2014 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 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，另有两个分部分别设在 B 区和 C 区，各个地区之间的距离分部如图 1-1 所示。

图 1-1

该单位的主要网络业务需求在 A 区，网络中心及服务器机房亦部署在 A 区；B 区的网络业务流量需求远大于 C 区；C 区虽然业务量小，但是网络可靠性高。根据业务需求，要求三个区的网络能够互联互通并且都能访问互联网。同时基于安全考虑，该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】（6 分）

为保障业务需求，该单位采用两家运营商接入 Internet。根据题目需求，回答以下问题：

1.两家运营商的 Internet 接入线路应部署在哪个区？为什么？

2.网络运营商提供了 MPLSVPN 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行成本，AB 区之间与 AC 区之间分别采用上述哪种方式进行互联？

【问题 2】（8 分）

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。所有冗余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	

根据网络部署需求，该单位采购了相应的网络设备，请根据题目说明及表 1-1,确 定表 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】（6 分）

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

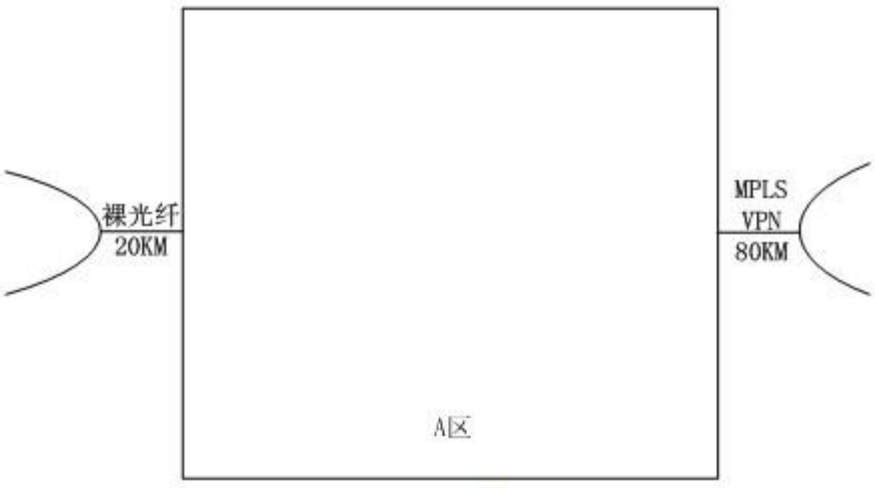

图 1-2

● 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答栏内。

【说明】

某公司采用 Windows Server 2003 操作系统搭建该公司的企业网站，要求用户在浏览器地址栏必须输入 https://www.gQngsi.com/index.html 或 https://117.112.89.67/index.html 来访问该公司网站。其中，index.html 文件存放在网站所在服务器 E:\gsdata 目录中。在服务器上安装完成 IIS6.0 后，网站的属性窗口【网站】、【主目录】选项卡分别如图 2-1 和图 2-2 所示。

图 2-1

图 2-2

【问题 1】（4 分）

1.按照题目说明，图 2-1 中的“IP 地址”文本框中的内容应为（1）；“SSL 端口”文本框中的内容为（2）。

2.在图 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站，必须至少勾选（4）复选框。

（4）备选答案：

（2）A．脚本资源访问　　B．读取　　C．写入　　D．目录浏览

【问题 2】（6 分）

1.配置该网站时，需要在如图 2-3 所示的【目录安全性】选项卡中单击【服务器证书】按钮来获取服务器证书。其中获取服务器证书的步骤顺序如下：①生成证书请求文件；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，当用户登录该网站时，通过验证 CA 的签名来确认该数字证书的有效性，从而（6），CA 颁发给 Web 网站的数字证书中不包括（7）。

图 2-3

图 2-4

（6）~（7）备选答案：

（6）

（3）A．验证网站的真伪　　B．判断用户的权限

C．加密发往服务器的数据　　D．解密所接受的客户端数据

（7）

（4）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】（2 分）

配置该网站时，在图 2-3 所示的窗口中单击【安全通信】栏目中的【编辑】按钮，弹出如图 2-4 所示的窗口。按照题目要求，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，此时应该勾选图 2-4 中的（9）框。

【问题 4】（2 分）

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 目前的版本是 3.0，被 IETF 定义在 RFC 6101 中。IETF 对 SSL 讲行升级后的继任者是（11）。

（10）备选答案如下：

（5）A．网络聊天　　B．网络视频　　C．网上交易　　D．网络下载

【问题 5】（1 分）

使用 HTTPS 能不能确保服务器自身的安全？

●

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、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 口的 IP 地址为 192.168.1.1/25；

（2）路由器 E1 口的 IP 地址为 192.168.1.129/25；
（3）路由器 E2 口的 IP 地址为 192.168.2.1/29；
（4）路由器 E3 口的 IP 地址为 192.168.2.33/29。
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 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 ethO 的 IP 地址为 192.168.2.4, ethl 的 IP 地址为 192.168.2.34。

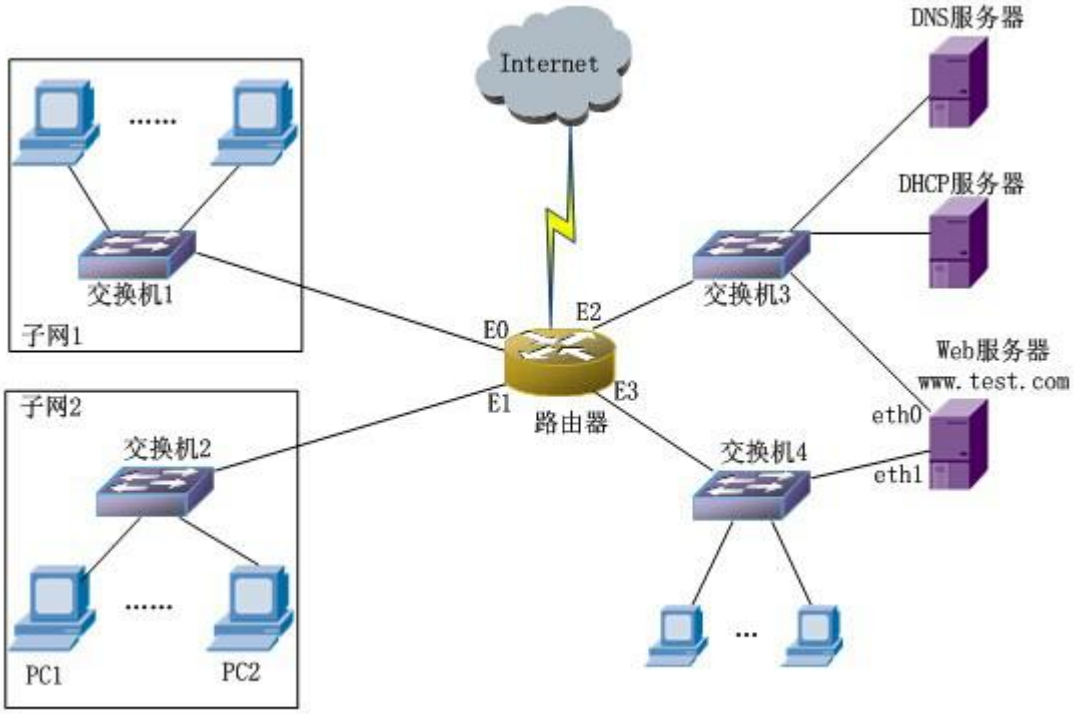

图 3-1

【问题 1】（3 分）

请完成图 3-1 中 Web 服务器 eth1 的配置。

DEVICE=eth1
BOOTPROTE=static
ONBOOT=yes
HWADDR=08:00:27:24:F8:9B
NETMASK=（1）
IPADDR=（2）
GATEWAY=（3）
TYPE=Ethernet
NAME="Syestem eht1"
IPV6INT=no

【问题 2】（3 分）

请完成图 3-1 中 DNS 服务网卡的配置。

DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:21:A1:78
NETMASK=（4）

IPADDR=（5）
GATEWAY=（6）
TYPE=Ethernet
NAME="Syestem eht0"
IPV6INT=no

【问题 3】（6 分）

请在（7）、（8）、（9）处填写恰当的内容。

在 Linux 系统中设置域名解释服务器，一直改域名服务器上文件 named.conf 的部分内容如下：

```
options {
  directory "/var/named";
  hostname  "ns1.test.com"
  allow-query    {any;};
  allow-recursion   {A;B;C;D};
  Recursion yes;
  };
acl "A"{192.168.1.0/25;};
acl "B"{192.168.1.128/25;};
acl "C"{192.168.2.0/29};
acl "D"{192.168.2.32/29;};
view "A"{
    Match-clients{A;};
    Recursion yes;
    Zone "test.com" {
    Type master;
    File "test.com.zone.A"
    };
    };
view "B"{
    Match-clients {any;};
    Recursion yes;
    Zone "test.com" {
    type master;
    file "test.com.zone.B"
    };
    };
```

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：

（3）A．192.168.1.8　　B．192.168.2.34

C．192.168.2.10　　D．192.168.2.6

（8）和（9）备选答案：

（4）A．192.168.2.4　　B．192.168.2.34

C．192.168.2.4 或者 192.168.2.34　　D．192.168.2.4 和 192.168.2.34

【问题 4】（8 分）

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;
}
```

根据这个文件中的内容，该 DHCP 服务的默认租期是（10）天，DHCP 客户机能 获得的 IP 地址范围是：从（11）到（12）获得的 DNS 服务器 IP 地址为（13）。

● 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 地建有分支机构，分支机构和总部需要在网络上进 行频繁的数据传输，该企业网络采用 IPSec VPN 虚拟专用网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。

该企业的网络拓扑结构如图 4-1 所示。

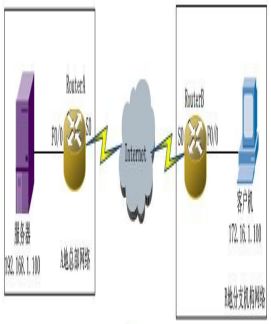

图 4-1

该企业的网络地址规划及配置如表 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】（7 分）

为了完成对 RouterA 和 RouterB 的远程连接管理，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 功能并设置全局配置模式的访问密码，请补充完成下列配置命令。

```
RouterA >enable
RouterA#configure terminal
RouterA(config)#interface f0/0                    //进入 F0/0 的 (1) 于模式
RouterA(config-if)#ip addr (2)   //为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut //   (3) FO/O 接口，默认所有路由器的接口都为 down 状态
RouterA(config-iQ#inter (4) //进入 loopback 0 的接口配置子模式
RouterA(config-if)#ip addr (5) // 为 loopback0 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(config4ine)#pass word abc00 1　　//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】（5 分）
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-iQ#ip nat outside　//定义 NAT 的内部和外部接 口
【问题 3】(4 分)
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 IPSecVPN，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 abcOOl 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 abcOOl 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 IETE 为保证在 Internet 上传送数据的安全保密性而制定的框架协议，该协议用用在 17 层，用于保证和认证用户 IP 数据包。
IP S ec 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。