

希赛网，专注于软考、PMP、通信考试的专业 IT 知识库和在线教育平台。希赛网在线题库，提供历年考试真题、模拟试题、章节练习、知识点练习、错题本练习等在线做题服务，更有能力评估报告，让你告别盲目做题，针对性地攻破自己的薄弱点，更高效的备考。

希赛网官网：<http://www.educity.cn/>

希赛网软件水平考试网：<http://www.educity.cn/rk/>

希赛网在线题库：<http://www.educity.cn/tiku/>

2016 年上半年网工案例分析真题答案与解析：<http://www.educity.cn/tiku/tp19498.html>

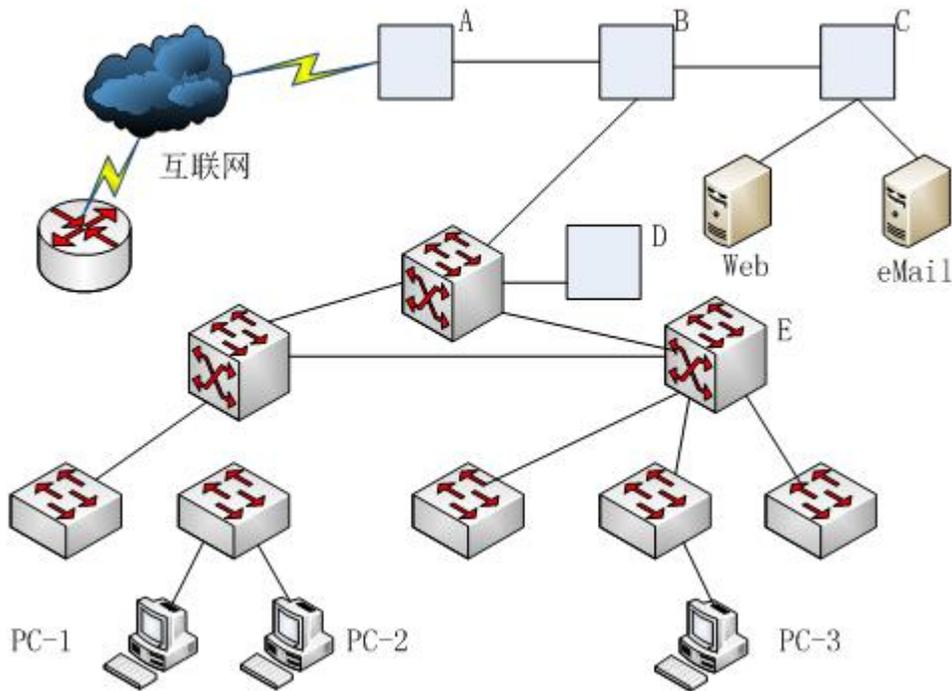
## 2016 年上半年网络工程师考试下午真题

### (参考答案)

● 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业网络拓扑如图 1-1 所示，A~E 是网络设备的编号。



**【问题 1】**（每空 1 分，共 4 分）

根据图 1-1，将设备清单表 1-1 所示内容补充完整。

表 1-1

设备名	在图中的编号
防火墙 USG3000	(1)
路由器 AR2220	(2)
交换机 QUIDWAY3300	(3)
服务器 IBM X3500M5	(4)

【问题 2】（每空 2 分，共 4 分）

以下是 AR2220 的部分配置。

```
[AR2220]acl 2000
[AR2220-acl-2000]rule normal pmut source 192.168.0.0 0.0.255.255
[AR2220-acl-2000]rule normal deny source any
[AR2220-acl-2000]quit
[AR2220]interface Ethemet0
[AR2220-Ethemet0]ip address 192.168.0.1 255.255.255.0
[AR2220-Ethemet0]quit
[AR2220]mterface Ethemet1
[AR2220-Ethemet1]ip address 59.41.221.100
255.255.255.0
[AR2220-Ethemet1]nat outbound 2000 mterface
[AR2220-Ethernet1]quit
[AR2220]ip route-static 0.0.0.0 0.0.0.0 59.74221.254
```

设备 AR2220 硬用 (5) 接口实现 NAT 功能，该接口地址韵网关是 (6)。

【问题 3】（每空 2 分，共 6 分）

若只允许内网发起 ftp、http 连接,并且拒绝来自站点 2.2.2.11 的 Java Applets 报文。在 USG3000 设备中有如下配置，请补充完整。

```
[USG3000]acl number 3000
[USG3000-acl-adv-3000] rule permit tcp destination-port eq www
[USG3000-acl-adv-3000] rule permit tcp destination-port eq ftp
[USG3000-acl-adv-3000] rule permit tcp destination-port eq ftp-data
[USG3000]acl number 2010
[USG3000-acl-basic-2010] rule (7) source 2.2.2.11.0.0.0
[USG3000-acl-basic-2010] rule permit source any
[USG3000] (8) interzone trust untrust
[USG3000-interzone-ttust-untrust] packet-filter 3000 (9)
[USG3000-interzone-ttust-untrust] detect ftp
[USG3000-interzone-ttust-untrust] detect http
[USG3000-interzone-ttust-untrust] detect java-blocking 2010
```

(7) ~ (9) 备选答案:

- (1) A. Firewall  
 B. trust  
 C. deny  
 D. permit  
 E. outbound  
 F. inbound

【问题 4】（每空 2 分，共 6 分）

PC-1、PC-2、PC-3、网络设置如表 1-2。

表 1-2

设备名	网络地址	网关	VLAN
PC-1	192.168.2.2/24	192.168.2.1	VLAN100
PC-2	192.168.3.2/24	192.168.3.1	VLAN200
PC-3	192.168.4.2/24	192.168.4.1	VLAN300

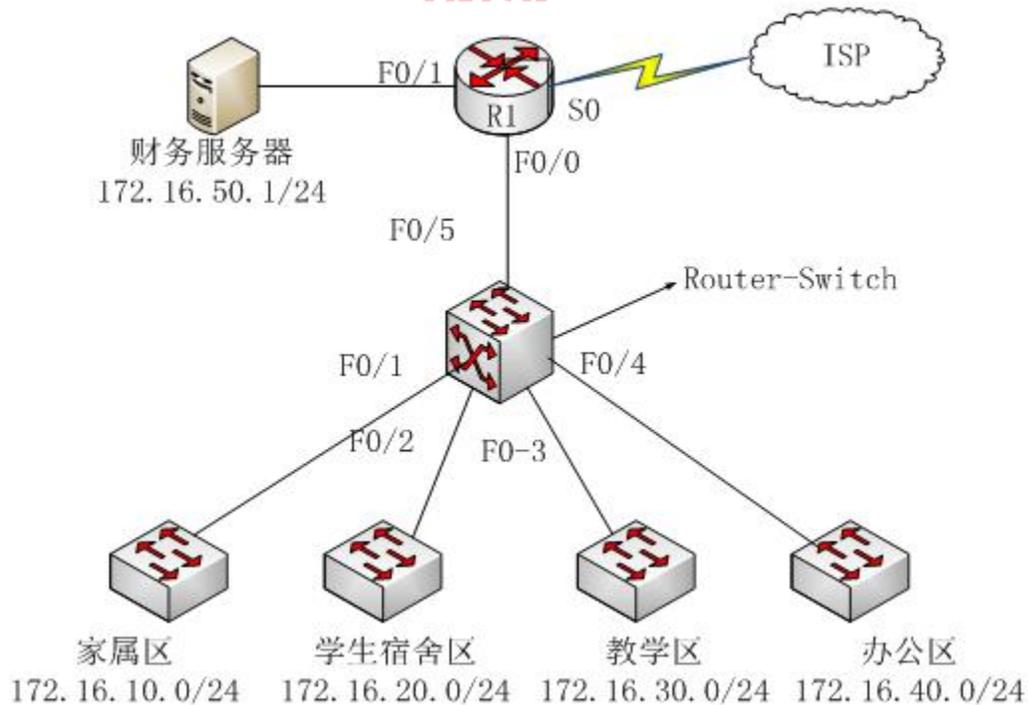
通过配置 RIP，使得 PC-1、PC-2、PC-3 能相互访问，请补充设备 E 上的配置，或解释相关命令。

```
// 配置 E 上 vlan 路由接口地址
interface vlanif 300
ip address (10) 255.255.255.0
interface vlanif 1000 //互通 VLAN
ip address 192.168.100.1 255.255.255.0
//配置 E 上的 rip 协议
rip
network 192.168.4.0
networkr (11)
//配置 E 上的 trunk 链路
int e0/1
Port link-type trunk //(12)
port trunk permit vlan all
```

- 阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某学校的网络拓扑结构图如图 2-1 所示。



**【问题 1】**（每空 1 分，共 7 分）

常用的 IP 访问控制列表有两种，它们是编号为(1) 和 1300~1399 的标准访问控制列表和编号为(2) 和 2000~2699 的扩展访问控制列表、其中，标准访问控制列表是根据 IP 报文的(3) 来对 IP 报文进行过滤，扩展访问控制列表是根据 IP 报文的(4)、(5)、上层协议和时间等来对 IP 报文进行过滤。一般地，标准访问控制列表放置在靠近(6) 的位置，扩展访问控制列表放置在靠近(7) 的位置。

【问题 2】（每空 1 分，共 10 分）

为保障安全，使用 ACL 对网络中的访问进行控制。访问控制的要求如下：

- (1)家属区不能访问财务服务器，但可以访问互联网；
- (2)学生宿舍区不能访问财务服务器，且在每天晚上 18:00~24:00 禁止访问互联网；
- (3)办公区可以访问财务服务器和互联网；
- (4)教学区禁止访问财务服务器，且每天 8:00~18:00 禁止访问互联网。

1. 使用 ACL 对财务服务器进行访问控制，请将下面配置补充完整。

```
R1(config)#access-list 1 (8) (9) 0.0.0.255
```

```
R1(config)#access-list 1 deny 172.16.10.0 0.0.0.255
```

```
R1(config)#access-list 1 deny 172.16.20.0 0.0.0.255
```

```
R1(config)#access-list 1 deny (10) 0.0.0.255
```

```
R1(config)#interface (11)
```

```
R1(config-if)#ip access-group 1 (12)
```

2. 使用 ACL 对 Internet 进行访问控制，请将下面配置补充完整。

```
Route-Switch(config)#time-range jxq //定义教学区时间范围
```

```
Route-Switch(config-time-range)# periodic daily (13)
```

```
Route-Switch(config)#time-range xsssq //定义学生宿舍区时间范围
```

```
Route-Switch(config-time-range)#periodic (14) 18:00 to 24:00
```

```
Route-Switch(config-time-range)#exit
```

```
Route-Switch(config)#access-list 100 permit ip 172.16.10.0 0.0.0.255 any
```

```
Route-Switch(config)#access-list 100 permit ip 172.16.40.0 0.0.0.255 any
```

```
Route-Switch(config)#access-list 100 deny ip (15) 0.0.0.255 time-range jxq
```

```
Route-Switch(config)#access-list 100 deny ip (16) 0.0.0.255 time-range xsssq
```

```
Route-Switch (config)#interface (17)
```

```
Route-Switch(config-if)#ip access-group 100out
```

【问题 3】（每空 1 分，共 3 分）

网络在运行过程中发现，家属区网络经常受到学生宿舍区网络的 DDoS 攻击，现对家属区网络和学生宿舍区网络之间的流量进行过滤，要求家属区网络可访问学生宿舍区网络，但学生宿舍区网络禁止访问家属区网络。

采用自反访问列表实现访问控制，请解释配置代码。

```
Route-Switch(config)#ip access-extended infilter
```

```
Route-Switch(config-ext-nacl)#permit ip any 172.16.20.0 0.0.0.255 reflect jsq (18)
```

```
Route-Switch(config-ext-nacl)#exit
```

```
Route-Switch(config)#ip access-list extended outfilter
```

```
Route-Switch(config-ext-nacl)# evaluate jsq (19)
```

```
Route-Switch(config-ext-nacl)#exit
```

```
Route-Switch(config)#interface fastethernet 0/1
```

```
Route-Switch(config-if)#ip access-group infilter in
```

```
Route-Switch(config-if)#ip access-group outfilter out // (20)
```

- 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业采用 Windows Server 2003 配置了 DHCP、DNS 和 WEB 服务。

【问题 1】（每空 1 分，共 4 分）

DHCP 服务器地址池 192.168.0.1~192.168.0.130，其中 192.168.0.10 分配给网关，192.168.0.11~192.168.0.15 分配给服务器，192.168.0.20 分配给网络管理员。

The screenshot shows the 'Create IP Address Pool' (新建作用域) window. It contains the following fields and text:

- IP 地址范围 (IP Address Range):** 必须通过确定一组连续的 IP 地址来定义作用域地址范围。 (Must be defined by a set of consecutive IP addresses.)
- 输入此作用域分配的地址范围 (Enter the address range for this pool):**
- 起始 IP 地址 (Start IP Address):** (1)
- 结束 IP 地址 (End IP Address):** (2)
- 子网掩码 (Subnet Mask):** 子网掩码定义 IP 地址的多少位用作网络/子网 ID，多少位用作主机 ID。您可以用长度或 IP 地址来指定子网掩码。 (The subnet mask defines how many bits of the IP address are used for the network/subnet ID and how many for the host ID. You can specify the subnet mask by length or IP address.)
- 长度 (Length):** 24
- 子网掩码 (Subnet Mask):** 255.255.255.0
- Navigation buttons:** < 上一步 (Previous Step), 下一步 (Next Step), 取消 (Cancel)

图 3-1

The screenshot shows the 'Add Exclusion' (添加排除) window. It contains the following fields and text:

- 添加排除 (Add Exclusion):** 排除是指服务器不分配的地址或地址范围。 (Exclusion refers to addresses or address ranges that the server does not allocate.)
- 键入您想要排除的 IP 地址范围。如果您想排除一个单独的地址，则只在“起始 IP 地址”键入地址。 (Enter the IP address range you want to exclude. If you want to exclude a single address, enter the address only in the "Start IP Address" field.)**
- 起始 IP 地址 (Start IP Address):** [Empty field]
- 结束 IP 地址 (End IP Address):** [Empty field]
- 添加 (Add):** [Button]
- 排除的地址范围 (Excluded address range):**
- (3)** [Text in the exclusion list]
- 删除 (Delete):** [Button]
- Navigation buttons:** < 上一步 (Previous Step), 下一步 (Next Step), 取消 (Cancel)

图 3-2

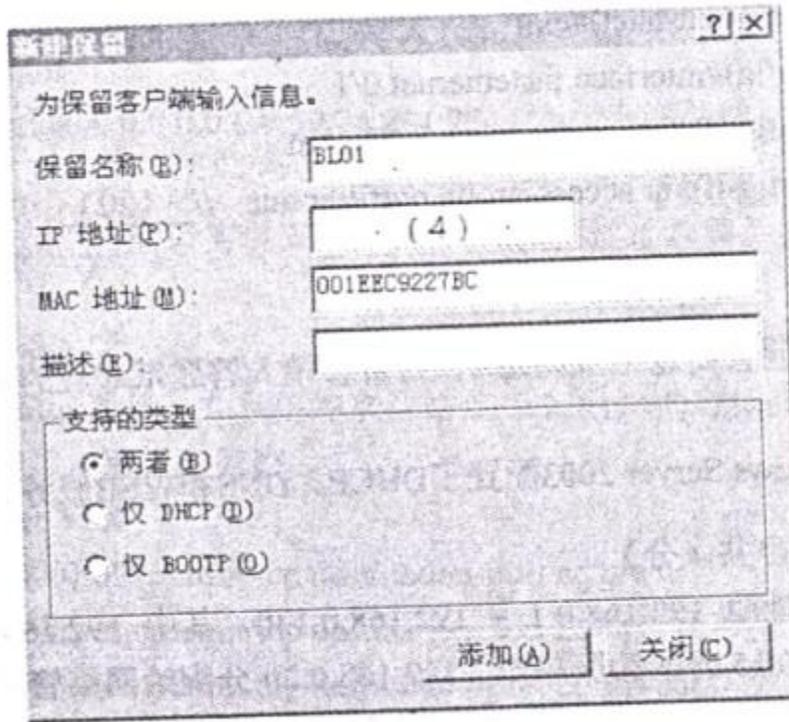


图 3-3

请填写图 3-1 至图 3-3 中 (1) ~ (4) 处空缺内容。

【问题 2】(每空 1.5 分, 共 9 分)

DNS 的配置如图 3-4 所示。

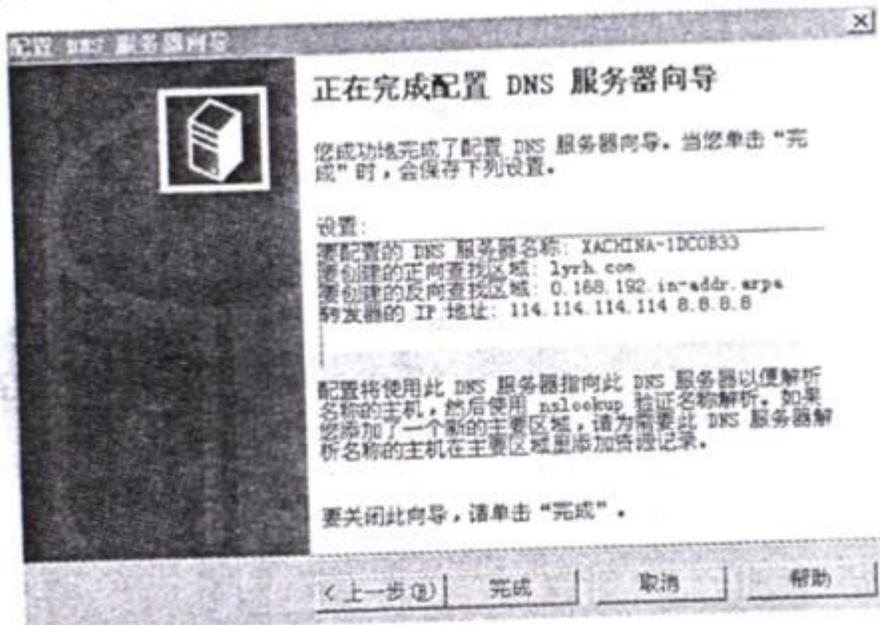


图 3-4

根据图 3-4 判断正误 (正确的答“对”, 错误的答“错”)。

- (3) A. YACHINA-1DC0B33 的 IP 地址为 114.114.114.114。 (5)  
 B. 该域名服务器无法解析的域名转发到 114.114.114.114 或 8.8.8.8。 (6)

- C. 域 lyrh.com 的资源记录包含在该 DNS 服务器中。 (7)
- D. 客户机的“首选 DNS 服务器”地址必须与该 DNS 服务器地址一致。 (8)
- E. 该域名服务器是 lyrh.com 的授权域名服务器。 (9)
- F. 该域名服务器支持 192.168.101.6 地址的反向域名查找。 (10)

【问题 3】(每空 2 分, 共 4 分)

Web 服务器的配置如图 3-5 所示。

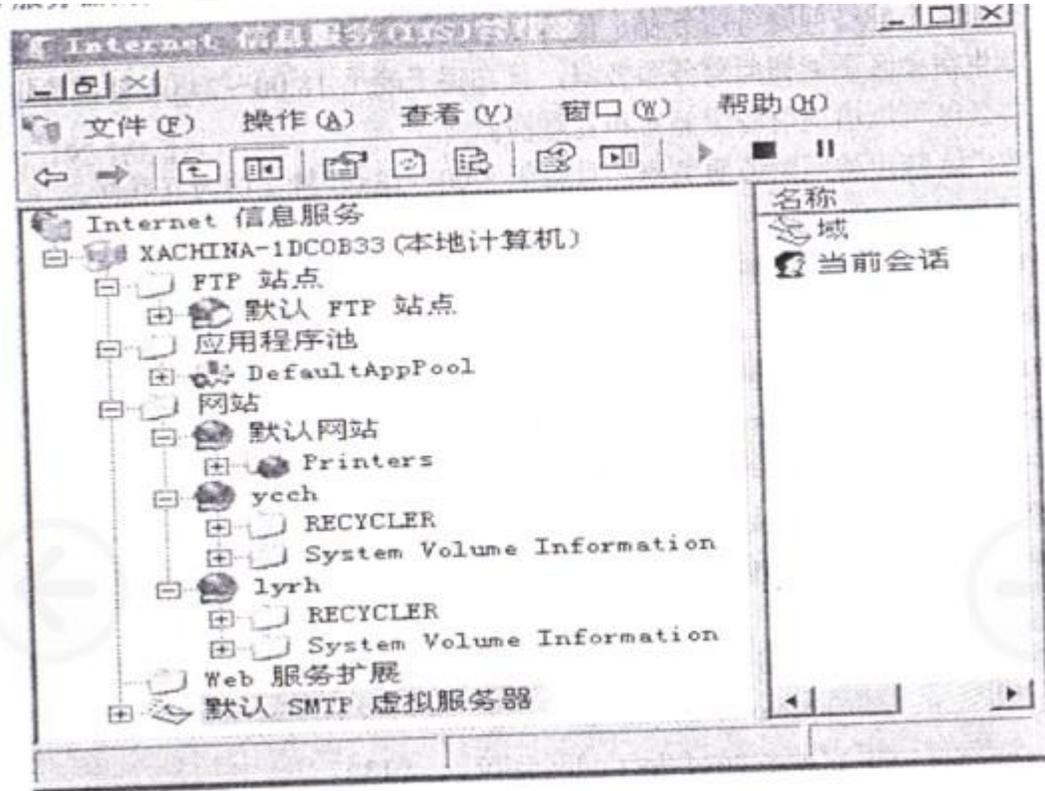


图 3-5

1. 如图 3-5 所示, 通过主机头的方式建立两个网站 www.ycch.com 和 www.lyrh.com 网站配置是 (11)。

(11)备选答案:

- (4) A. 相同的 IP 地址, 不同的端口号
- B. 不同的 IP 地址, 相同的目录
- C. 相同的 IP 地址, 不同的目录
- D. 相同的主机头, 相同的端口号

2. 除了主机头方式, 还可以采用 (12) 方式在一台服务器上配置多网站。

【问题 4】(每空 1 分, 共 3 分)

Windows Server 2003 管理界面如图 3-6 所示。

- 1. 图 3-6 中设备打“?”的含义是 (13), 设备打“x”的含义是 (14)。
- 2. 图 3-6 中 1394 网络适配器能连接什么设备? (15)。

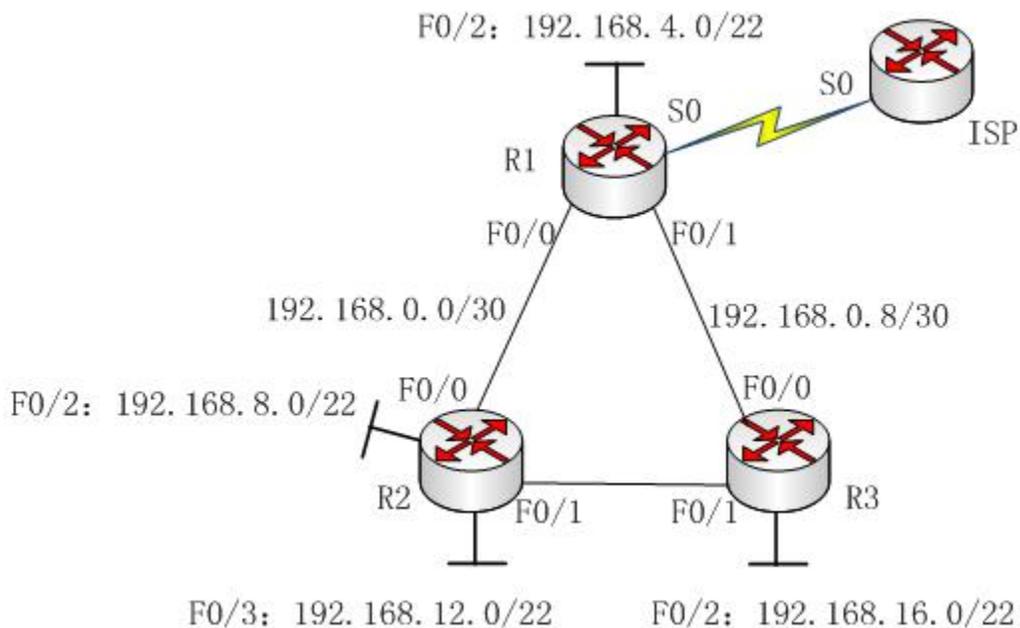


图 3-6

● 阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司有 3 个分支机构，网络拓扑结构及地址分配如图 4-1 所示。



【问题 1】（每空 1 分，共 11 分）

公司申请到 202.111.1.0/29 的公有地址段，采用 NAPT 技术实现公司内部访问互联网的要求，其中，192.168.16.0/22 网段禁止访问互联网。R1、R2 和 R3 的基本配置已正确配置完成，其中 R1 的配置如下。请根据拓扑结构，完成下列配置代码。

R1 的基本配置及 NAPT 配置如下：

```
R1>enable
R1#config terminal
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastethernet 0/1
R1(config-if)#ip address 192.168.0.9 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastethernet 0/2
R1(config-if)#ip address (1) 255.255.252.0 //使用网段中最后一个地址
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0
R1(config-if)#ip address 202.111.1.1 255.255.255.248
R1(config-if)#no shutdown
R1(config)#ip nat pool ss 202.111.1.1 (2) netmask (3)
R1(config)# interface (4) fastethernet 0/0-1
R1(config-if)#ip nat (5)
R1(config-if)#interface serial 0
R1(config-if)#ip nat (6)
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.0.0 (7)
R1(config)#ip nat inside (8) list (9) pool (10) (11)
```

【问题 2】（每空 2 分，共 4 分）

在 R1、R2 和 R3 之间运行 OSPF 路由协议，其中 R1、R2 和 R3 的配置如下。

行号 配置代码

```
1 R1(config)#router ospf 1
2 R1(config-router)#network 192.168.4.0 0.0.3.255 area 0
3 R1(config-router)#network 192.168.0.0 0.0.0.3 area 0
4 R1(config-router)#network 192.168.0.8 0.0.0.3 area 0

5 R2>enable
6 R2#config terminal
7 R2(config)#router ospf 2
8 R2(config-router)#network 192.168.8.0 0.0.3.255 area 0
9 R2 (config-router)#network 192.168.12.0 0.0.3.255 area 0
10 R2 (config-router)#network 192.168.0.4 0.0.3 area 0

11 R3>enable
12 R3#config terminal
13 R3(config)#router ospf 3
14 R3(config-router)#network 192.168.0.8 0.0.3 area 0
15 R3(config-router)#network 192.168.0.4 0.0.3 area 0
```

1. 配置完成后，在 R1 和 R2 上均无法 ping 通 R3 的局域网，可能的原因是 (12)。

(12) 备选答案：

- (4) A. 在 R3 上未宣告局域网路由
- B. 以上配置中第 7 行和第 13 行配置错误
- C. 第 1 行配置错误
- D. R1、R2 未宣告直连路由。

2. 在 OSPF 中重分布默认路由的命令是：(13)。

(13) 备选答案：

- (5) A. R1#default-informaton originate
- B. R1(config-if)#default-information originate
- C. R1(config-router)#default-information originate
- D. R1(config)#default-information originate

希赛在线题库