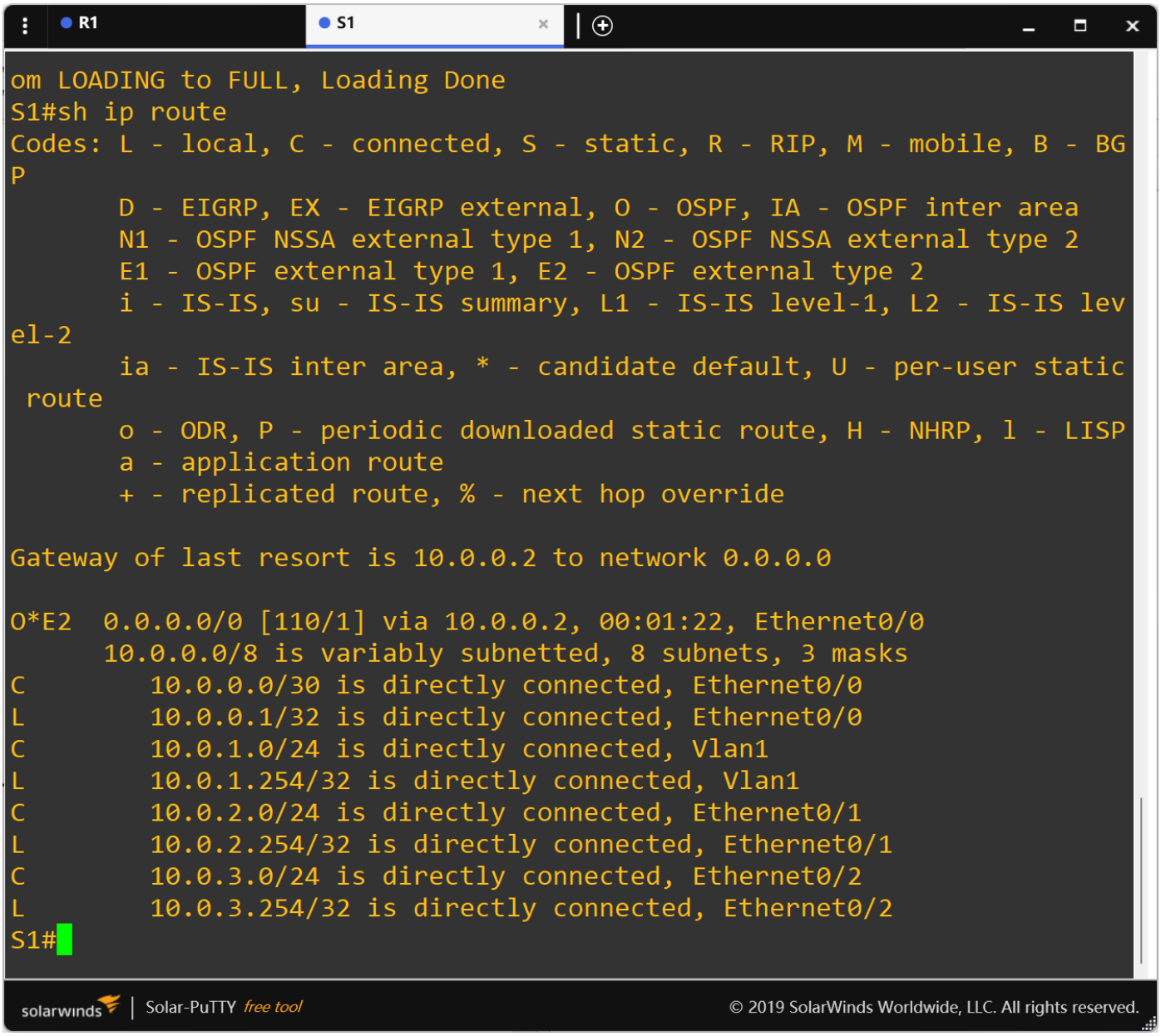
```
PC2> ping 100.1.2.1

100.1.2.1 icmp_seq=1 timeout
100.1.2.1 icmp_seq=2 timeout
100.1.2.1 icmp_seq=3 timeout
100.1.2.1 icmp_seq=4 timeout
100.1.2.1 icmp_seq=5 timeout

PC2> ip 10.0.3.1 255.255.255.0 10.0.3.254
Checking for duplicate address...
PC2 : 10.0.3.1 255.255.255.0 gateway 10.0.3.254

PC2> ping 10.0.3.254

84 bytes from 10.0.3.254 icmp_seq=1 ttl=255 time=0.176 ms
84 bytes from 10.0.3.254 icmp_seq=2 ttl=255 time=0.202 ms
84 bytes from 10.0.3.254 icmp_seq=3 ttl=255 time=0.316 ms
84 bytes from 10.0.3.254 icmp_seq=4 ttl=255 time=0.264 ms
84 bytes from 10.0.3.254 icmp_seq=5 ttl=255 time=0.225 ms

PC2>
```

3. 配置默认路由重分布

   R1:

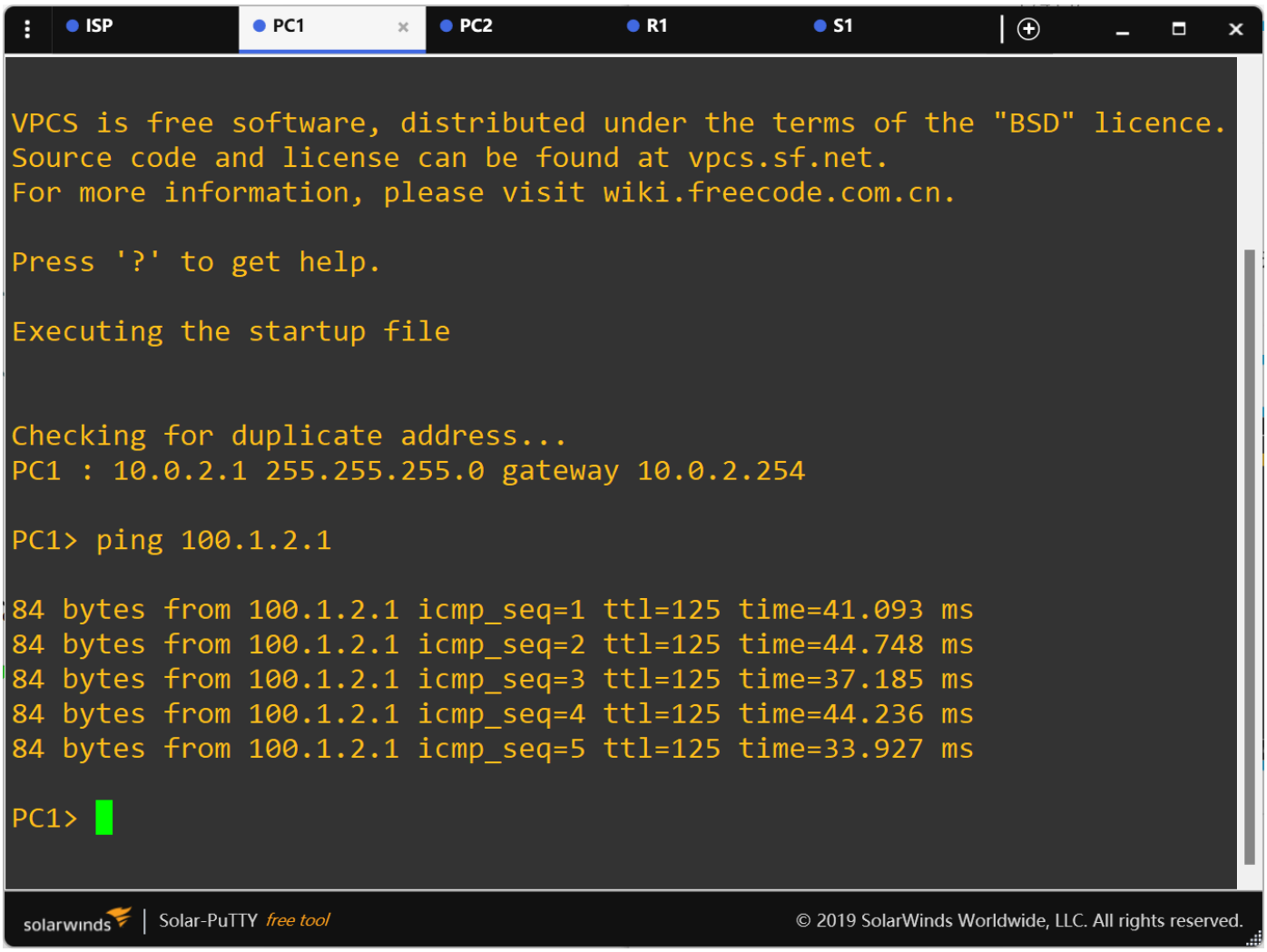

R1
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is 100.1.1.2 to network 0.0.0.0
100.0.0.0/30 is subnetted, 1 subnets
C 100.1.1.0 is directly connected, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O 10.0.2.0/24 [110/11] via 10.0.0.1, 00:00:01, FastEthernet0/1
O 10.0.3.0/24 [110/11] via 10.0.0.1, 00:00:01, FastEthernet0/1
C 10.0.0.0/30 is directly connected, FastEthernet0/1
O 10.0.1.0/24 [110/2] via 10.0.0.1, 00:00:01, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 100.1.1.2
R1#
solarwinds
Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

S1:



4. 配置动态NAPT

   PC1:


ISP
PC1
PC2
R1
S1
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
Checking for duplicate address...
PC1 : 10.0.2.1 255.255.255.0 gateway 10.0.2.254
PC1> ping 100.1.2.1
84 bytes from 100.1.2.1 icmp_seq=1 ttl=125 time=41.093 ms
84 bytes from 100.1.2.1 icmp_seq=2 ttl=125 time=44.748 ms
84 bytes from 100.1.2.1 icmp_seq=3 ttl=125 time=37.185 ms
84 bytes from 100.1.2.1 icmp_seq=4 ttl=125 time=44.236 ms
84 bytes from 100.1.2.1 icmp_seq=5 ttl=125 time=33.927 ms
PC1>
solarwinds
Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

PC2:

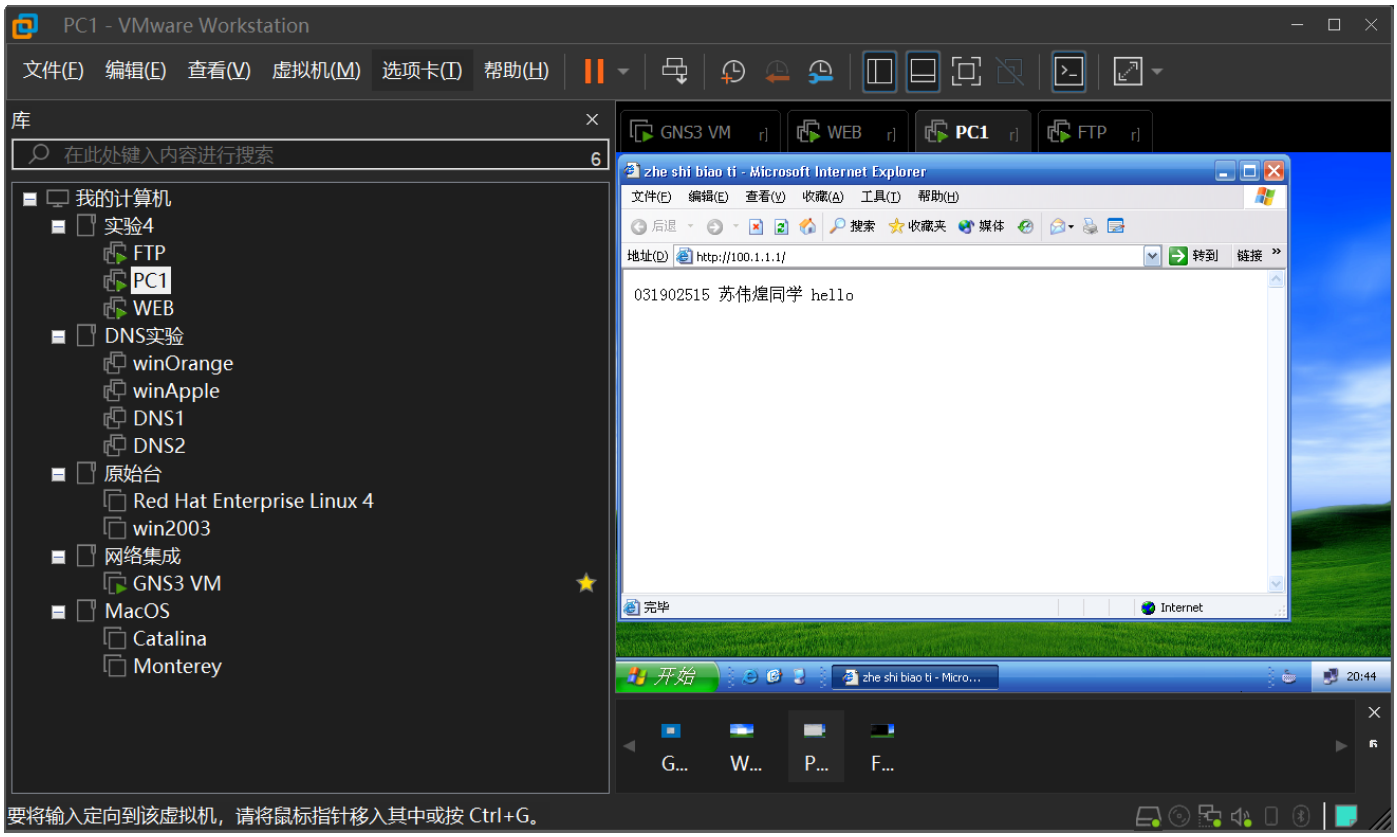

```
R1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 100.1.1.1:30479   10.0.2.1:30479     100.1.2.1:30479    100.1.2.1:30479
icmp 100.1.1.1:38671   10.0.2.1:38671     100.1.2.1:38671    100.1.2.1:38671
icmp 100.1.1.1:30735   10.0.2.1:30735     100.1.2.1:30735    100.1.2.1:30735
icmp 100.1.1.1:29711   10.0.2.1:29711     100.1.2.1:29711    100.1.2.1:29711
icmp 100.1.1.1:38927   10.0.2.1:38927     100.1.2.1:38927    100.1.2.1:38927
icmp 100.1.1.1:29967   10.0.2.1:29967     100.1.2.1:29967    100.1.2.1:29967
icmp 100.1.1.1:39183   10.0.2.1:39183     100.1.2.1:39183    100.1.2.1:39183
icmp 100.1.1.1:30223   10.0.2.1:30223     100.1.2.1:30223    100.1.2.1:30223
icmp 100.1.1.1:39439   10.0.2.1:39439     100.1.2.1:39439    100.1.2.1:39439
icmp 100.1.1.1:38415   10.0.2.1:38415     100.1.2.1:38415    100.1.2.1:38415
R1#
```

5. 配置静态NAPT

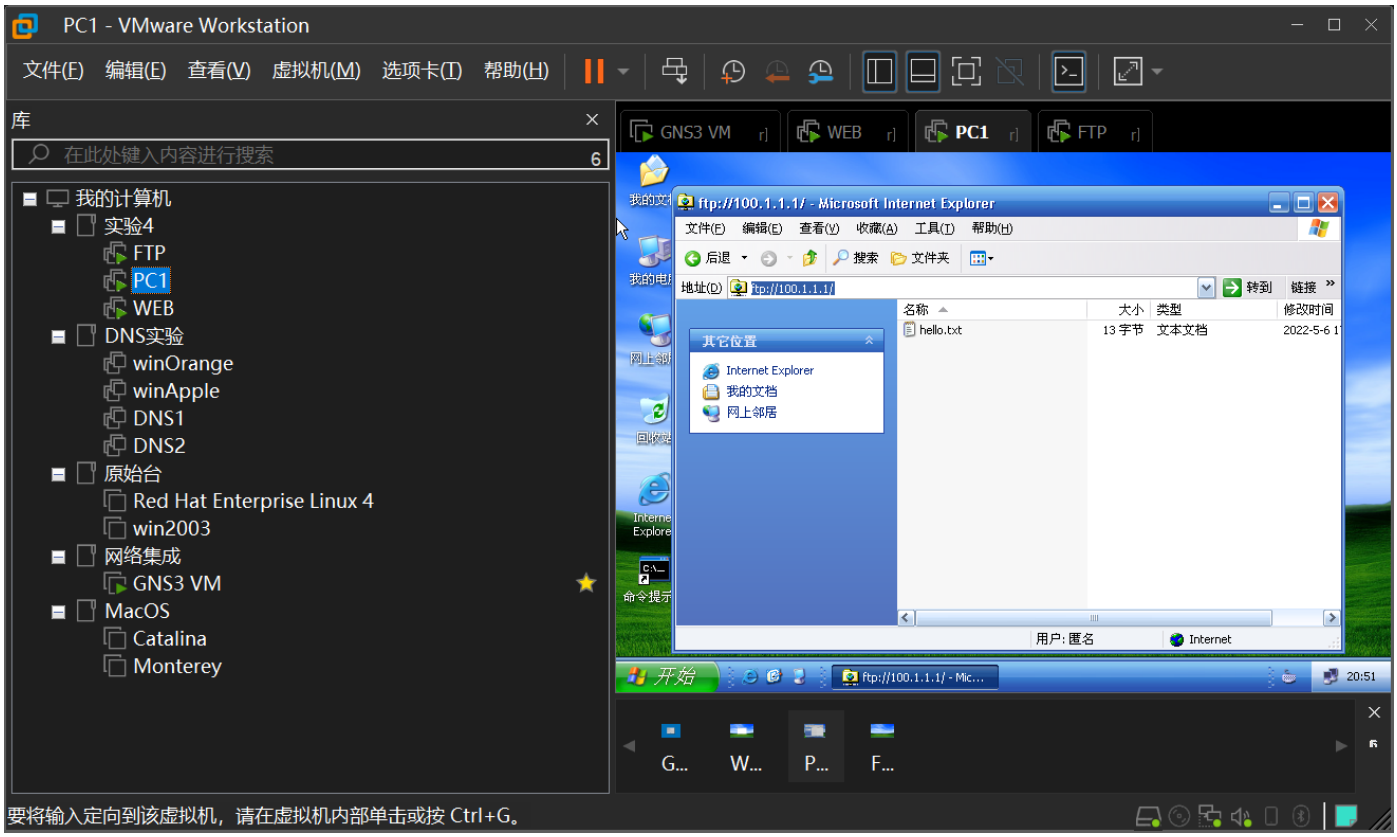
结果:

```
R1#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.1:20       10.0.1.2:20        ---                ---
tcp 100.1.1.1:21       10.0.1.2:21        ---                ---
tcp 100.1.1.1:80       10.0.1.1:80        ---                ---
```

测试:



ftp



after ftp

```
R1#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.1:1062     10.0.1.2:1062      100.1.2.1:1044     100.1.2.1:1044
tcp 100.1.1.1:1063     10.0.1.2:1063      100.1.2.1:1046     100.1.2.1:1046
tcp 100.1.1.1:20       10.0.1.2:20        ---                ---
tcp 100.1.1.1:21       10.0.1.2:21        ---                ---
tcp 100.1.1.1:80       10.0.1.1:80        ---                ---
tcp 100.1.1.1:20       10.0.1.2:20        100.1.2.1:1042     100.1.2.1:1042
tcp 100.1.1.1:80       10.0.1.1:80        100.1.2.1:1036     100.1.2.1:1036
tcp 100.1.1.1:80       10.0.1.1:80        100.1.2.1:1040     100.1.2.1:1040
R1#
```

6. 隐藏外部主机真实地址

- (4)在R1上使用NAT隐藏外部主机真实地址。外部真实主机到内部地址的映射为：100.1.2.1->10.1.1.1

R1

```
ip nat outside source static 100.1.2.1 10.1.1.1 add-route
```

```
R1#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.1:1062     10.0.1.2:1062      100.1.2.1:1044     100.1.2.1:1044
tcp 100.1.1.1:1063     10.0.1.2:1063      100.1.2.1:1046     100.1.2.1:1046
tcp 100.1.1.1:20       10.0.1.2:20        ---                ---
tcp 100.1.1.1:21       10.0.1.2:21        ---                ---
tcp 100.1.1.1:80       10.0.1.1:80        ---                ---
tcp 100.1.1.1:20       10.0.1.2:20        100.1.2.1:1042     100.1.2.1:1042
tcp 100.1.1.1:80       10.0.1.1:80        100.1.2.1:1036     100.1.2.1:1036
tcp 100.1.1.1:80       10.0.1.1:80        100.1.2.1:1040     100.1.2.1:1040
R1#
```

```
PC1> ping 10.1.1.1

84 bytes from 10.1.1.1 icmp_seq=1 ttl=125 time=48.995 ms
84 bytes from 10.1.1.1 icmp_seq=2 ttl=125 time=41.467 ms
84 bytes from 10.1.1.1 icmp_seq=3 ttl=125 time=34.218 ms
84 bytes from 10.1.1.1 icmp_seq=4 ttl=125 time=39.900 ms
84 bytes from 10.1.1.1 icmp_seq=5 ttl=125 time=44.075 ms
```

```
R1#sh ip nat tran
Pro Inside global      Inside local       Outside local      Outside global
icmp 100.1.1.1:25379   10.0.2.1:25379     10.1.1.1:25379     100.1.2.1:25379
tcp 100.1.1.1:1062     10.0.1.2:1062      100.1.2.1:1044     100.1.2.1:1044
tcp 100.1.1.1:1063     10.0.1.2:1063      100.1.2.1:1046     100.1.2.1:1046
icmp 100.1.1.1:25635   10.0.2.1:25635     10.1.1.1:25635     100.1.2.1:25635
tcp 100.1.1.1:20       10.0.1.2:20        ---                ---
tcp 100.1.1.1:21       10.0.1.2:21        ---                ---
icmp 100.1.1.1:25891   10.0.2.1:25891     10.1.1.1:25891     100.1.2.1:25891
tcp 100.1.1.1:80       10.0.1.1:80        ---                ---
--- ---                ---                10.1.1.1           100.1.2.1
tcp 100.1.1.1:20       10.0.1.2:20        100.1.2.1:1042     100.1.2.1:1042
icmp 100.1.1.1:26147   10.0.2.1:26147     10.1.1.1:26147     100.1.2.1:26147
icmp 100.1.1.1:25123   10.0.2.1:25123     10.1.1.1:25123     100.1.2.1:25123
tcp 100.1.1.1:80       10.0.1.1:80        100.1.2.1:1036     100.1.2.1:1036
tcp 100.1.1.1:80       10.0.1.1:80        100.1.2.1:1040     100.1.2.1:1040
R1#
```