

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）。

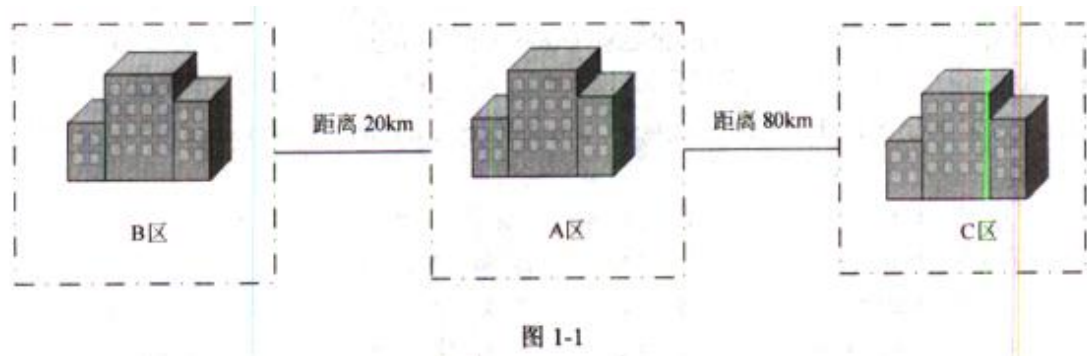
例题	解答栏
（1）	5
（2）	20

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

表 1-1

区 域	汇 聚 点	接 入 点	备 注
A	办公楼	124	所有区域采用三层局域网结构部署,其中 A 区采用双核心交换机冗余。所有汇聚点采用单模光纤上联至核心交换机。所有接入交换机采用双绞线上联至汇聚交换机
	资料室	86	
	网管中心	78	
	设计中心	200	
	生产区	115	
B	办公楼	106	
	培训中心	126	
	宿舍	198	
C	办公楼	86	
	营销中心	54	

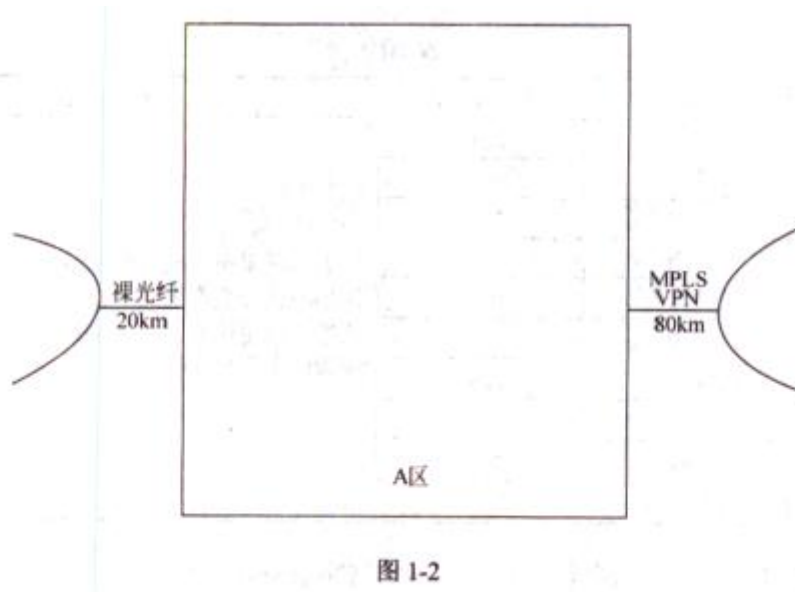
根据网路部署需求,该单位采购了相应的网络设备,请根据题目说明及表所规定 1-2 所示的设备数量及合理的部署位置(注:不考虑双绞线的距离限制)。

表 1-2

设 备 类 型	设 备 数 量	部 署 区 域
核心交换机	(1)	A 区
核心交换机	1	B 区
核心交换机	1	C 区
汇聚交换机	5	A 区
汇聚交换机	3	B 区
汇聚交换机	2	C 区
SFP 单模模块	5	(2) 区
SFP 单模模块	7	(3) 区
SFP 单模模块	22	(4) 区
24 口接入交换机	(5)	A 区
24 口接入交换机	(6)	B 区
24 口接入交换机	(7)	C 区
千兆服务器接入交换机	1	A 区
服务器	3	A 区
路由器	1	(8) 区
认证及流控设备	1	A 区
防火墙	1	A 区

【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符栏内。

【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



图2-1



图2-2

【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）。



图 2-3



图 2-4

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端进行双向认证，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端之间提供安全通信，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 IETF 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

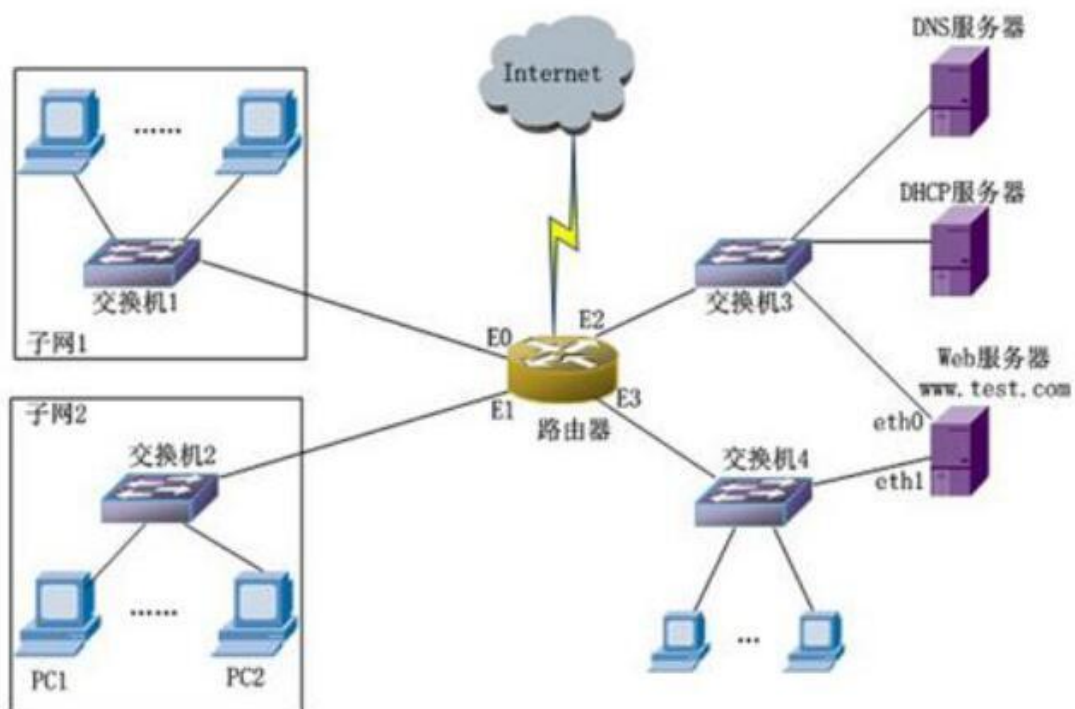


图 3-1

【问题 1】

请完成图 3-1 中 web 服务器 eth1 的配置。

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:24:F8:9B
NETMASK= (1)
IPADDR= (2)
GATEWAY= (3)
TYPE=Ethernet
NAME="System eth1"
IPV6INIT=no
```

【问题 2】

请完成图 3-1 中 DNS 服务器网卡的配置。

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:21:A1:78
NETMASK= (4)
IPADDR= (5)
GATEWAY= (6)
TYPE=Ethernet
NAME="System eth0"
IPV6INIT=no
```

【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：

```
authoritative;
ddns-updates off;
max-lease-time 604800;
default-lease-time 604800;
allow unknown-clients;
option domain-name-servers 192.168.2.2;
ddns-update-style none;
allow client-updates;
subnet 192.168.2.32 netmask 255.255.255.248 {
    option routers 192.168.2.33;
    range 192.168.2.35 192.168.2.38;
}
```

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：

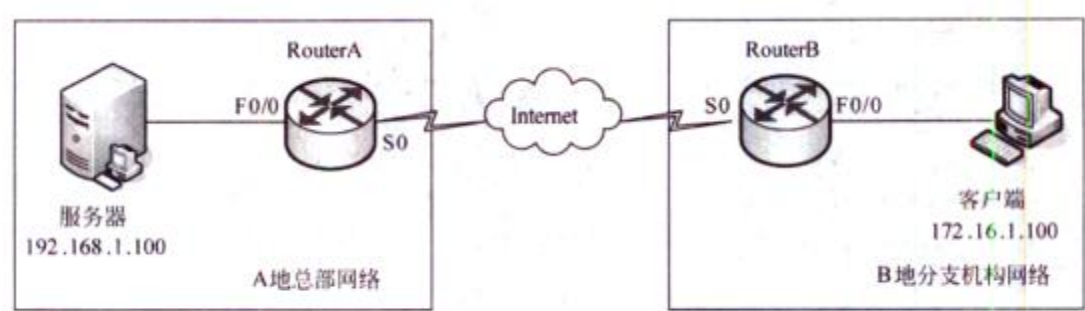


图 4-1

该企业网络地址规划与配置如表 4-1 所示。

表 4-1 网络规划地址配置表

设 备	IP 地址	设 备	IP 地址
RouterA	F0/0:192.168.1.1/24 S0:202.102.100.1/30	RouterB	F0/0:172.16.1.1/24 S0:202.102.100.2/30
总部服务器	192.168.1.100/24	分支机构客户端	172.16.1.100/24

【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 telnet 功能并设置全局模式访问密码，请补充下列配置命令。

```

RouterA >enable
RouterA#configure terminal
RouterA(config)#interface f0/0 //进入 F0/0 的 (1) 子模式
RouterA(config-if)#ip addr (2) //为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut // (3) F0/0 接口, 默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter (4) //进入 loopback 0 的接口配置子模式
RouterA(config-if)#ip addr (5) //为 loopback 0 接口配置 IP 地址
.....
RouterA(config)# (6) //进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001 //配置 vty 口令为"abc001"
RouterA(config)#enable password abc001 //配置全局配置模式的明文密码为"abc001"
RouterA(config)# enable (7) abc001 //配置全局配置模式的密文密码为"abc001"
.....

```

【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。

```

RouterA(config)#access-list 101 (8) ip 192.168.1.0 0.0.0.255 172.16.1.0
0.0.0.255
RouterA(config)# access-list 101 (9) ip 192.168.1.0 0.0.0.255 any
//定义需要被 NAT 的数据流
RouterA(config)#ip nat inside source list 101 interface (10) overload
//定义 NAT 转换关系
RouterA(config)#int (11)
RouterA(config-if)#ip nat inside
RouterA(config)#int (12)
RouterA(config-if)#ip nat outside //定义 NAT 的内部和外部接口
.....

```

【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。

```

RouterB(config)# access-list 102 permit ip ____ (13) ____ //定义需要通过VPN加密传输的数据流
RouterB(config)#crypto isakmp ____ (14) ____ //启用 ISAKMP (IKE)
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#group 2
RouterB(config)#crypto isakmp identity address ____
RouterB(config)#crypto isakmp key abc001 address ____ (15) ____ //指定共享密钥和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
RouterB(cfg-crypto-trans)#model tunnel
RouterB(config)#crypto map abc001 10 ipsec-isakmp
.....
RouterB(config)#int ____ (16) ____
RouterB(config-if)#crypto map abc001 //在外部接口上应用加密图
.....

```

【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。