2017 年下半年网络工程师下午真题+答案

详细解析完整版

第 1 题：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】

某企业组网方案如图 1-1 所示，网络接口规划如表 1-1 所示。公司内部员工和外部访客均可通过无线网络访问企业网络，内部员工无线网络的 SSID 为 Employee，访客无线网络的 SSID 为 Visitor。

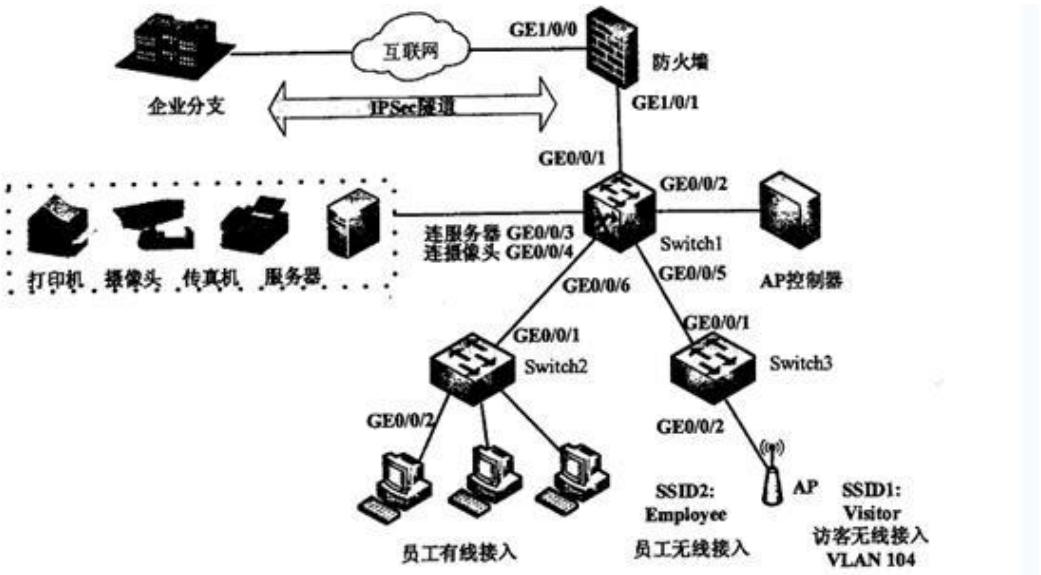

图1-1

表1-1

设备名	接口编号	所属VLAN	IP地址
防火墙	GE1/0/0	-	200.1.1.1/24
	GE1/0/1	-	192.168.99.254/24
AP控制器	GE0/0/1	10	VLANIF10:192.168.10.1/24
Switch1	GE0/0/1	99	VLANIF10:192.168.10.254/24
	GE0/0/2	10	VLANIF99:192.168.99.1/24
	GE0/0/3	101	VLANIF100:192.168.100.1/24
	GE0/0/4	102	VLANIF101.192.168.101.1/24
	GE0/0/5	100、103、104	VLANIF102:192.168.102.1/24
	GE0/0/6	100	VLANIF103:192.168.103.1/24
			VLANIF104:192.168.104.1/24
Switch2	GE0/0/1	100	-
	GE0/0/2	100	-
Switch3	GE0/0/1	100、103、104	-
	GE0/0/2	100、103、104	-

题：1.1 （6 分）

防火墙上配置 NAT 功能，用于公私网地址转换。同时配置安全策略，将内网终端用户所在区域划分为 Trust 区域，外网划分为 Untrust 区域，保护企业内网免受外部网络攻击。补充防火墙数据规划表 1-2 内容中的空缺项。

表1-2

安全策略	圆安全域	目的安全域	源地址/区域	目的地址/区域
egress	trust	untrust	192.168.100.0/24 192.168.101.0/24 192.168.103.0/24 192.168.104.0/24	-
Local_untrust	Local	untrust	(1)	200.1.1.2/32
untrust_Local	untrust	Local	untrust	(2)
NAT策略（转换前）	trust	untrust	srcip	(3)

注：Local 表示防火墙本地区域；srcip 表示源 ip。

题：1.2 （4 分）

在点到点的环境下，配置 IPSec VPN 隧道需要明确（ 4）和（5）题：1.3 （6 分）

在 Switch1 上配置 ACL 禁止访客访问内部网络，将 Switch1 数据规划表 1-3 内容中的空缺项补充完整。

表1-3

项目	VLAN	源IP	目的IP	动作
ACL	(6)	(7)	192.168.100.0/0.0.0.255 192.168.101.0/0.0.0.255 192.168.102.0/0.0.0.255 192.168.103.0/0.0.0.255	(8)

题：1.4 （4 分）

AP 控制器上部署 WLAN 业务，采用直接转发，AP 跨三层上线。认证方式：无线用户通过预共享密钥方式接入。

在 Switch1 上 GEO/O/2 连接 AP 控制器，该接口类型配置为(9)模式，所在 VLAN 是(10)。

答案解析：

1、192.168.99.0/24

2、200.1.1.1/32

3、0.0.0.0/0 或 any

答案解析：

4-5 隧道的源目 IP 地址

答案解析：

6、vlan104

7、192.168.104.0/0.0.0.255

8、deny

答案解析：

9、access

10、VLAN 10

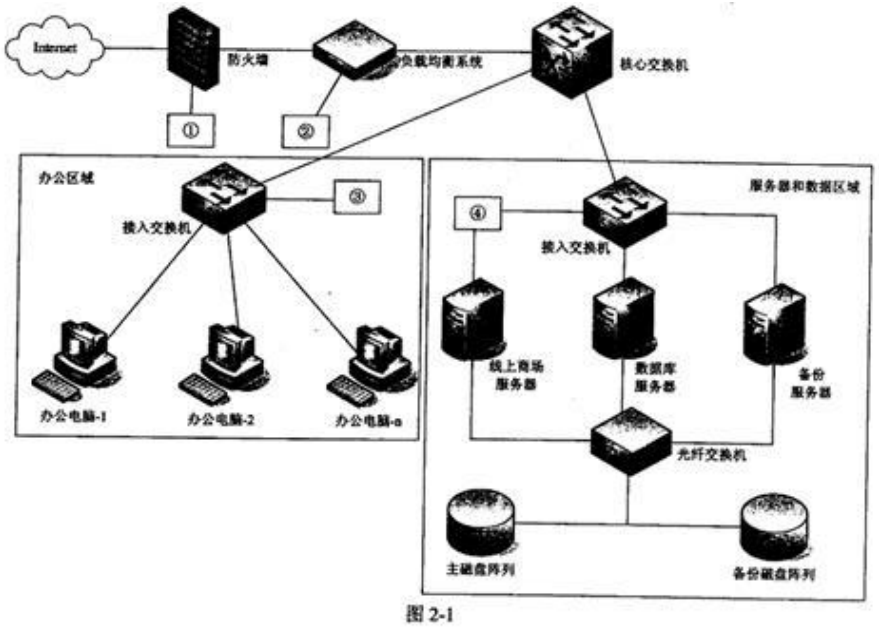

图 2-1

由说明可知，企业网通过 IPSec 隧道与分支相连，因此需要配置隧道的源目 IP 地址。Local 代表防火墙本地区域，即直连网段。要通过 ACL 实现访问控制：禁止访客访问内部网络。访客对应网段为 VLAN104 即 192.168.104.0/24，动作应该为 deny. AP 控制器连接在核心交换机的 GE0/0/2 端口，对应说明所属于 VLAN 为 100.因此端口类型为 access。

第 2 题:（共 20 分）

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 是某企业网络拓扑，网络区域分为办公区域、服务器区域和数据区域，线上商城系统为公司提供产品在线销售服务。公司网络保障部负责员工办公电脑和线上商城的技术支持和保障工作。

题：2.1 （6 分）

某天，公司有一台电脑感染“勒索”病毒，网络管理员应采取（1 ）、（2）、（3）措施。

（1）~（3）备选答案：

A. 断开已感染主机的网络连接 B. 更改被感染文件的扩展名

C. 为其他电脑升级系统漏洞补丁

D. 网络层禁止 135/137/139/445 端口的 TCP 连接

E. 删除已感染病毒的文件题：2.2 （8 分）

图 2-1 中，为提高线上商城的并发能力，公司计划增加两台服务器，三台服务器同时对外提供服务，通过在图中（4）设备上执行（5）策略，可以将外部用户的访问负载 平均分配到三台服务器上。

(5) 备选答案：A. 散列 B. 轮询 C. 最少连接 D. 工作-备份

其中一台服务器的 IP 地址为 192.168.20.5/27，请将配置代码补充完整。ifcfg-eml 配置片段如下：

DEVICE=eml TYPE=Ethernet

UUID=36878246-2a99-43b4-81df-2db1228eea4b ONBOOT=yes

NM_CONTROLLED=yes
BOOTPROTO=none
HWADDR=90:B1:1C:51:F8:25

IPADDR=192.168.20.5 NETMASK=（6）GATEWAY=192.168.20.30 DEFROUTE=yes IPV4_FAILURE_FATAL=yes IPV6INTI=no
配置完成后，执行 systemct1（7）network 命令重启服务。题：2.3 （4 分）
网络管理员发现线上商城系统总是受到 SQL 注入、跨站脚本等攻击，公司计划购置（8）设备/系
统，加强防范；该设备应部署在图 2-1 中设备①~④的（9）处。
A．杀毒软件 B．主机加固 C．WAF（Web 应用防护系统）D．漏洞扫描题：2.4 （2 分）
图 2-1 中，存储域网络采用的是（10）网络。
答案解析：1-3：A D C
答案解析：4、负载均衡系统 5、B6、255.255.255.2247、restart
答案解析：8、C9、4
答案解析：10、FC-SAN
勒索病毒利用的是 Windows 系统漏洞，通过系统默认开放 135、137、445 等文件共享端口发起的病毒攻击。因此应该要先将感染的主机断开网络连接，然后将其它主机也断开连接，并禁止共享端口，然后升级操作系统。
实现负载均衡可直接在此网络上的负载均衡设备上实现，并执行轮询设置，这样可实现对各服务器的负载均衡操作。
由说明可知服务器的 IP 地址为：192.168.20.5/27，因此可知子网掩码为：255.255.255.224.
启用网络服务的命令： systemctl enable network
Web 应用防护系统，简称：WAF，Web 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。能够有效发现及阻止 SQL 注入、网页篡改、跨站脚本等攻击。主要对服务器区域进行检测和保护。
存储网络，采用光纤连接存储区域，实现高速存储访问，符合 FCSAN 的特点。并且 FCSAN 支持块级调用，适合对大型数据库提供存储服务。
第 3 题：（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】
某公司有两个办事处，分别利用装有 Windows Server 2008 的双宿主机实现路由功能，此功能由 Wmdows Server 2008 中的路由和远程访问服务来完成。管理员分别为这两台主机其中一个网卡配置了不同的 IP 地址，如图 3-1 所示。

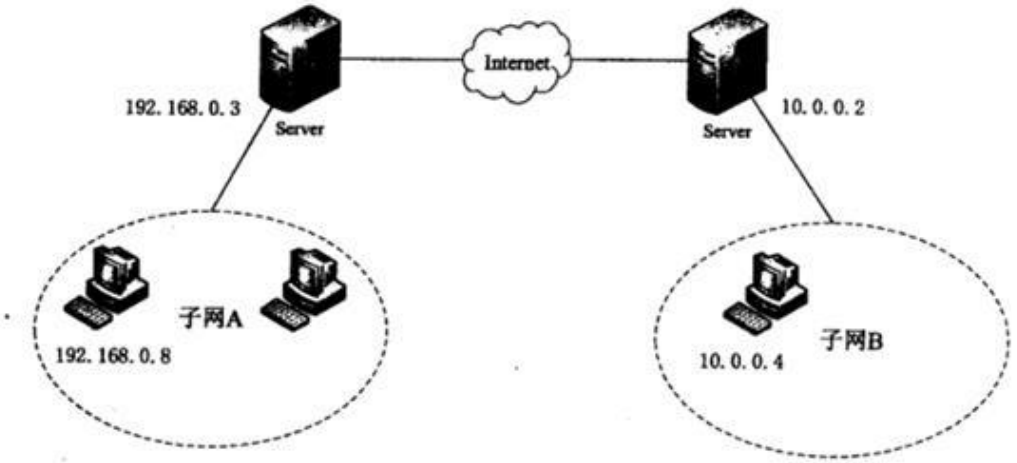

图 3-1

题：3.1 （4 分）

在“管理您的服务器”中点击“添加或删除角色”，此时应当在服务器角色中选择（1）来完成路由和远程访问服务的安装。在下列关于路由和远程访问服务的选项中，不正确的是（2）。

（1）备选答案：A. 文件服务器 B. 应用程序服务器（IIS，ASP.NET）C. 终端服务器 D. 远程访问/VPN 服务

（2）备选答案：

A. 可连接局域网的不同网段或子网，实现软件路由器的功能

B. 把分支机构与企业网络通过 Intranet 连接起来，实现资源共享

C. 可使远程计算机接入到企业网络中访问网络资源

D. 必须通过 VPN 才能使远程计算机访问企业网络中的网络资源题：3.2 （4 分）

两个办事处子网的计算机安装 Win7 操作系统，要实现两个子网间的通信，子网 A 和子网 B 中计算机的网关分别为（3）和（4）。子网 A 中的计算机用 ping 命令来验证数据包能否路由到子网 B 中，图 3-2 中参数使用默认值，从参数（5）可以看出数据包经过了（6）个路由器。

```
C:\>ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

图 3-2

（3）备选答案：

A.192.168.0.0 B.192.168.0.1 C.192.168.0.3 D.无须配置网关

（4）备选答案：

A.10.0.0.0

B.10.0.0.1

C.10.0.0.2

D.无须配置网关

（5）备选答案：

A. bytes

B. time

C. TTL

D. Lost

题：3.3 （8分）

Windows Server 2008 支持 RIP 动态路由协议。在 RIP 接口属性页中，如果希望路由器每隔一段时间向自己的邻居广播路由表以进行路由信息的交换和更新，则需要在“操作模式”中选择（7）。在“传出数据包协议”中选择（8），使网络中其它运行不同版本的邻居路由器都可接受此路由器的路由表：在“传入数据包协议”中选择（9），使网络中其他运行不同版本的邻居路由器都可向此 广播路由表。

（7）备选答案：

A. 周期性是更新模式

B. 自动-静态更新模式

（8）备选答案：

A. RIPv1 广播

B. RIPv2 多播

C. RIPv2 广播

（9）备选答案：

A. 只是 RIPv1

B. 只是 RIPv2

C. RIPv1 和 v2

D. 忽略传入数据包

为了保护路由器之间的安全通信，可以为路由器配置身份验证。选中“激活身份验证”复选框，并在“密码”框中键入一个密码。所有路由器都要做此配置，所配置的密码（10）。

（10）备选答案：

A. 可以不同

B. 必须相同题

3.4 （4 分）

由于在子网 A 中出现病毒，需在路由接口上启动过滤功能，不允许子网 B 接收来自子网 A 的数据包，在选择入站筛选器且筛选条件是“接收所有除符合下列条件以外的数据包”时，如图 3-3 所示，由源网络 IP 地址和子网掩码得到的网

络地址是（11），由目标网络 IP 地址和子网掩码得到的网络地址是（12），需要选择协议（13）。如果选择协议（14），则会出现子网 A 和子网 B 之间 ping 不通但是子网 B 能接受来自子网 A 的数据包的情况。

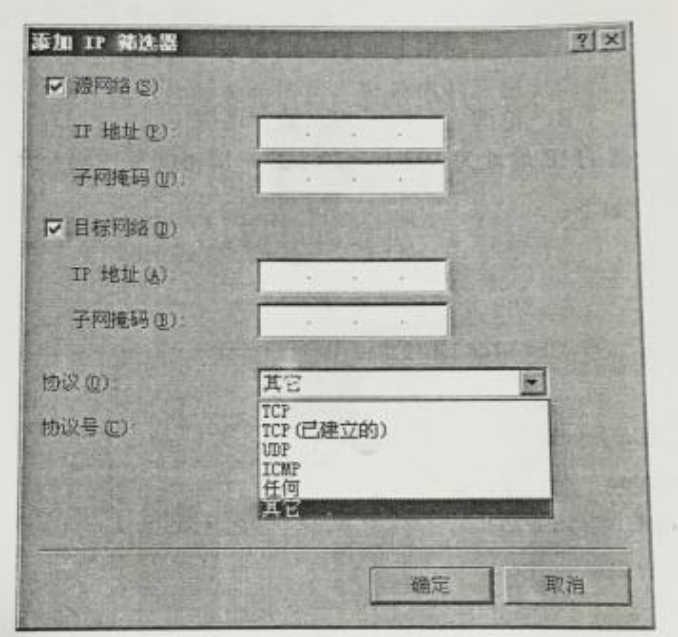

图 3-3

（11）备选答案：

A. 192.168.0.0

B. 192.168.0.1

C. 192.168.0.3

D. 192.168.0.8

（12）备选答案：

A. 10.0.0.0

B. 10.0.0.1

C. 10.0.0.3

D. 10.0.0.4

（13）~（14）备选答案：

A. ICMP

B. TCP

C. UDP

D. 任何

答案解析：

1、D

2、D

答案解析：

3、C

4、C

5、C

6、128

答案解析：

7、A

8、A

9、C

10、B

答案解析：

11-14 A A D A

通过文字及图形说明，可知子网 A 连接在 192.168.0.0 网段，而子网 B 处在 10.0.0.0 网段，对应的网关地址分别为网段连接的服务器 IP。Ping 命令通常用于测试连通性，利用的 ICMP 的回送请求或回答报文，其中 TTL 值代表跳数，以 255 跳开始，每经过一个路由器，就会减 1。

为支持 RIP 动态路由协议，可自己相应配置，RIP 有两个版本，V1 只支持有类路由信息，并以广播的方式发送整个路由表给邻居，V2 支持无类别路由，以组播的方式发送整个路由表信息进行路由收敛。

为了确保路由器之间的安全通信，可在路由器和路由器之间增加身份验证，并且相互连接的双方密码信息要一致。

第 4 题:（共 15 分）

阅读以下说明，回答问题 1 至问题 2，将解答填入答题纸对应的解答栏内。【说

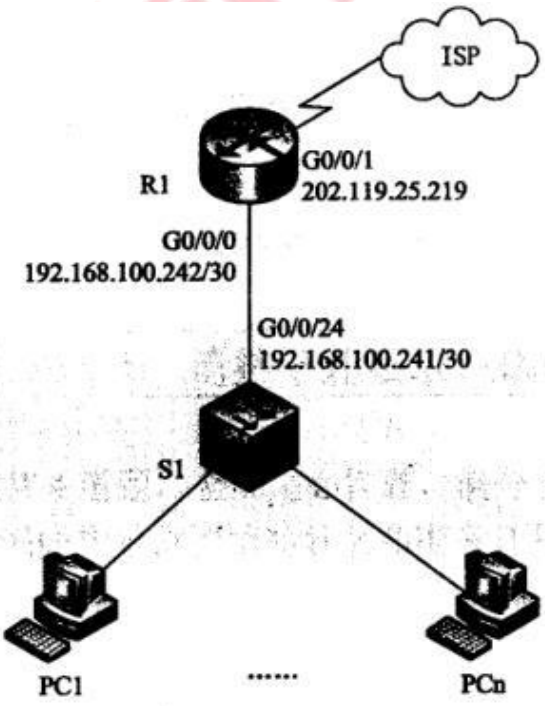

图 4-1

明】某公司网络拓扑图如图 4-1 所示。

为了便于管理公司网络，管理员根据不同部门对公司网络划分了 VLAN，VLAN 编号及 IP 地址规划如表 4-1 所示，考虑到公司以后的发展，每个部门的 IP 地址规划均留出了一定的余量，请根据需求，将下表补充完整。

表 4-1

部门	VLAN 编号	主机数量	IP 地址范围	子网掩码
行政部门	VLAN 100	32	192.168.100.129-（1）	（2）
营销部门	VLAN 105	68	192.168.100.1-192.168.100.126	255.255.255.128
财务部门	VLAN 110	8	192.168.100.193-192.168.100.222	（3）
后勤部门	VLAN 115	8	（4）-192.168.100.238	255.255.255.240

公司计划使用 24 接口的二层交换机作为接入层交换机，根据以上主机数量在不考虑地理位置的情况下，最少需要购置（5）台接入层交换机。

题：4.2 （10 分）

公司申请了 14 个公网 IP 地址，地址范围为 202.119.25.209-202.119.25.222，其中，202.119.25.218-202.119.25.222 作为服务器和接口地址保留，其他公网 IP 地址用于公司访问

Internet。公司使用 PAT 为营销部门提供互联网访问服务。请根据描述，将下面配置代码补充完整。 system-view

[Huawei] (6) R1

[R1]user-interface （7） // 进 入 console 用 户 界 面 视 图

[R1-ui-console0]authentication-mode (8)

Please configure the login password (maximum length 16):huawei

[R1-ui-console0]quit

[R1]int GigabitEthernet，0/0/0

[R1-GigabitEthernet0/0/0]ip address 192.168.100.242 255.255.255.252

[R1-GigabitEthernet0/0/0] (9)

[R1] (10) 2000

[R1-acl-2000] (11) 5 permit source 192.168.100.0 (12)

[R1-acl-basic-2000]quit

[R1]nat address-group 1 (13) 202.119.25.217 [R1]interrface GigabitEthemet 0/0/1

[R1-GigabitEthemet 0/0/1]ip address (14) 255.255.255.240

[R1-GigabitEthemet 0/0/1] (15) outbound 2000 address-group 1

[R1]rip

[R1-rip-1]version 2

[R1-rip-1]network 192.168.100.0

交换机配置略……

答案解析：

1、192.168.100.190

2、255.255.255.192

3、255.255.255.240

4、192.168.100.225

5、7

答案解析：

6、sysname // 配置设备名

7、console 0

8、password //配置 console 口密码

9、quit //退出接口视图

10、acl //定义 ACL

11、rule //配置 ACL 规则

12、0.0.0.127//指定可进行地址转换的内网网段

13、202.119.25.209 // 定义全局公有地址池范围

14、202.119.25.219 //配置 R1 的接口 IP 地址

15、NAT //华为路由器执行 NAT 时，缺省为 PAT 方式 。如果不采用 NAT，则在语句最后加上 no-pat。

IP 地址及子网掩码的确定，华为设备的基本配置。由图形说明可知行政部需要 32 个有效主机地址，因此分配主机位位数 6 位，网络位位数为 26 位。对应子网掩码为：255.255.255.192，

对应的网段为:192.168.100.128,最后一个有效 IP 地址为:192.168.100.190。同理可求得其它几个部门的 IP 及子网掩码。