**全国计算机技术与软件专业技术资格（水平）考试**

**2014年上半年 网络工程师 下午试卷**

（考试时间 14:00～16:30 共 150 分钟）

|  |
| --- |
| **请按下述要求正确填写答题纸** |

1.在答题纸的指定位置填写你所在的省、自治区、直辖市、计划单列市的名称。

2.在答题纸的指定位置填写准考证号、出生年月日和姓名。

3.答题纸上除填写上述内容外只能写解答。

4.本试卷共 4 道题，都是必答题，满分 75 分。

5.解答时字迹务必清楚，字迹不清时，将不评分。

6.仿照下面例题，将解答写在答题纸的对应栏内。

**例题**

2014年上半年全国计算机技术与软件专业技术资格（水平）考试日期是（1）

月（2）日。

因为正确的解答是“5 月 20 日”，故在答题纸的对应栏内写上“5”和“20”

（参看下表）。

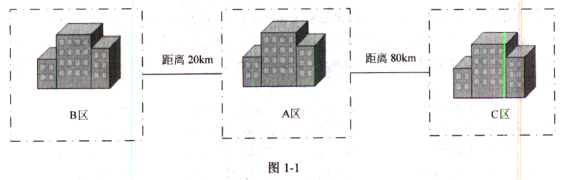
|  |  |
| --- | --- |
| 例题 | 解答栏 |
| （1） | 5 |
| （2） | 20 |

**试题一（共20分）**

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】**

某单位计划部署园区网络，该单位总部设在A区，另有两个分别设在B区和C区，各个地区之间距离分布如图1-1所示。



该单位的主要网络业务需求在A区，在网络中心及服务器机房亦部署在A区；B的网络业务流量需求远大于C区；c区的虽然业务流量小，但是网络可靠性要求高。根据业务需要，要求三个区的网络能够互通并且都能够访问互联网，同时基于安全考虑单位要求采用一套认证设备进行身份认证和上网行为管理。

**【问题1】**

为了保障业务需求，该单位采用两家运营商接入internet。根据题目需求，回答下列问题；

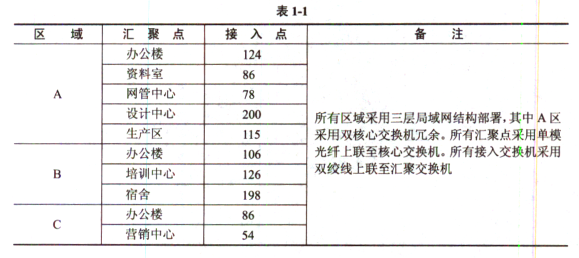
1. 两家运营商的internet接入线路应部署在哪个区？为什么？

2. 网络运营商提供的mpls vpn和千兆裸光纤两种互联方式，哪一种可靠性高？为什么？

3. 综合考虑网络需求及运营成本，在AB区之间与AC区之间分别采用上述那种方式进行互联？

**【问题2】**

该单位网络部署接入点情况如表1-1所示

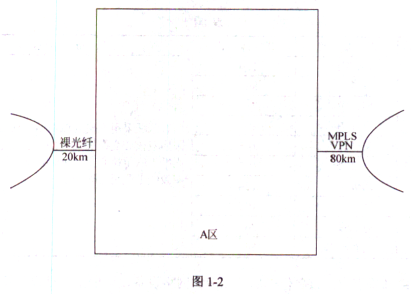


根据网路部署需求，该单位采购了相应的网络设备，请根据题目说明及表所规定1-2所示的设备数量及合理的部署位置（注：不考虑双绞线的距离限制）。



**【问题3】**

根据题目要求，在图1-2的方框中画出该单位A区网络拓扑示意图（汇聚层以下不画）。

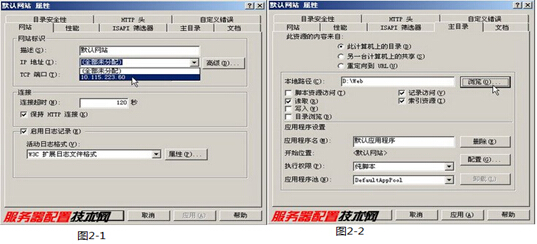


**试题二（共15分）**

阅读以下说明，回答问题1至问题5,将解答填入答题纸对应的解荇栏内。

**【说明】**

某公司采用winserver2003操作系统搭建该公司的企业网站，要求用户在浏览器地址必须输入https://www.gongsi.com/index,.html或https://117.112.89.67/index.html来访问该公司的网站。其中，index.html文件存放在网站服务器E:\gsdata目录中。在服务器上安装完成iis6.0后网站属性窗口[网站]，[主目录]选项卡分别如图2-1



**【问题1】**

1.按照题目说明。图2-1中的‘ip地址’文本框中的内容为（1）：SSL端口文本框内容为（2）

2.按图2-2中，本地路径文本框中的内容为（3）；同时要保障用户通过题目要求的方式来访问网址，必须至少勾选（4）复选框。

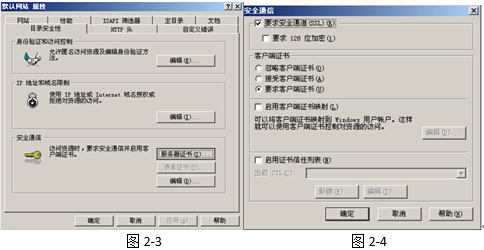
（4）备选答案

A,脚本资源访问 B,读取 C,写入 D.目录浏览

**【问题2】**

1.配置该网站时，要在如图2-3所示【目录安全性】选项卡中单击【服务器证书】来获取服务器证书，其中获取服务器证书的步骤顺序如下：①生产证书请求文件，②（5），③从CA导出证书文件④在IIS服务器上导入并安装证书。

配置完成后，当用户登陆该网站时，通过验证CA的签名来确认数字证书的有效性，从而（6）。CA颁发给web网站的数字证书不包括（7）。



6-7备选答案：

（6）A.验证网站的真伪 B.判断用户的权限，C.加密发完服务器的数据 D.解密所接受的客户端数据

（7）A.证书的有效期 B.网站的公钥 C.证书的序列号 D.网站的私钥

**【问题3】**

配置该网站时，在图2-3的窗口中单击【安全通信】栏目中的【编辑】按钮，弹出如图2-4所示窗口，按题目要求。客户端浏览器只能通过https方式访问服务器，此时应勾选图2-4中的（8）框，如果要求客户端和服务器进行双向认证，此时应勾选图2-4的（9）框。

**【问题4】**

HTTPS用于在客户计算机和服务器之间提供安全通信，广泛用于因特网上安全敏感的应用，例如（10）应用。

HTTPS使用安全套接字层（SSL）进行信息交换。SSL目前版本是3.0，被IETFf定义在RFC6101中。IETF对SSL进行升级后的继任者是（11）。

（10）备选答案如下：

A.网络聊天 B.网络视频 C.网上交易 D.网络下载

**【问题5】**

使用https能不能确保服务器自身安全？

**试题三（共20分）**

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】**

某单位网络拓扑结构如图3-1所示，在linux系统下构建DNS服务器，在DHCP服务器和web服务器。要求如下。

1. 路由器连接各个子网的接口信息如下：

（1） 路由器e0的ip地址192.168.1.1/25

（2） 路由器e1的ip地址192.168.1.129/25

（3） 路由器e2的ip地址192.168.2.1/25

（4） 路由器e3的ip地址192.168.2.33/25

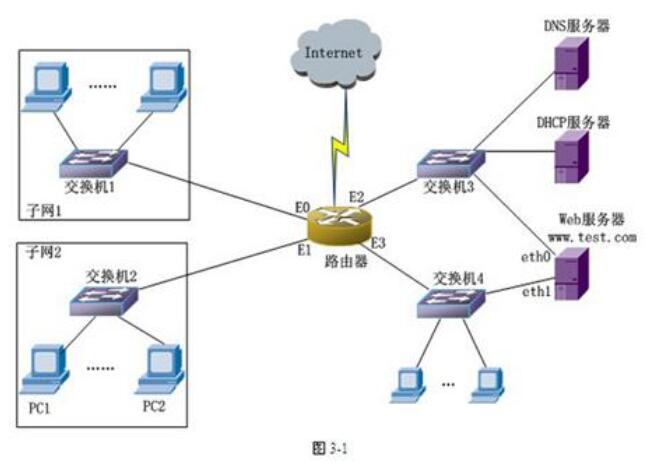
2.子网1和子网2内的客户机通过DHCP服务器动态分配ip地址：

3.服务器设置固定的IP地址，其中

（1）DNS服务器采用bind构建，IP地址为192.168.2.2

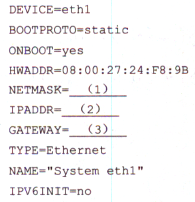
（2）DHCP服务器IP地址为192.168.2.3

（3）web服务器网卡eth0的IP地址为192.168.2.4,eth1的IP地址为192.168.2.34



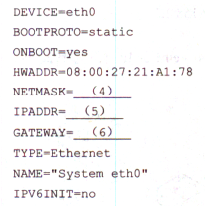
**【问题1】**

请完成图3-1中web服务器eth1的配置。



**【问题2】**

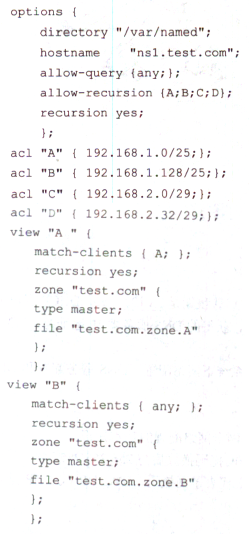
请完成图3-1中DNS服务器网卡的配置。



**【问题3】**

在（7）（8）（9）处填写恰当的内容。

在Linux系统中设置域名解析服务器，已知域名服务器上文件named.conf 的部分内容如下：



test.com.zone.A文件的部分配置如下: WWW IN A 192.168.2.4

test.com.zone.B文件的部分配置如下:WWW IN A 192.168.2.34

IP地址（7）不允许使用该DNS进行递归查询，子网1和子网2中的客户端访问www.test.com时，该DNS解析返回的IP地址分别为（8）和（9）。

(7) 备选答案：

A. 192.168.1.8 B.192.168.1.133

C. 192.168.2.10 D.192.168.2.6

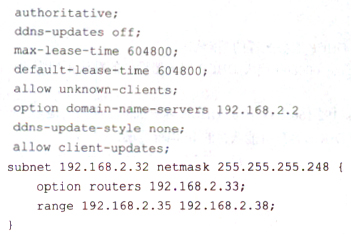
(8) 和（9)备选答案：

A. 192.168.2.4 B.192.168.2.34

C. 192.168.2.4 或者192.168.2.34 D.192.168.2.3 和192.168.2.34

**【问题4】**

DHCP服务器配置文件如下所示：



根据这个文件内容。该DHCP服务器默认租期是（10）天，DHCP客户机能获得IP地址范围是从（11）到（12），获得DNS服务器IP地址为（13）。

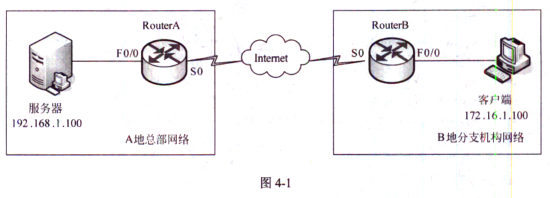
**试题四（共20分）**

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。

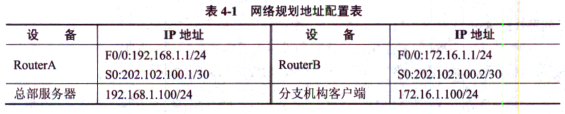
**【说明】**

某企业总部设立在A地，在B地有分支机构，分支机构和总部需要在网络上进行频繁的数据传输，该企业采用IPSec VPN虚拟专用技术实现分支机构和总部之间安全，快捷，经济的跨区域网络连接。

该企业网络拓扑结构如图4-1所示：

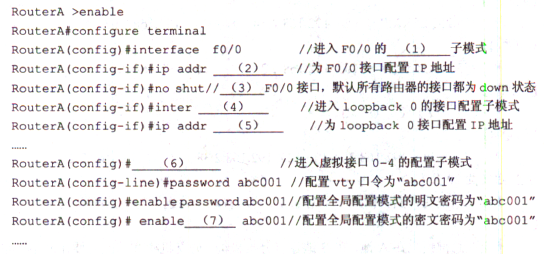


该企业网络地址规划与配置如表4-1所示。



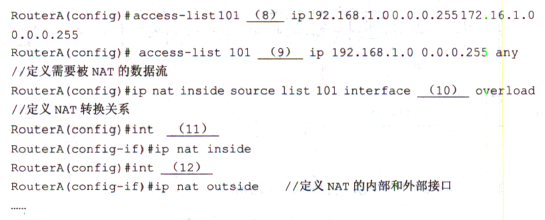
**【问题1】**

为了完成对routerA和routerB远程连接管理，以routerA为例，完成初始化路由器，并配置routerA的远程管理地址（192.168.1.20），同时开启routerA的telent功能并设置全局模式访问密码，请补充下列配置命令。



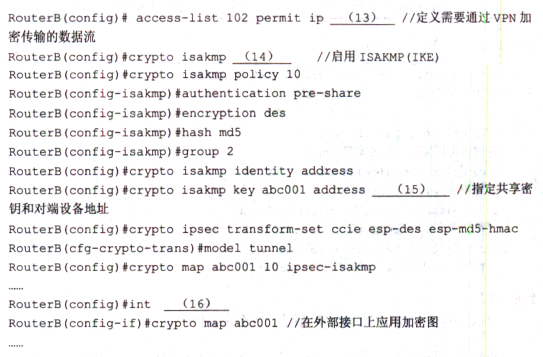
**【问题2】**

VPN是建立在两个局域网出口之间的隧道连接，所以两个VPN设备必须能够满足内网访问互联网的要求，以及需要配置NAT。按照题目要求以RouterA为例，请补充完成下列配置命令。



**【问题3】**

配置IPSec VPN时要注意隧道两端的设备配置参数必须对应匹配，否则VPN配置将会失败。以RouterB为例配置IPSec VPN，请完成相关配置命令。



**【问题4】**

根据题目要求，企业分支机构与总部之间采用IPSec VPN技术互连，IPSec (IP Security)是IETF为保证在Internet上传送数据的安全保密性而制定的框架协议，该协议应用在 （17) 层，用于保证和认证用户IP数据包。

IPSec VPN可使用的模式有两种，其中（18) 模式的安全性较强，(19)模式的安全性较弱。IPSec主要由AH、ESP和IKE组成，在使用IKE协议时，需要定义IKE协商策略，该策略由（20) 进行定义。