

【软考达人】

# 软考资料免费获取

- 1、最新软考题库
- 2、软考备考资料
- 3、考前压轴题



**微信扫一扫，立马获取**



**6W+ 免费题库**



**免费备考资料**

PC版题库: [ruankaodaren.com](http://ruankaodaren.com)

## 2018 年下半年网络工程师考试下午真题（专业解析+ 参考答案）

1、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】

某园区组网方案如图 1-1 所示，数据规划如表 1-1 内容所示。

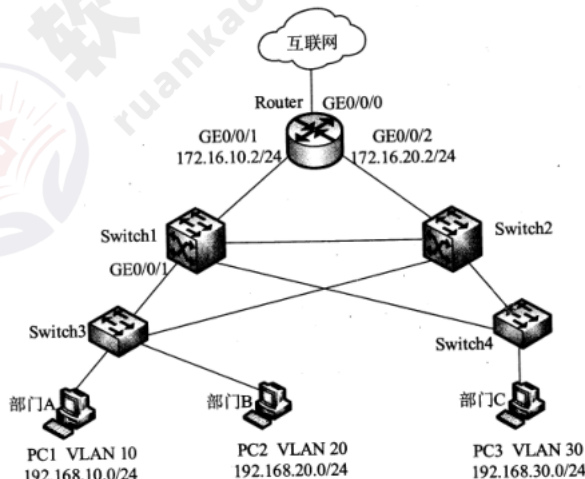


图 1-1

表 1-1

操作	准备项	数据	说明
配置接口和 VLAN	Eth-Trunk 类型	静态 LACP	Eth-Trunk 链路有手工负载分担和静态 LACP 两种工作模式
	端口类型	连接交换机的端口设置为 trunk，连接 PC 的端口设置为 access	
	VLAN ID	Switch3: VLAN 10、20 Switch1: VLAN 10、20、30、100、300	交换机有省缺 VLAN 1，为二层隔离部门 A、B，将部门 A 划到 VLAN 10，部门 B 划到 VLAN 20，Switch1 通过 vlanif100 连接出口路由器

配置核心交换机路由	IP 地址	Switch1: vlanif100 172.16.10.1/24 vlanif300 172.16.30.1/24 vlanif10 192.168.10.1/24 vlanif20 192.168.20.1/24	Vlanif100 是 Switch1 与出口路由器对接 VLAN 300 用于 Switch1 与 Switch2 对接 Switch1 上配置 VLAN 10、VLAN 20 的 IP 地址后，部门 A 与部门 B 之间可以通过 Switch1 互访 Switch1 上需要配置一条缺省路由，下一跳指向出口路由器；配置一条备用路由，下一跳指向 Switch2
配置出口路由器	公网接口 IP 地址	GE0/0/0: 202.101.111.2/30	GE0/0/0 为出口路由器连接 Internet 的接口，一般称为公网接口
	公网网关	202.101.111.1/30	该地址是与出口路由器对接的运营商设备 IP 地址，出口路由器上需要配置一条缺省路由，用于内网流量转发到 Internet
	内网接口 IP 地址	GE0/0/1: 172.16.10.2/24 GE0/0/2: 172.16.20.2/24	GE0/0/1、GE0/0/2 为出口路由器连接内网的接口，GE0/0/1 用于连接主设备，GE0/0/2 用于连接备份设备

问题内容：【问题 1】(8 分，每空 2 分)

以 Switch3 为例配置接入层交换机，补充下列命令片段。

```
<HUAWEI>( 1 )
[HUAWEI] sysname Switch3
[Switch3] vlan batch( 2 )
[Switch3] interface GigabitEthernet 0/0/3
[Switch3-GigabitEthernet0/0/3] port link-type( 3 )
[Switch3-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[Switch3-GigabitEthernet0/0/3] quit
[Switch3] interface GigabitEthernet 0/0/1
[Switch3-GigabitEthernet0/0/1] port link-type( 4 )
[Switch3-GigabitEthernet0/0/1] port default vlan 10
[Switch3-GigabitEthernet0/0/1] quit
[Switch3] stp bpdu-protection
```

【问题 2】(8 分，每空 2 分)

以 Switch1 为例配置核心层交换机，创建其与接入交换机、备份设备以及出口路由器的互通 VLAN，补充下列命令。

```
<HUAWEI>system-view
[HUAWEI] sysname Switch1
[Switch1] vlan batch( 5 )
[Switch1] interface GigabitEthernet0/0/1
[Switch1-GigabitEthernet0/0/1] port link-type trunk
[Switch1-GigabitEthernet0/0/1] port trunk allow-pass( 6 )
[Switch1-GigabitEthernet0/0/1] quit
[Switch1] interface Vlanif 10
[Switch1-Vlanif10] ip address 192.168.10.1 24
[Switch1-Vlanif10] quit
[Switch1] interface Vlanif 20
[Switch1-Vlanif20] ip address 192.168.20.1 24
[Switch1-Vlanif20] quit
[Switch1] interface GigabitEthernet 0/0/7
[Switch1-GigabitEthernet0/0/7] port link-type trunk
[Switch1-GigabitEthernet0/0/7] port trunk allow-pass vlan 100
[Switch1-GigabitEthernet0/0/7] quit
[Switch1] interface Vlanif 100
[Switch1-Vlanif100] ip address( 7 )
[Switch1-Vlanif100] quit
[Switch1] interface GigabitEthernet 0/0/5
[Switch1-GigabitEthernet0/0/5] port link-type access
[Switch1-GigabitEthernet0/0/5] port default vlan 300
[Switch1-GigabitEthernet0/0/5] quit
[Switch1] interface Vlanif 300
[Switch1-Vlanif300] ip address( 8 )
[Switch1-Vlanif300] quit
```

【问题3】(4分，每空2分)

如果配置静态路由实现网络互通，补充在 Switch1 和 Router 上配置的命令片段。

[Switch1] ip route-static( 9 )//默认优先级

[Switch1] ip route-static 0.0.0.0 0.0.0.0 172.16.30.2 preference 70

[Router] ip route-static( 10 )//默认优先级

[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.10.1

[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.20.1  
preference70

[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.10.1

[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.20.1  
preference70

2、阅读下列说明，回答问题1至问题4，将解答填入答题纸的对应栏内。

【说明】

图2-1为A公司和公司总部的部分网络拓扑，A公司员工办公区域DHCP分配的IP段为10.0.36.1/24，业务服务器IP地址为10.0.35.1，备份服务器IP地址为10.0.35.2；公司总部备份服务器IP地址为10.0.86.200。

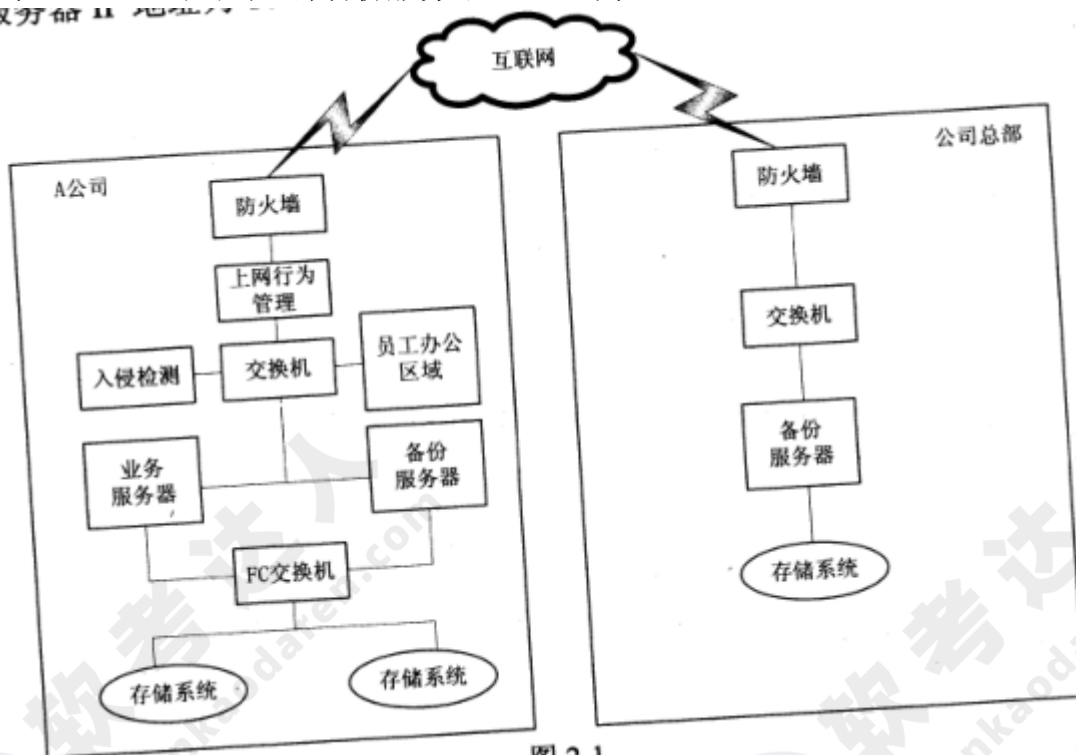


图2-1

问题内容：【问题1】(4分，每空2分)

网络威胁会导致非授权访问、信息泄露、数据被破坏等网络安全事件发生，其常见的网络威胁包括窃听、拒绝服务、病毒、木马、( 1 )等，常见的网络安全防范措施包括访问控制、审计、身份认证、数字签名、( 2 )、包过滤和检测等。



(1) 备选答案：

- A. 数据完整性破坏
- B. 物理链路破坏
- C. 存储介质破坏
- D. 电磁干扰

(2) 备选答案：

- A. 数据备份
- B. 电磁防护
- C. 违规外联控制
- D. 数据加密

【问题 2】(6 分，每空 2 分)

某天，网络管理员在入侵检测设备上发现图 2-2 所示网络威胁日志，从该日志可判断网络威胁为( 3 )，网络管理员应采取( 4 )、( 5 )等合理有效的措施进行处理。

时间戳	源主机	目标主机	协议	检测严重性	攻击阶段	显著对象
2018-07-18 09:33:59	10.0.36.249	106.75.115.143	HTTP	①高	C&C 通信	URL: http://1.7654.com/theinote/online?code=Yc1qsQ2c...
2018-07-18 09:22:45	10.0.36.249	106.75.115.143	HTTP	①高	C&C 通信	URL: http://1.7654.com/theinote/kunbang?code=Yc1qsQ...
2018-07-18 09:07:53	10.0.36.249	106.75.115.143	HTTP	①高	C&C 通信	URL: http://1.7654.com/theinote/jingpin?code=Yc1qsQ2...
2018-07-18 09:07:46	10.0.36.249	106.75.115.143	HTTP	①高	C&C 通信	URL: http://1.7654.com/theinote/kunbang?code=Yc1qsQ...
2018-07-18 09:04:21	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/ileope...
2018-07-18 09:04:17	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/kunba...
2018-07-18 09:04:11	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/jingpin...
2018-07-18 09:03:41	10.0.36.249	106.75.115.143	HTTP	①高	C&C 通信	URL: http://1.7654.com/theinote/jingpin?code=Yc1qsQ2...
2018-07-18 09:03:20	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/kunba...
2018-07-18 09:03:19	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/jingpin...
2018-07-18 08:51:19	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/kunba...
2018-07-18 08:51:18	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/jingpin...
2018-07-18 08:48:41	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/online...
2018-07-18 08:48:36	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/kunba...
2018-07-18 08:48:29	10.0.36.249	106.75.95.184	HTTP	①高	C&C 通信	URL: http://kj.kpzip.com/kuaizipreport/kuaizipreport/jingpin...

图 2-2

(3) 备选答案：

- A. 跨站脚本攻击
- B. 拒绝服务
- C. 木马
- D. sql 注入

(4)~(5) 备选答案：

- A. 源主机安装杀毒软件并查杀
- B. 目标主机安装杀毒软件并查杀
- C. 将上图所示 URL 加入上网行为管理设备黑名单
- D. 将上图所示 URL 加入入侵检测设备黑名单
- E. 使用漏洞扫描设备进行扫描

【问题 3】(4 分，每空 1 分)

A 公司为保障数据安全，同总部建立 ipsecVPN 隧道，定期通过 A 公司备份服务器向公司总部备份数据，仅允许 A 公司的备份服务器、业务服务器和公司总部

的备份服务器通讯，图 2-3 为 A 公司防火墙创建 VPN 隧道第二阶段协商的配置页面，请完善配置。其中，本地子网：( 6 )、本地掩码：( 7 )、对方子网：( 8 )、对方掩码：( 9 )。

本地子网

本地掩码

对方子网

对方掩码

图 2-3

【问题 4】(6 分)

根据业务发展，购置了一套存储容量为 30TB 的存储系统，给公司内部员工每人配备 2TB 的网盘，存储管理员预估近一年内，员工对网盘的平均使用空间不超过 200GB，为节省成本，启用了该存储系统的自动精简 (Thin provisioning 不会一次性全部分配存储资源，当存储空间不够时，系统会根据实际所需要的容量，从存储池中多次少量的扩展存储空间) 配置功能，为 100 个员工提供网盘服务。请简要叙述存储管理员使用自动精简配置的优点和存在的风险。

3、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】

某公司网络划分为两个子网，其中设备 A 是 DHCP 服务器，如图 3-1 所示。

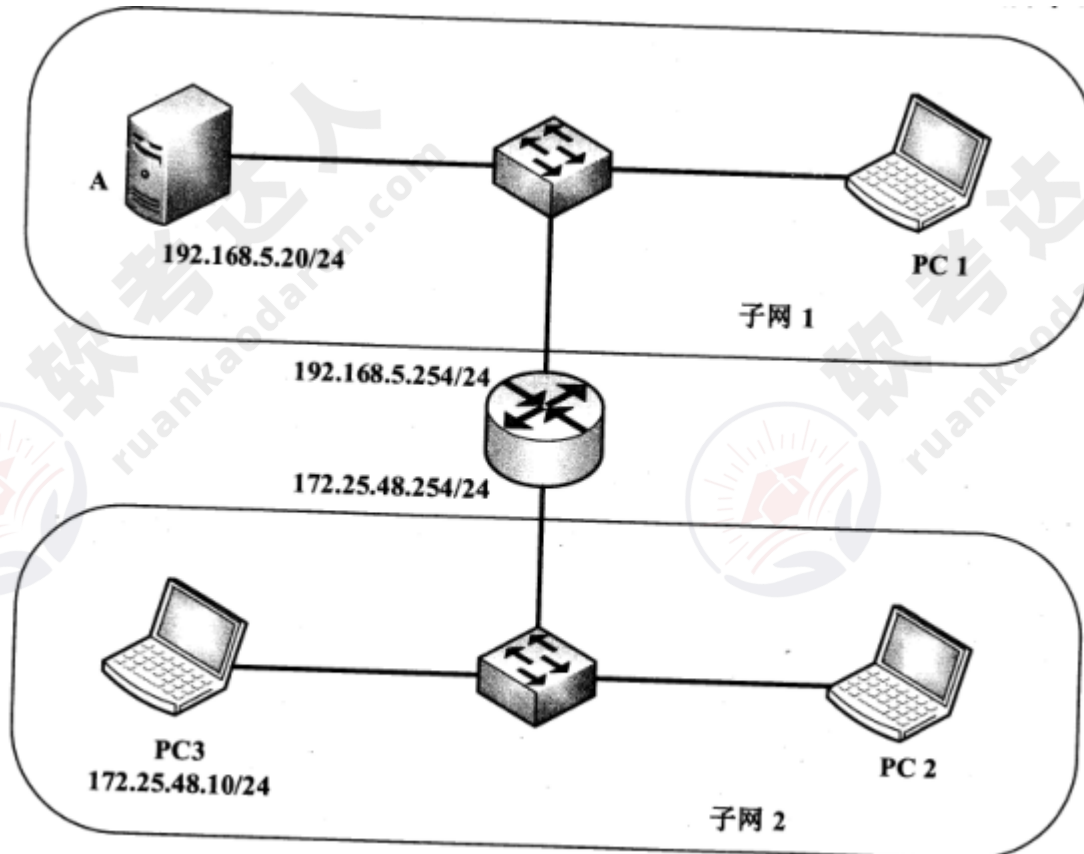


图 3-1

问题内容：【问题 1】(6 分，每空 2 分)

DHCP 在分配 IP 地址时使用( 1 )的方式， 而此消息不能通过路由器，所以子网 2 中的客户端要自动获得 IP 地址，不能采用的方式是( 2 )。 DHCP 服务器向客户端出租的 IP 地址一般有一个租借期限，在使用租期过去( 3 )时，客户端会向服务器发送 DHCP REQUEST 报文延续租期。

(1) 备选答案：

- A. 单播
- B. 多播
- C. 广播
- D. 组播

(2) 备选答案：

- A. 子网 2 设置 DHCP 服务器
- B. 使用三层交换机作为 DHCP 中继
- C. 使用路由器作为 DHCP 中继
- D. IP 代理

(3) 备选答案：

- A. 25%
- B. 50%
- C. 75%
- D. 87.5%

【问题 2】(5 分，每空 1 分)

在设置 DHCP 服务时，应当为 DHCP 添加( 4 )个作用域。子网 1 按照图 3-2 添加作用域，其中子网掩码为( 5 )， 默认网关为( 6 )。在此作用域中必须排除某个 IP 地址，如图 3-3 所示，其中“起始 IP 地址”处应填写( 7 )。 通常无线子网的默认租约时间为( 8 )

(8) 备选答案：

- A. 8 天
- B. 6 天
- C. 2 天
- D. 6 或 8 小时

**添加作用域**

作用域是网络可能的 IP 地址范围。只有创建作用域后，DHCP 服务器才能将 IP 地址分配给各个客户端。

**DHCP 服务器的配置设置**

作用域名称(S): 子网A的作用域

起始 IP 地址(T): 192.168.5.15

结束 IP 地址(E): 192.168.5.200

子网类型(B): 有线(租用持续时间将为 8 天)

☒ 激活此作用域(A)

**传播到 DHCP 客户端的配置设置**

子网掩码(U):

默认网关(可选)(D):

确定 取消



**新建作用域向导**

**添加排除和延迟**  
排除是指服务器不分配的地址或地址范围。延迟是指服务器将延迟 DHCP OFFER 消息传输的时间段。

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。

起始 IP 地址(S):  结束 IP 地址(E):

排除的地址范围(C):

子网延迟(毫秒)(L):

< 上一步(B) 下一步(N) >

【问题 3】(4 分，每空 2 分)

如果客户机无法找到 DHCP 服务器，它将从 (9) 网段中挑选一个作为自己的 IP 地址，子网掩码为 (10)。

(9) 备选答案：

- A. 192.168.5.0
- B. 172.25.48.0
- C. 169.254.0.0
- D. 0.0.0.0

4、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】

某企业的网络结构如图 4-1 所示。企业使用双出口，其中 ISP1 是高速链路，网

关为 202.100.1.2, ISP2 是低速链路, 网关为 104.114.128.2。

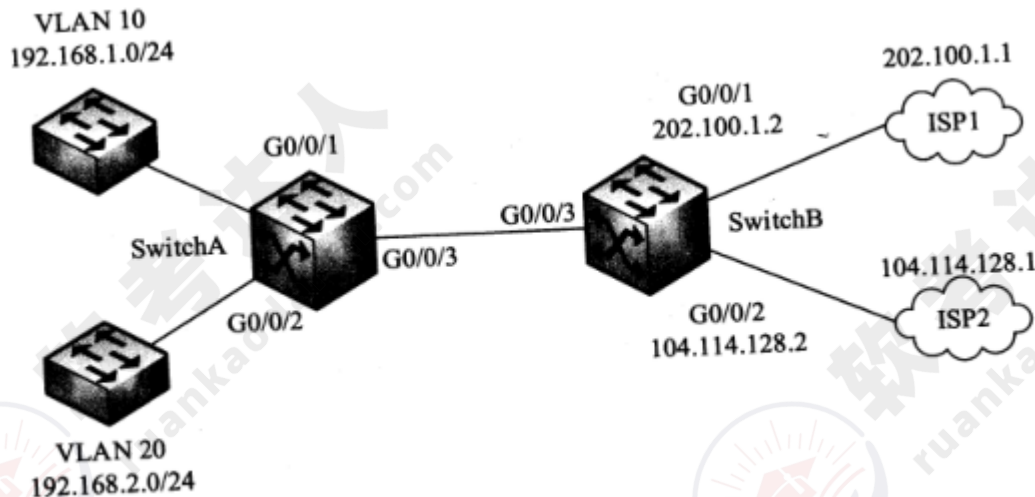


图 4-1

问题内容：【问题 1】(13 分, 每空 1 分)

公司内部有两个网段, 192.168.1.0/24 和 192.168.2.0/24, 使用三层交换机 SwitchB 实现 VLAN 间路由。为提高用户体验, 网络管理员决定带宽要求较高的 192.168.1.0 网段的数据通过高速链路访问互联网, 带宽要求较低的 192.168.2.0 网段的数据通过低速链路访问互联网。请根据描述, 将以下配置代码补充完整。

```
[SwitchB] acl 3000
[SwitchB-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255
destination 192.168.2.0 0.0.0.255
[SwitchB-acl-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255
destination 192.168.1.0 0.0.0.255
[SwitchB-acl-adv-3000] quit
[SwitchB] acl 3001 //匹配内网 192.168.1.0/24 网段的用户数据流
[SwitchB-acl-adv-3001] rule permit ip source ( 1 ) 0.0.0.255
[SwitchB-acl-adv-3001] quit
[SwitchB] acl 3002 //匹配内网 192.168.2.0/24 网段的用户数据流
[SwitchB-acl-adv-3002] rule permit ip ( 2 ) 192.168.2.0 0.0.0.255
[SwitchB-acl-adv-3002] quit
[SwitchB] traffic classifier c0 operator or
[SwitchB-classifier-c0] ( 3 ) acl 3000
[SwitchB-classifier-c0] quit
[SwitchB] traffic classifier c1 ( 4 ) or
[SwitchB-classifier-c1] if-match acl 3001
[SwitchB-classifier-c1] quit
[SwitchB] traffic classifier c2 operator or
[SwitchB-classifier-c2] if-match acl ( 5 )
[SwitchB-classifier-c2] ( 6 ) quit
[SwitchB] traffic behavior b0
[SwitchB-behavior-b0] ( 7 )
[SwitchB-behavior-b0] quit
```

```
[SwitchB] traffic behavior b1
[SwitchB-behavior-b1] redirect ip-nexthop( 8 )
[SwitchB-behavior-b1] quit
[SwitchB] traffic behavior b2
[SwitchB-behavior-b2] redirect ip-nexthop( 9 )
[SwitchB-behavior-b2] quit
[SwitchB] traffic policy p1
[SwitchB-trafficpolicy-p1] classifier c0 behavior( 10 )
[SwitchB-trafficpolicy-p1] classifier c1 behavior( 11 )
[SwitchB-trafficpolicy-p1] classifier c2 behavior b2
[SwitchB-trafficpolicy-p1] quit
[SwitchB] interface ( 12 )
[SwitchB-GigabitEthernet0/0/3] traffic-policy p1( 13 )
SwitchB-GigabitEthernet0/0/3] return
```

【问题 2】(2 分)

在问题 1 的配置代码中，配置 ACL 3000 的作用是：( 14 )。

【问题 3】(5 分，每空 1 分)

公司需要访问 Internet 公网，计划通过配置 NAT 实现私网地址到公网地址的转换，ISP1 公网地址范围为 202.100.1.1~202.100.1.5；ISP2 公网地址范围为 104.114.128.1~104.114.128.5。

请根据描述，将下面的配置代码补充完整。

```
.....
[SwitchB]nat address-group 0 202.100.1.3 202.100.1.5
[SwitchB]nat address-group 1 104.114.128.3 104.114.128.5
[SwitchB]acl number 2000
[SwitchB-acl-basic-2000]rule 5 ( 15 )source 192.168.1.0 0.0.0.255
[SwitchB]acl number 2001
[SwitchB-acl-basic-2001]rule 5 permit source 192.168.2.0 0.0.0.255
[SwitchB]interface GigabitEthernet0/0/3
[SwitchB-GigabitEthernet0/0/3]nat outbound( 16 )address group 0 no-
pat
[SwitchB-GigabitEthernet0/0/3]nat outbound( 17 )address group 1 no-
pat
[SwitchB-GigabitEthernet0/0/3]quit
[SwitchB] ip route-static 192.168.1.0 0.0.0.255( 18 )
[SwitchB] ip route-static 192.168.2.0 0.0.0.255( 19 )
.....
```

详细答案及解析尽在希赛网