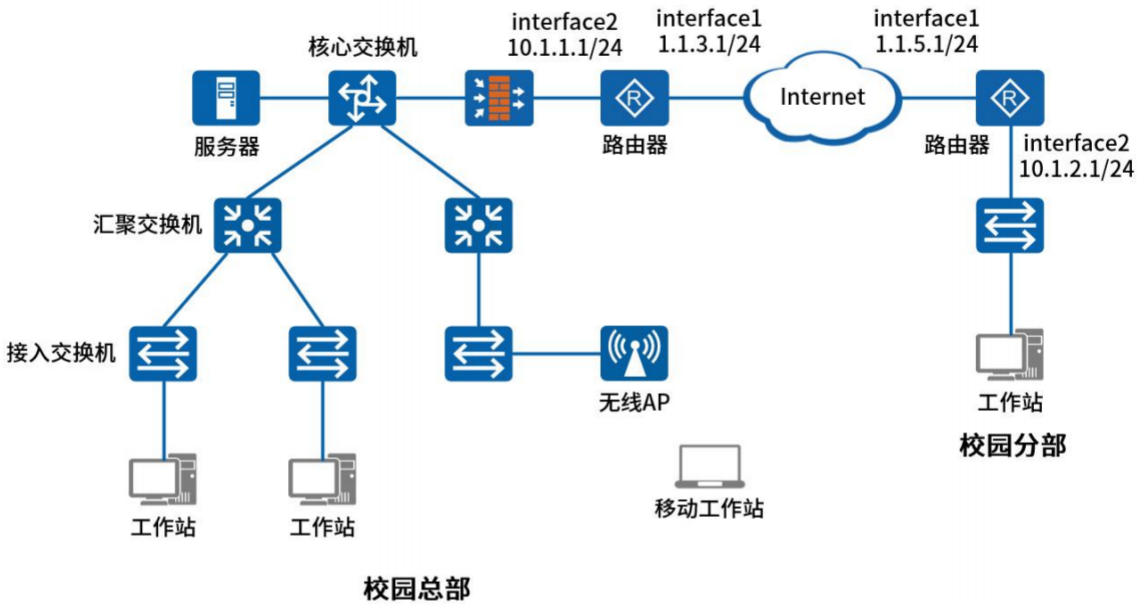
2024 上半年网络工程师第一期模考试卷（案例分析）

1、

某学校欲构建校园网，根据实际情况，计划在校园总部采用有线网络和无线网络相结合的接入方式，校园分部通过 Internet 采用 VPN 技术与校园总部互联，该校园网的网络拓扑结构如图所示。



问题内容：

问题 1（6 分）
IPSec 是 IETF（Internet Engineering Task Force）制定的一组开放的网络安全协议。它并不是一个单独的协议，而是一系列为 IP 网络提供安全性的协议和服务的集合，包括认证头 AH（Authentication Header）和封装安全载荷 ESP（Encapsulating Security Payload）两个安全协议、密钥交换和用于验证及加密的一些算法等。
请补充完成下面表空缺处。

安全特性	AH	ESP
协议号	51	（1）
数据完整性校验	支持（验证整个IP报文）	支持（传输模式：不验证IP头，隧道模式：验证整个IP报文）
数据源验证	（2）	支持
数据加密	（3）	（4）
防报文重放攻击	（5）	支持
IPSec NAT-T（NAT穿越）	（6）	支持

问题 2（5 分）
封装模式是指将 AH 或 ESP 相关的字段插入到原始 IP 报文中，以实现对报文的认证和加密，封装模式有（1）模式和（2）模式两种。（3）两种模式的区别是什么？
问题 3（3 分）
IKEv1 协商阶段 1 支持两种协商模式：（1）和（2），其中（3）模式减少了交换信息的数目，提高了协商的速度，但是没有对身份信息进行加密保护。
问题 4（6 分）
R-A 为校园分部网关，R-B 为校园总部网关，分部与总部通过公网建立通信，含组播通信。现需求对分公司与总部之间相互访问的流量进行安全机密保护，且支持隧道中间存在 NAT 设备的 NAT 穿越场景。故本例采用（1）技术解决。采用 ACL 方式建立隧道时，配置基于 ACL 的 IPsec 策略，以设备 A 为例，请完善配置命令。
[DeviceA] acl 3000
[DeviceA-acl4-advance-3000] rule 5 permit ip source （2） destination （3）
[DeviceA-acl4-advance-3000] quit

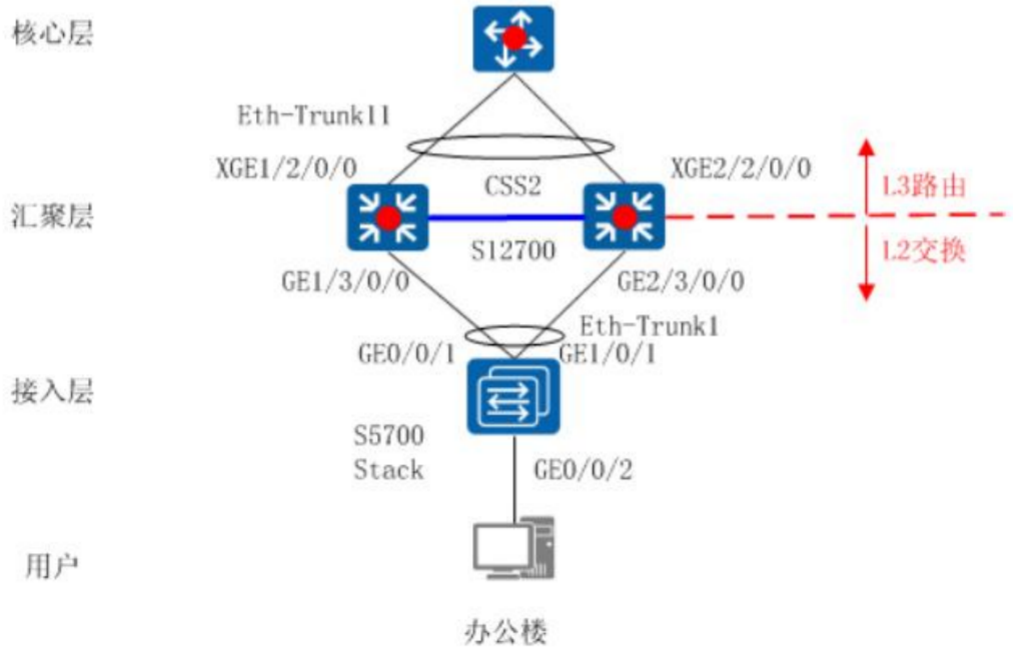
试题答案：

问题 1（6 分）
（1）50
（2）支持
（3）不支持
（4）支持
（5）支持
（6）不支持
问题 2（5 分）
（1）传输
（2）隧道
（3）传输模式和隧道模式的区别在于：

从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行验证和加密。隧道模式下可以隐藏内部 IP 地址，协议类型和端口。
从性能来讲，隧道模式因为有一个额外的 IP 头，所以它将比传输模式占用更多带宽。
从场景来讲，传输模式主要应用于两台主机或一台主机和一台 VPN 网关之间通信；隧道模式主要应用于两台 VPN 网关之间或一台主机与一台 VPN 网关之间的通信。
当安全协议同时采用 AH 和 ESP 时，AH 和 ESP 协议必须采用相同的封装模式。
问题 3（3 分）
（1）主模式
（2）野蛮模式
（3）野蛮
问题 4（6 分）
（1）GER over IPSec
（2）1.1.3.1 0
（3）1.1.5.1 0

3、

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】
本企业网络方案使用接入层汇聚双堆叠双归上行组网方式。如图：



问题内容：

问题 1（6 分）
1、本例中，采用接入层汇聚层双堆叠双归上行组网方案，可以满足用户的业务

需求：
用户接入：接入层部署业务口堆叠，简化配置和管理，每组堆叠都以链路聚合双上行至汇聚层交换机，提高链路级可靠性。
2、汇聚层部署交换网硬件集群，与接入层构成树形组网，简化配置和管理，上下行均采
用链路聚合，链路聚合的作用是：（1）、（2）。
3、接入交换机连接终端的端口部署为（3）端口，加快网络收敛并防止端口状态改变引起网络震荡。汇聚交换机部署 ARP 安全，防止泛洪攻击和欺骗攻击，部署（4），可以防止 DHCP 仿冒攻击，上行端口部署 OSPF 验证以提高 OSPF 网络安全性，配置根保护，防止高优先级 BPDU 引起抢根。
问题 2（14 分）
部分配置如下，请补充完整命令或解释命令。
配置汇聚与核心设备路由互通。
配置各接口的 IP 地址。核心设备的配置此处不再赘述。
[S12700] interface Vlanif（5）
[S12700-Vlanif100] ip address 100.0.0.10 255.255.255.0
[S12700-Vlanif100] quit
[S12700] interface Vlanif（6）
[S12700-Vlanif200] ip address 200.0.0.10 255.255.255.0
[S12700-Vlanif200]quit
配置 S12700 与核心设备采用 OSPF 协议互通。
[S12700]（7）
[S12700-ospf-1]（8）
[S12700-ospf-1-area-0.0.0.0] network 100.0.0.0 0.0.0.255
[S12700-ospf-1-area-0.0.0.0] network 200.0.0.0 0.0.0.255
[S12700-ospf-1-area-0.0.0.0] （9）
[S12700-ospf-1]quit
[S12700] interface Vlanif 200
[S12700-Vlanif200] ospf authentication-mode md5 1 cipher HUAWEI123 //（10）
[S12700-Vlanif200]quit
在汇聚交换机上配置相应的安全措施
在 S12700 上使能 DHCP，相应接口上配置 DHCP 监听业务。
[S12700]（11）//在 S12700 上使能 DHCP
[S12700] dhcp snooping enable
[S12700] interface Eth-Trunk 1
[S12700-Eth-Trunk1]

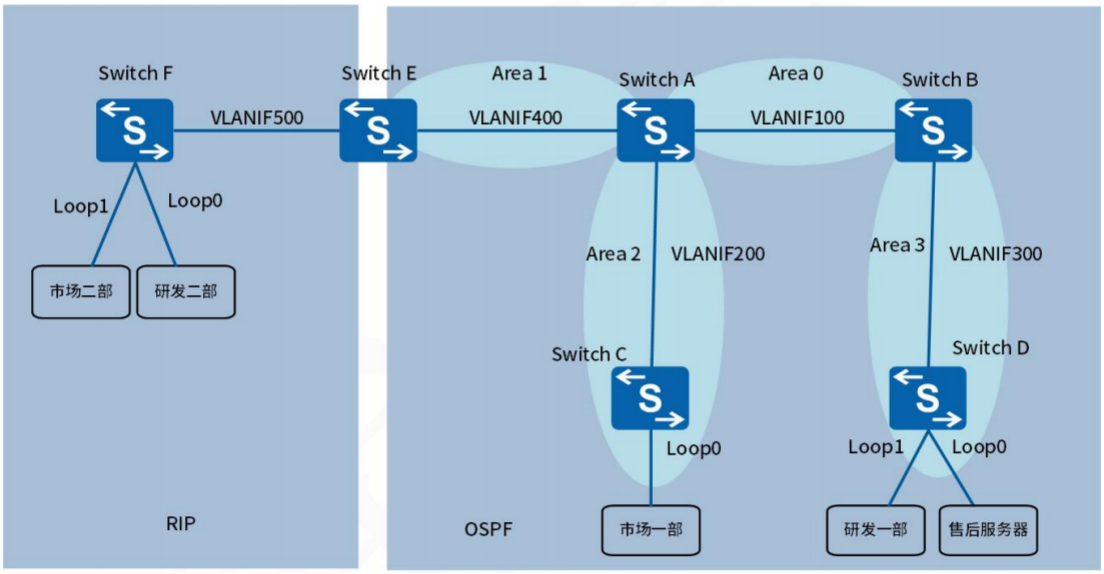
试题答案：

问题一（6 分）：
（1）提高带宽
（2）链路可靠性
（3）边缘
（4）DHCP Snooping

问题 2（14 分）：
（5）100
（6）200
（7）ospf 1
（8）area 0
（9）quit
（10）配置 S12700 与核心设备接口的验证方式为 MD5
（11）dhcp enable

4、

如图所示，公司甲使用 OSPF 路由协议实现公司设备全网互通，公司乙使用 RIP 路由协议实现全网互通，后来公司甲和公司乙有合作，要求将两个公司之间的各个部门可以实现互通。Switch A 和 Switch B 作为公司核心设备负责各个部门间的通信。
由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：
使得公司乙的研发二部所在网段无法被引入到公司甲。
使得公司甲的市场一部不能访问研发一部。
使得研发一部和售后服务部不能访问市场二部。



设备各接口配置情况下下表：

设备	接口	IP地址	设备	接口	IP地址
SwitchA	VLANIF100	10.1.1.1/24	SwitchB	VLANIF100	10.1.1.2/24
	VLANIF200	10.2.1.1/24		VLANIF300	10.3.1.1/24
	VLANIF400	10.4.1.1/24			
SwitchC	VLANIF200	10.2.1.2/24	SwitchD	VLANIF300	10.3.1.2/24
	Loop0	192.168.3.1/24（市场一部）		Loop0	192.168.1.1/24（售后服务部）
				Loop1	192.168.2.1/24（研发一部）
SwitchE	VLANIF400	10.4.1.2/24	SwitchF	VLANIF500	10.5.1.2/24
	VLANIF500	10.5.1.1/24		Loop0	192.168.4.1/24（研发二部）
				Loop1	192.168.5.1/24（市场二部）

问题内容：

【问题 1】12 分
各设备的接口 IP 配置省略…
以 SwitchE 为例，配置其 OSPF 和 RIP
在 Switch E 上使能指定网段的 OSPF 路由功能。
<SwitchE> （ 1 ）
[SwitchE] ospf
[SwitchE-ospf-1] area 1
[SwitchE-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255

在 Switch E 上使能指定网段的 RIP 功能。
[SwitchE] rip
[SwitchE-rip-1] （ 2 ） //配置 RIP 的版本
[SwitchE-rip-1] undo summary
[SwitchE-rip-1] network 10.0.0.0
[SwitchE-rip-1] quit

请完成配置命令，实现在 Switch E 上将直连路由和 OSPF 路由引入到 RIP 网络中，同时将将直连路由和 RIP 路由引入到 OSPF 网络中。
（ 3 ）（4 分）

SwitchC 上的配置命令片段
[SwitchC] acl basic 2000
[SwitchC-acl-ipv4-basic-2000] rule 0 deny source （ 4 ）
[SwitchC-acl-ipv4-basic-2000] rule permit source （ 5 ）
[SwitchC-acl-ipv4-basic-2000] quit
[SwitchC] ospf
[SwitchC-ospf-1] filter-policy 2000 （ 6 ）
[SwitchC-ospf-1] quit
在 Switch D 上的配置片段

//（ 请说明交换机 D 上的配置的作用 7 空 ）（2 分）
<SwitchD> system-view
[SwitchD] acl basic 2000
[SwitchD-acl-ipv4-basic-2000] rule 0 deny source 192.168.5.0 0.0.0.255
[SwitchD-acl-ipv4-basic-2000] rule permit source any
[SwitchD-acl-ipv4-basic-2000] quit
[SwitchD] ospf
[SwitchD-ospf-1] filter-policy 2000 import
[SwitchD-ospf-1] quit
在 Switch E 上的配置片段
创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.4.0/24。
[SwitchE] acl basic 2000
[SwitchE-acl-ipv4-basic-2000] rule 0 deny source 192.168.4.0 0.0.0.255
[SwitchE-acl-ipv4-basic-2000] rule permit source any
[SwitchE-acl-ipv4-basic-2000] quit
[SwitchE] ospf
[SwitchE-ospf-1] filter-policy 2000 （ 8 ） rip 1
[SwitchE-ospf-1] quit

【问题 2】3 分
在 SwitchE 上的这一条命令是否可以不配置，[SwitchE-acl-ipv4-basic-2000] rule permit source any，请简要说明原因？
（ 9 ）

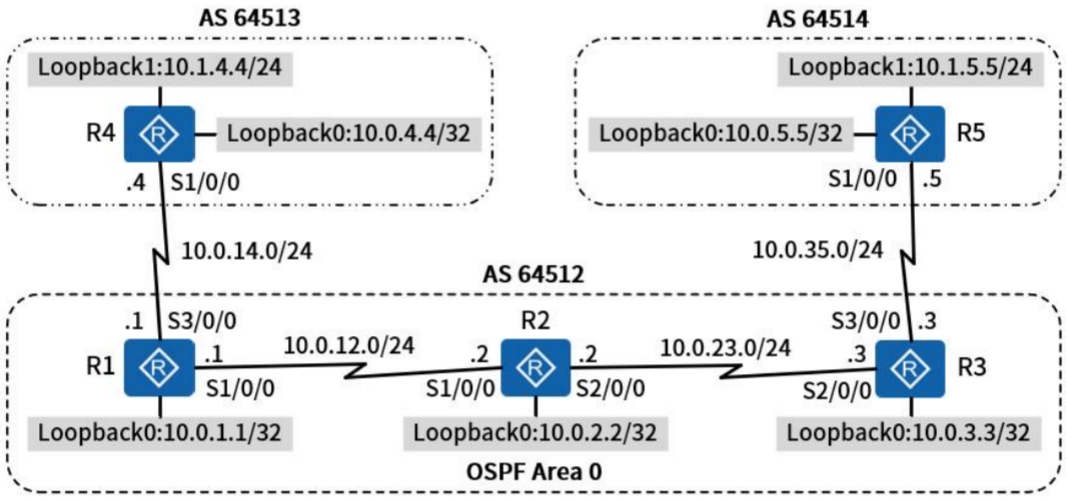
试题答案：

【问题 1】12 分
1、system-view
2、version 2
3、（4 分）
[SwitchE] rip
[SwitchE-rip-1] import-route direct
[SwitchE-rip-1] import-route ospf
[SwitchE-rip-1] quit
[SwitchE] ospf
[SwitchE-ospf-1] import-route direct
[SwitchE-ospf-1] import-route rip
[SwitchE-ospf-1] quit
4、192.168.2.0 0.0.0.255
5、any
6、import
7、上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.5.0/24，并通过指定访问控制列表 ACL 2000 来对要加入到路由表的路由信息进行过滤。（或者简单描述，在 SwitchD 上过滤掉市场二部的路由信息）（2 分）
8、export

【问题 2】3 分
9、答：不行，因为路由信息过滤功能配合 ACL 使用时，ACL 默认隐含的语句是拒绝所有，如果不配置这一条命令，那么将会把所有网段路由全部过滤掉，两公司之间将不能相互通信，则没有达到题目的说明要求。

4、

你是公司的网络管理员。公司的网络采用了 BGP 协议作为路由协议。公司的网络由多个自治系统组成，不同的分支机构使用了不同的 AS 号，现在你需要完成公司网络的搭建工作。在公司总部使用了 OSPF 作为 IGP，公司内部不同分支机构使用的是私有的 BGP AS 号。在完成网络搭建以后，你还需要观察 BGP 路由信息的传递。
给所有路由器配置 IP 地址和掩码，其中 R4 和 R5 的 loopback 1 接口掩码为 24 位，模拟用户网络。
给所有路由器配置 IP 地址和掩码，其中 R4 和 R5 的 loopback 1 接口掩码为 24 位，模拟用户网络。



问题内容：

问题 1（基础配置与 IP 编址）（2 分）

```
<R1>system-view
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24
[R1-Serial1/0/0]quit
[R1]interface Serial 3/0/0
[R1-Serial3/0/0]ip address 10.0.14.1 24
[R1-Serial3/0/0]quit
```

[R1]interface LoopBack 0
[R1-LoopBack0]ip address （1） （2）
[R1-LoopBack0]quit
完成此配置后，R2、R3、R4、R5 配置类似。
问题 2（4 分）
在 AS 64512 中使用 OSPF 作为 IGP，将 Loopback 0 连接的网段发布进 OSPF。R1 的 S1/0/0 连接的网段运行 OSPF。
[R1]router id 10.0.1.1
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 （3）
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-1]quit
R2、R3 的 OSPF 配置类似。
如果修改了 Router ID，需执行（4）命令使新的 Router ID 生效。
由于设备上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级值。在不同协议发现同一条路由时，优先级值（5）的路由将被优选。
缺省情况下，OSPF 路由的优先级值为（6）。
问题 3（7 分）
建立 IBGP 对等体
在 R1、R2、R3 上配置 IBGP 全互联。使用 Loopback0 地址作为更新源。
[R1]（1）
[R1-bgp]peer （2） as-number 64512 //配置和 R2 路由器 IBGP
[R1-bgp]peer 10.0.2.2 connect-interface （3）
R1 和 R3 配置 IBGP 全互联命令类似。
在 R1 上在 BGP 进程下使用 timer 修改 BGP 的 keep alive 时间为 30 秒，hold 时间为 90 秒。
[R1-bgp] bgp 64512
[R1-bgp] timer keepalive （4） hold （5）
在 R2 上默认的配置参数 Active Hold Time 为（6）s，Keepalive Time 为（7）s。
问题 4（7 分）
配置 EBGP 对等体
在 R4 上配置 BGP，本地 AS 号为 64513，与 R1 建立 EBGP 对等体关系。在建立对等体关系时，指定更新源为 Loopback 0 接口的地址，并指定 ebgp-max-hop 为 2。添加到对端 Loopback 0 接口地址的 32 位的静态路由，使之能正常建立对等体关系。
（1）为什么在这里需要 ebgp-max-hop 指定为 2？（3 分）
（2）请说明 BGP 路由协议的防环机制？（4 分）

试题答案：

问题 1（2 分）
（1）10.0.1.1
（2）32
问题 2（4 分）
（1）0.0.0.0
（2）reset ospf 1 process
（3）低
（4）10
问题 3（7 分）
（1）bgp 64512
（2）10.2.2.2
（3）LoopBack 0
（4）30
（5）90
（6）180
（7）60
问题 4（7 分）
（1）（3 分）
通常情况下，EBGP 对等体之间必须具有直连的物理链路，如果不满足这一要求，则必须使用 peer ebgp-max-hop 命令允许它们之间经过多跳建立 TCP 连接。BGP 使用 Loopback 口建立 EBGP 邻居时，必须配置命令 peer ebgp-max-hop（其中 hop-count≥2），否则邻居无法建立。peer ebgp-max-hop 命令用来配置允许 BGP 同非直连网络上的对等体建立 EBGP 连接，并同时可以指定允许的最大跳数。
（2）（4 分）
BGP 从设计上避免了环路的发生。
AS 之间：BGP 通过携带 AS 路径信息来标记途经的 AS，带有本地 AS 号的路由将被丢弃，从而避免了域间产生环路。
AS 内部：BGP 在 AS 内学到的路由不再通告给 AS 内的 BGP 邻居，避免了 AS 内产生环路。