

第 1 题:【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。

题: 1.1 (8 分, 每空 2 分)

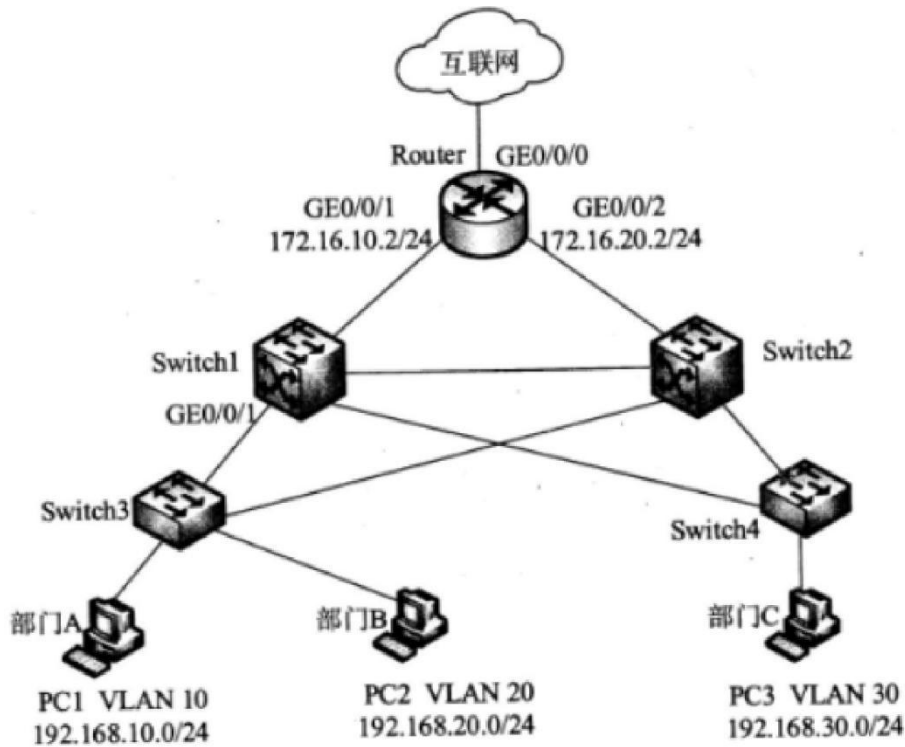


图 1-1

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

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 题：1.2 (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

题：1.3 (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

答案解析:



(1) system-view

(2) 10 20

(3) Trunk

(4) Access

试题分析:

(1) system-view 进入系统视图

(2) 创建 vlan10 和 vlan20

(3) 设置接口为 trunk 口

(4) 设置接口为 access 口

答案解析:

(5) 10 20 30 100 300

(6) vlan all 或 vlan 10 20

(7) 172.16.10.1 24

(8) 172.16.30.1 24

试题分析

(5) 批量创建 vlan10、20、30、100、300

(6) 设置允许的 vlan 通过

(7) 设置 vlan100 的接口 ip

(8) 设置 vlan300 的接口 ip

答案解析:

(9) 0.0.0.0 0.0.0.0 172.16.10.2

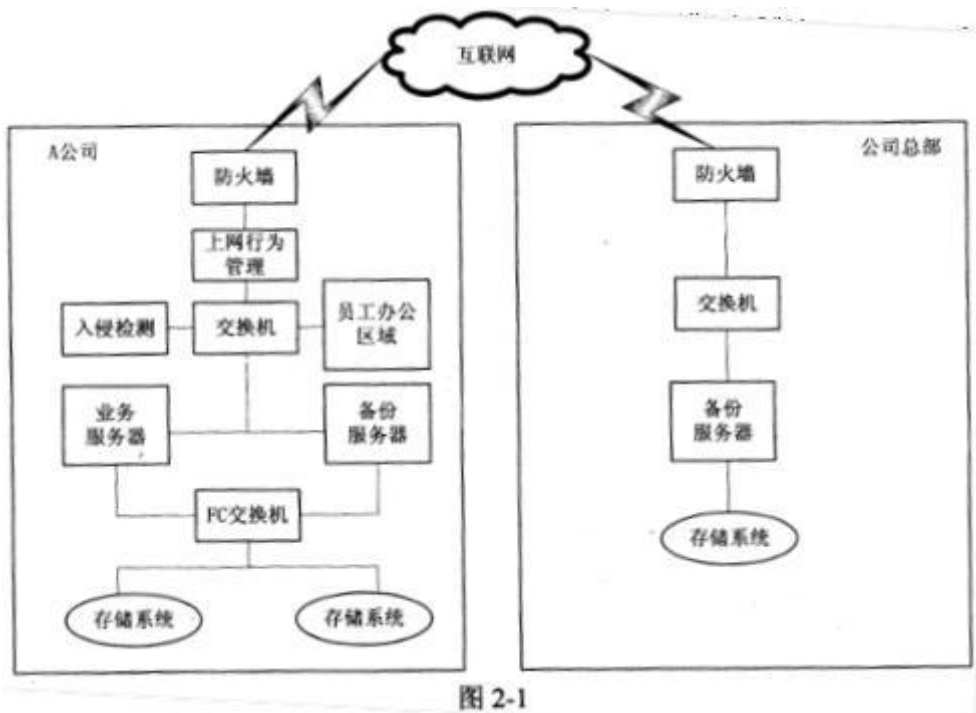
(10) 0.0.0.0 0.0.0.0 202.101.111.1

试题分析:

(9) 设置的是核心交换机的默认路由,正常情况下直接发往路由器的 g0/0/1 接口,当链路出现问题,才把数据包发往 switch2 (10) 在路由器上设置默认路由,下一跳指向互联网接口即公网网关 202.101.111.1

第 2 题:【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。

题：2.1 (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

题：2.2 (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	查看对象
2018-07-18 09:33:59	10.0.36.249	106.75.115.143	HTTP	高	C&C 通信	URL: http://1.7654.com/heirote/online?code=Yc1qsQ2c...
2018-07-18 09:22:45	10.0.36.249	106.75.115.143	HTTP	高	C&C 通信	URL: http://1.7654.com/heirote/kunbang?code=Yc1qsQ...
2018-07-18 09:07:53	10.0.36.249	106.75.115.143	HTTP	高	C&C 通信	URL: http://1.7654.com/heirote/jingpin?code=Yc1qsQ2...
2018-07-18 09:07:46	10.0.36.249	106.75.115.143	HTTP	高	C&C 通信	URL: http://1.7654.com/heirote/kunbang?code=Yc1qsQ...
2018-07-18 09:04:21	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/kuope...
2018-07-18 09:04:17	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/kunba...
2018-07-18 09:04:11	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/jingpin...
2018-07-18 09:03:41	10.0.36.249	106.75.115.143	HTTP	高	C&C 通信	URL: http://1.7654.com/heirote/jingpin?code=Yc1qsQ2...
2018-07-18 09:03:20	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/kunba...
2018-07-18 09:03:19	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/jingpin...
2018-07-18 08:51:19	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/kunba...
2018-07-18 08:51:18	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/jingpin...
2018-07-18 08:48:41	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/online...
2018-07-18 08:48:36	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/kunba...
2018-07-18 08:48:29	10.0.36.249	106.75.95.184	HTTP	高	C&C 通信	URL: http://kqzp.com/kuazipreport/kuazipreport/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

题: 2.3 (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	<input type="text"/>
本地掩码	<input type="text"/>
对方子网	<input type="text"/>
对方掩码	<input type="text"/>

图 2-3

题: 2.4 (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。

答案解析:

(1) A 数据完整性破坏

(2) D 数据加密

试题分析:

(1) 常见的外部威胁

病毒、蠕虫和特洛伊木马 - 在用户设备上运行的恶意软件和任意代码间谍软件和广告软件
用户设备上安装的软件, 秘密收集关于用户的信息零日攻击 (也称零小时攻击)

在出现漏洞的第一天发起的攻击黑客攻击由经验丰富的人员对用户设备或网络资源发起的攻击
拒绝服务攻击意图使网络设备上的应用和进程减缓或崩溃的攻击数据拦截和盗窃通过公司
网络捕获私人信息的攻击身份盗窃窃取用户的登录凭据来访问私人数据的攻击破坏数据完整性-数据被人为修改

答案解析:

(3) C 木马

(4) A 源主机安装杀毒软件并查杀

(5) C 将上图所示 URL 加入上网行为管理设备黑名单

试题分析:

(3) 从图中可以看出源主机始终是 10.0.36.249, 一直在访问相同的目的地主机和网页。说明这台主机可能中了病毒。跨站脚本攻击 (也称为 XSS) 指利用网站漏洞从用户那里恶意盗取信息。

拒绝服务攻击, 英文名称是 Denial of Service, 简称 DOS, 即拒绝服务, 造成其攻击行为被称为 DoS 攻击, 其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络, 使得所有可用网络资源都被消耗殆尽, 最后导致合法的用户请求无法通过。

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展, 使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验也参差不齐, 相当大一部分程序员在编写代码的时候, 没有对用户输入数据的合法性进行判断, 使应用程序存在安全隐患。用户可以提交一段数据库查询代码, 根据程序返回的结果, 获得某些他想得知的数据, 这就是所谓的 SQL Injection, 即 SQL 注入。

(4)(5) AC

因为是源主机一直在发起连接, 所以是在源主机上安装杀毒软件并进行查杀。

已经定位到是某台主机出现问题, 没必要使用漏洞扫描设备进行扫描。同时把 URL 加入上网行为管理的黑名单, 以禁止主机访问该网站。

答案解析:

(6) 10.0.35.0 (7) 255.255.255.252 (8) 10.0.86.200 (9) 255.255.255.255

试题分析:

(6) 题目中要求配置 vpn 对接之后需要互访的网段, 即配置感兴趣流本地子网和本地掩码指

的是本端访问对端的网段，对方子网和对方掩码指的是对端来访问本端的网段。同时题目中指



出仅允许 A 的备份服务器和业务服务器和总部的备份服务器通信。

所以本地网段是 10.0.35.0/30，而对端网段是主机 10.0.86.200/32

答案解析：

自动精简配置 (Thin Provisioning)，可以为客户虚拟出比实际物理存储更大的虚拟存储空间，为用户提供存储超分配的能力。只有写入数据的虚拟存储空间才能真正分配到物理存储，未写入的虚拟存储空间不占用物理存储资源。可以帮助客户大幅降低存储的初始投资成本。进行自动精简配置最大的问题就是有可能出现实际空间不足的情况。所以在自动精简配置中监控容量的是十分重要的。

第 3 题：【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

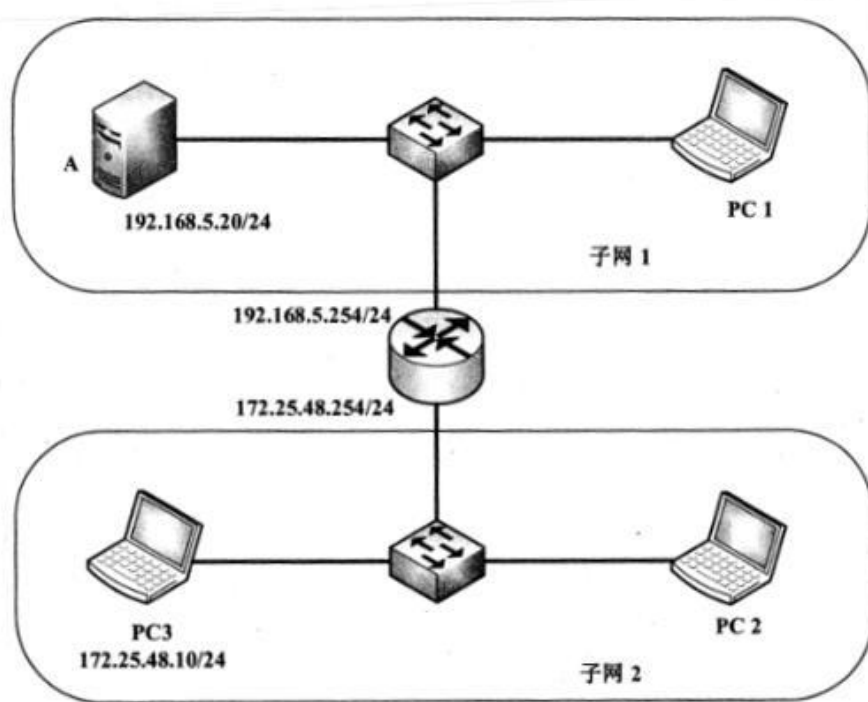


图 3-1

题：3.1 (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%

题: 3.2 (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

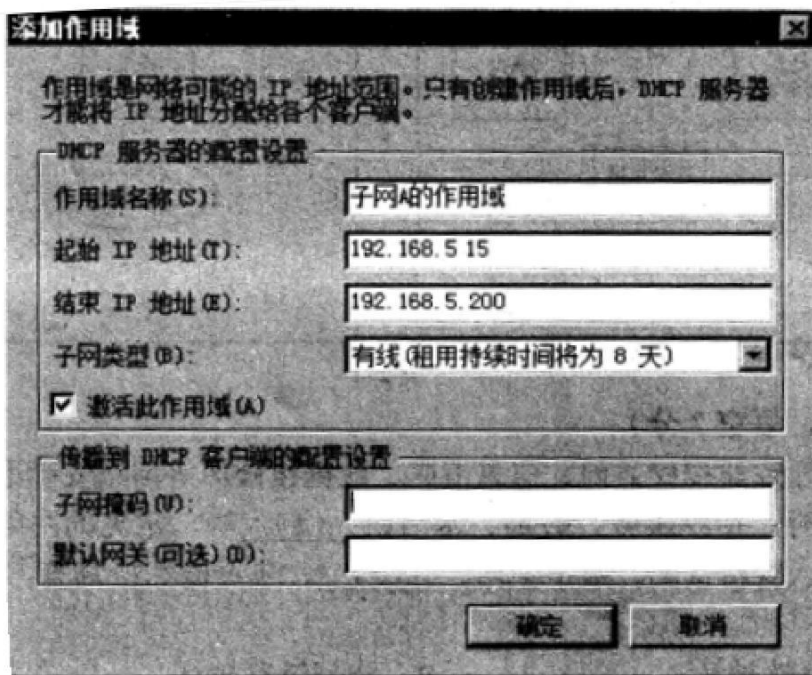


图 3-2

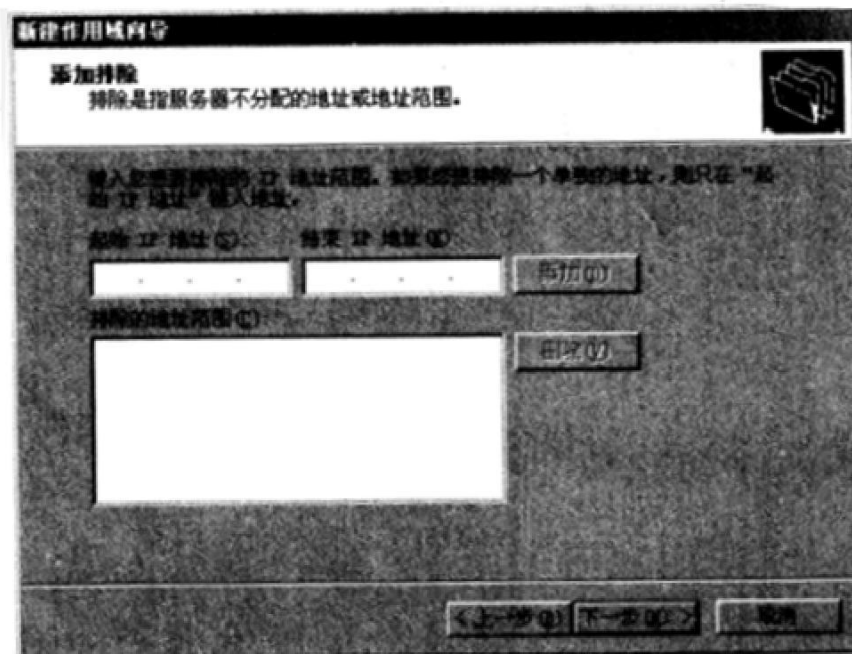


图 3-3

题：3.3 (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

答案解析：

(1)(2)(3) C D B

试题分析：

(1) A 或 C (此题有争议)，部分书本是描述 dhcp 的 4 个过程全是广播包。但是有些描述是服务器以单播回应。根据 RFC 文档，服务器回应数据包时，以单播还是广播回应取决于数据包中的 bootp flag 字段是否置 1。

(2) 代理 IP 可以用来隐藏真实 IP，类似于 NAT，访问网站是通过代理服务器来做一个中转，所以目标服务器只能看到代理服务器的 IP 地址 (3) 客户端主机获取到 ip 后，当租约到达 50%，会向服务器发送 dhcp request 报文延续租期。

答案解析：

(4) 2 (5) 255.255.255.0 (6) 192.168.5.254 (7) 192.168.5.20 (8) D

试题分析：

(4) 图中有 2 个子网，需要给 2 个子网分配 ip 地址。所以需要 2 个作用域 (5) 可以从图 3-1 中看出子网 A 的掩码是 24 位，所以子网掩码是 255.255.255.0

(6) 默认网关是路由器的接口 192.168.5.254 (7) 分配 ip 的范围为

学习交流群：460763000

192.168.5.15—192.168.5.200, dhcp 服务器的 ip192.168.5.20 在这个范围内, 所以需要排除掉这个地址 (8) 通过无线获取的 ip 地址, 租约一般以小时为单位

答案解析:

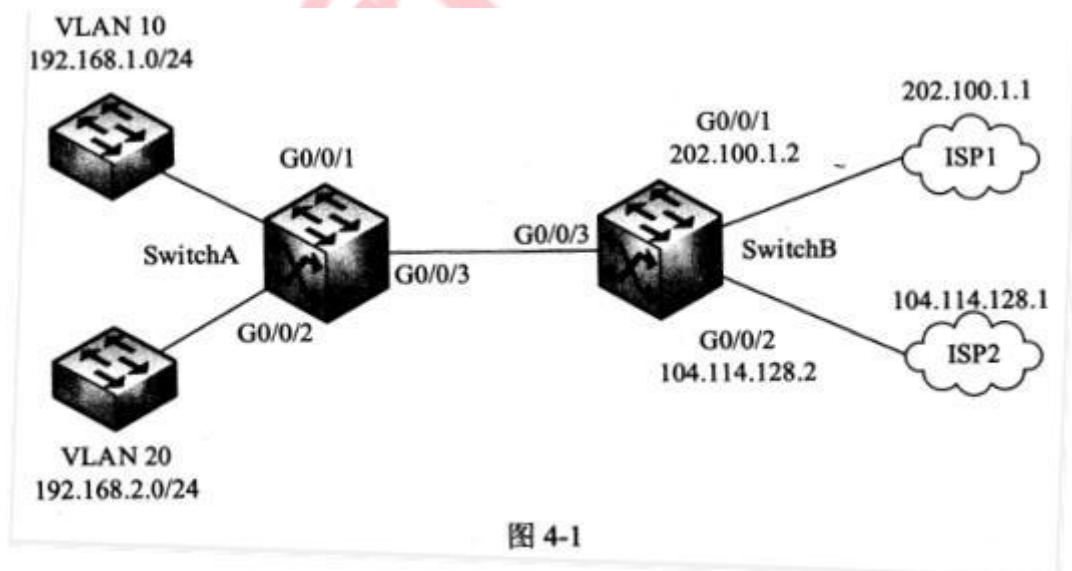
(9) C (10) 255.255.0.0

试题分析:

(9)(10) 当获取不到 ip 时, 会自动获取一个 169.254.0.0/16 网段中的地址

第 4 题:【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。



题: 4.1 (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-classifer-c2]
if-match acl( 5 ) [SwitchB-classfer-c2]( 6 ) quit [SwitchB] traffic
behavior b0 [SwitchB-behavior-b0](7) [SwitchB-behavior-b0] quit
[SwitchB] traffic behavior bl [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-GigabitEthenet0/0/3] traffic-policy
pl( 13 ) SwitchB-GigabitEthernet0/0/3] return 题： 4.2 (2 分)
```

在问题 1 的配置代码中，配置 ACL 3000 的作用是:(14)。题： 4.3 (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 )
```

.....

答案解析:

- (1) 192.168.1.0 (2) Source (3) If-match (4) Operator (5) 3002
(6) Quit (7) Permit (8) 202.100.1.1 (9) 104.114.128.1 (10) b0
(11) b1 (12) Gigabitethernet0/0/3 (13) Inbound

试题分析:

(1) 由题知, 是过滤出内网 192.168.1.0/24 的流量 (2) 和上一空语句类似, 内网作为源 (3) 定义流分类, 设置匹配 (4) Operator 是可选参数, 按照下面语句照抄即可 (5) 该流分类匹配 acl3002 (6) Quit 退出到系统视图 (7) 定

义流行为为允许 permit (8) 定义流行为, 该语句指代设置下一跳 (9) 同 8 问类似 (10) 将流分类和流行为关联起来, 组成流策略 (11) 同 10 问类似 (12) 进入到 g0/0/3 接口 (13) 在接口入方向调用该策略

答案解析:

(14) 过滤出内网需要互访的流量, 允许其通过

答案解析:

(15) Permit (16) 2000 (17) 2001 (18) G0/0/3 (19) G0/0/3

试题分析:

(15) 做 nat 转换, 通过基本 acl 把内网流量过滤出来 (16) 将 acl 表和地址池关联起来 (17) 和 16 问类似 (18) (19) 设置静态路由, 指向内网的流量从接口 G0/0/3 出去