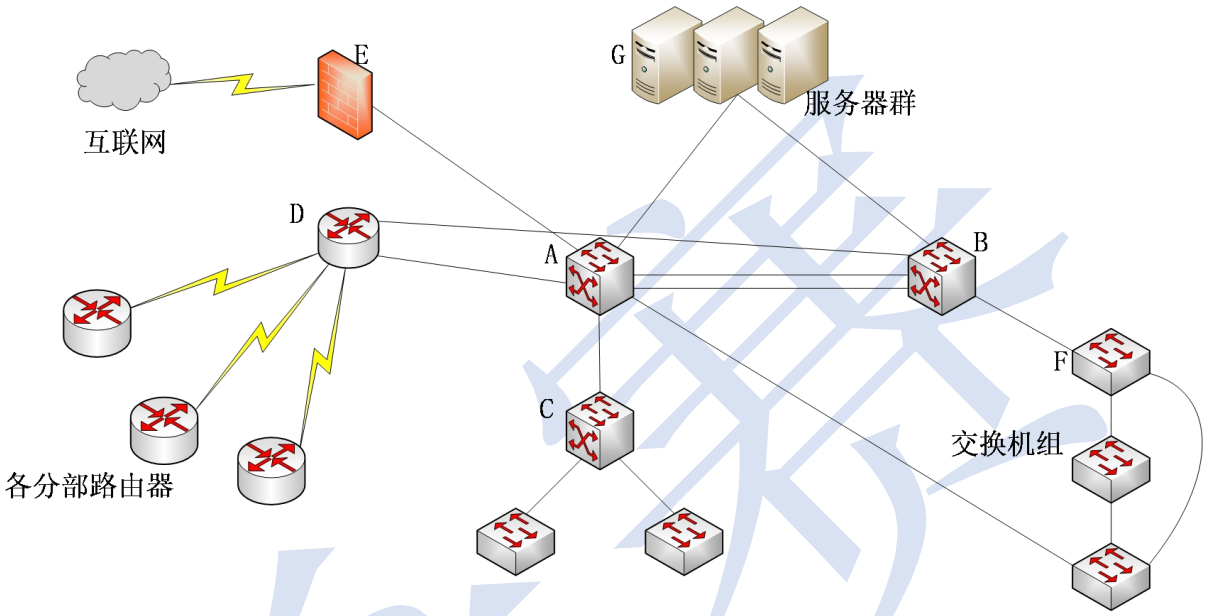
2021 年上半年网络工程师考试公开模拟试卷 1（案例题）

1、

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】
某企业网络拓扑如图 1-1 所示。



问题内容：

【问题 1】（4 分）
根据图 1-1，对该网络主要设备清单表 1-1 所示内容补充完整。

表 1-1

在网络中的编号	产品描述
A，B	核心主、备交换机
（1）	汇聚交换机
交换机组 F	（2）
（3）	路由器
E	（4）

【问题 2】（10 分）
1．网络中 A.B 设备连接的方式是什么？请说明这种链接方式具备的三点优势。（8 分）
2．交换机组 F 的连接方式是什么？采用这种连接方式的好处是什么？（2 分）
【问题 3】（6 分）

若考虑到成本问题，对总部和分部的连接用 VPN 的方式，在分部路由器上做下列配置，请解释相关命令

[RA]ipsec proposal tran1
[RA-ipsec-proposal-tran1] Encapsulation-mode tunnel //（5）
[RA-ipsec-proposal-tran1] Transform esp（6）
[RA-ipsec-proposal-tran1] esp encryption-algorithm 3des（7）
[RA-ipsec-proposal-tran1] esp authentication-algorithm sha1（8）
[RA-ipsec-proposal-tran1]quit
该命令片段配置的是 （9）.

（9）备选答案：

A、在接口应用安全策略
B、Ipsce 安全提议
C、定义需要保护的数据流
D、路由映射

试题答案：

【问题 1】（4 分）
（1）C
（2）接入交换机
（3）D
（4）防火墙
【问题 2】（10 分）
1，根据图中标识可以看出是采用链路聚合，也叫链路捆绑。在两台设备间采用链路聚合后，在不考虑协议开销的前题下，其带宽是原来单链路带宽的 2 倍。
2，图中 F 组交换机先是串接在一起，最后上、下两个设备通过一条链路级联起来，该连接方式即是菊花式堆叠，该堆叠不但方便了对设备的管理，提供链路冗余，还提升了网络的可靠性，为保障该菊花式堆叠与上行设备的可靠性，该堆叠采用了双上行接入方式。
【问题 3】（6 分）
（5）IPSEC VPN 工作模式为隧道模式
（6）安全提议中选择的安全协议为 ESP
（7）安全提议中选的加密算法 3DES
（8）安全提议选的验证算法 SHA1
（9） B

试题解析：

【问题 1】（4 分）
根据图中的拓扑及网络分层的设计思想，就能解答出该题，题意中已给出 A、B 设备是核心层设备，连接核心设备的 C 下面再连接了两台交换机，因此可以推断出该设备是汇聚层交换机。交换机组 F 为接入层交换机，D 是与分部路由器相连的设备，根据题意和设备型号可以推断出

是路由器。E 根据拓扑图及图标标识就可以推断出是防火墙。

（1）C

（2）接入交换机

（3）D

（4）防火墙

【问题 2】（10 分）

1，根据图中标识可以看出是采用链路聚合，也叫链路捆绑。在两台设备间采用链路聚合后，在不考虑协议开销的前题下，其带宽是原来单链路带宽的 2 倍。

2，图中 F 组交换机先是串接在一起，最后上、下两个设备通过一条链路级联起来，该连接方式即是菊花式堆叠，该堆叠不但方便了对设备的管理，提供链路冗余，还提升了网络的可靠性，为保障该菊花式堆叠与上行设备的可靠性，该堆叠采用了双上行接入方式。

【问题 3】（6 分）

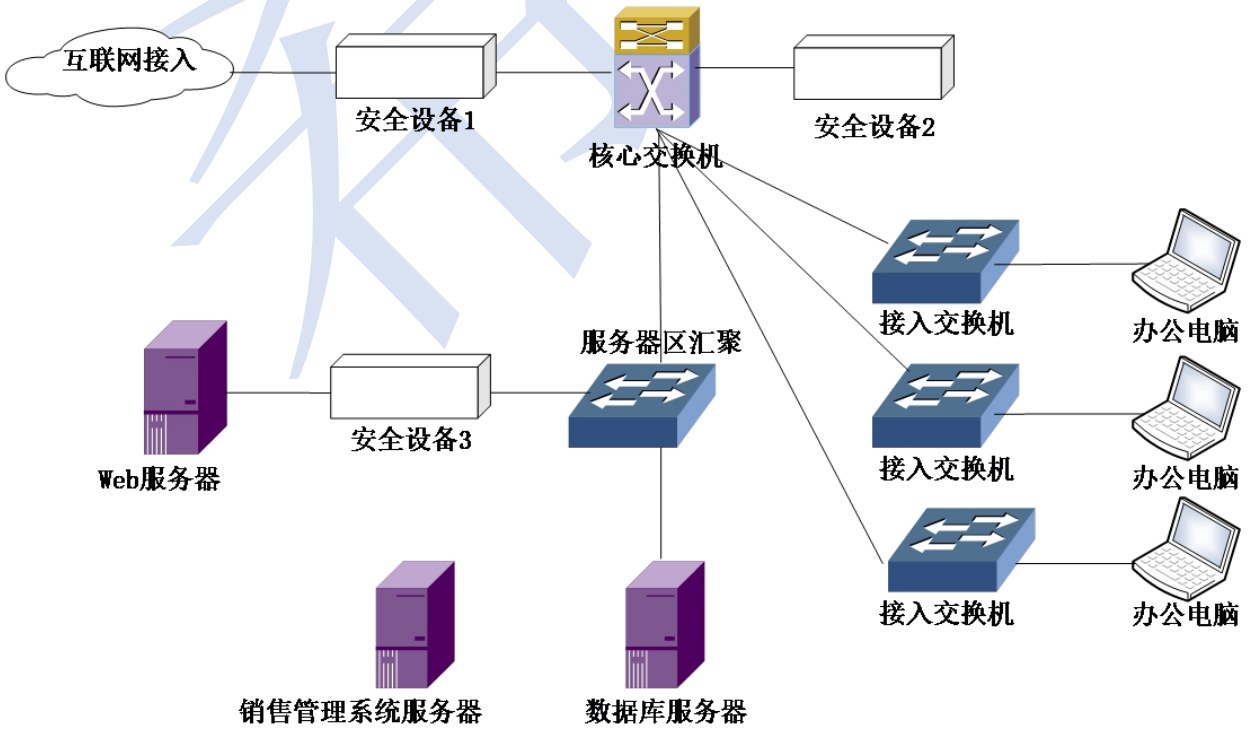
该段命令是配置安全提议：安全提议保存 IPSEC 提供安全服务时准备使用的一组特定参数：包括安全协议、加密、验证算法、工作模式等等，以便 IPSEC 通信双方协商各种安全参数。IPSEC 安全网关必须具有相同的安全提议才可以就安全参数协商一致。

2、

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。

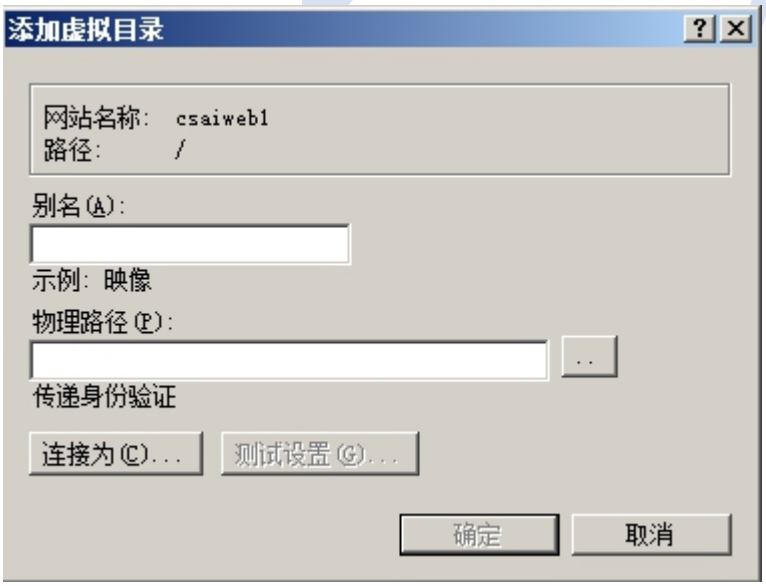
【说明】

图 3-1 是某互联网服务企业网络拓扑，该企业主要对外提供网站消息发布、在线销售管理服务，Web 网站和在线销售管理服务系统采用 JavaEE 开发，中间件使用 Weblogic，采用访问控制、NAT 地址转换、异常流量检测、非法访问阻断等网络安全措施。



问题内容：

【问题 1】（6 分）
根据网络安全防范需求，需在不同位置部署不同的安全设备，进行不同的安全防范，为上图中的安全设备选择相应的网络安全设备。
在安全设备 1 处部署（1）；在安全设备 2 处部署（2）；在安全设备 3 处部署（3）。
（1）～（3）备选答案：A．防火墙 B．入侵检测系统（IDS） C．入侵防御系统（IPS）
【问题 2】（5 分）
结合上述拓扑，请简要说明入侵防御系统（IPS）的不足和缺点。
【问题 3】（4 分）
WEB 服务器所使用的软件主要是 Windows server 平台的 IIS 组件和 Linux 平台上的（4）组件。Windows Server 2008 R2 的 IIS 版本为 IIS 7.5,并且默认（5）安装 IIS 服务 。
（5）选项：A：没有 B：已经
【问题 4】（5 分）
在 IIS7.5 中集成了一些常见错误代码的提示页。其中
（6）错误：服务器找不到请求的网页。
（7）错误 ：服务器不支持请求中所用的 HTTP 协议版本。
虚拟目录：实现将一个网站的文件分散存储在同一计算机的不同路径和其他计算机中。如图所示，目前已经为 www.educity.cn 网站添加了如下的虚拟目录，并指定端口为 8080，请写出访问改虚拟目录的 URL：（8）。
请写出实现虚拟主机 3 种方式（9）、（10）、（11）。



试题答案：

问题 1：（共 6 分）
（1）A
（2）B
（3）C

问题 2：（共 5 分）
访问 WEB 服务器的流量都要经过 IPS，IPS 是入侵防御系统，IPS 会对数据包做重组，会对数据的传输层，网络层，应用层中各字段做分析并与签名库做比对，如果没有问题，才转发出去。IPS 规划在这个位置会加大网络的延迟。同时，网络中部署一个 IPS 会存在有单点故障。
问题 3：（共 5 分）
（4）Apache
（5）A
（6）404
（7）505
（8）www.educity.cn:8080/csaiweb1

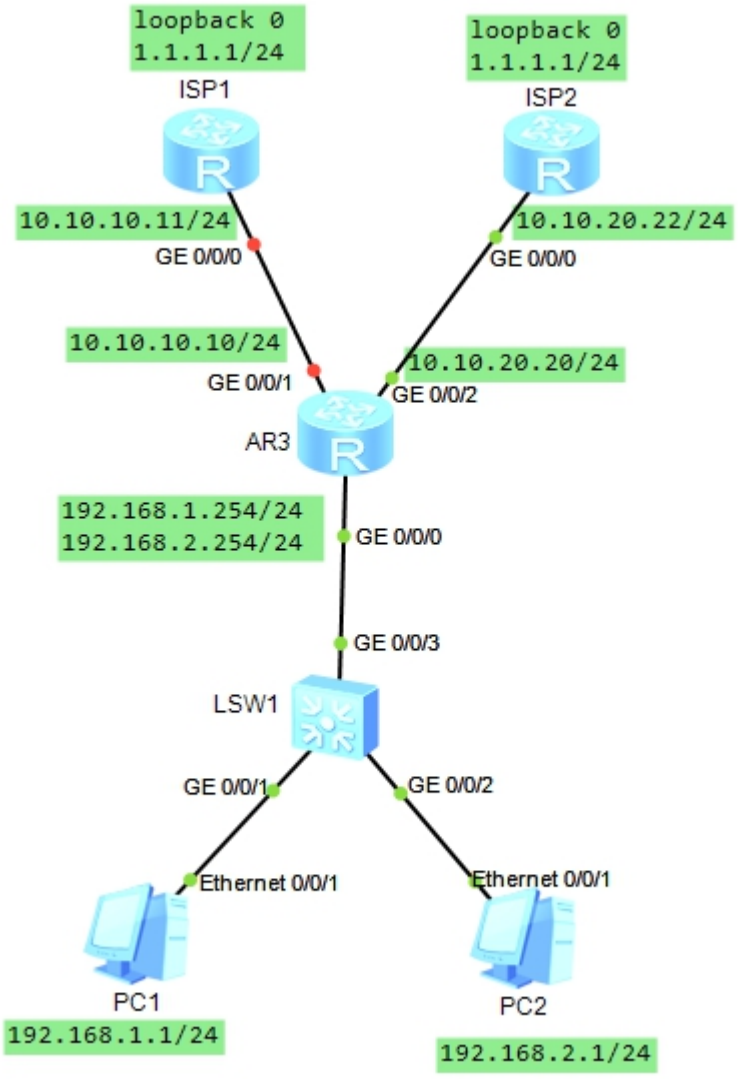
（9）使用不同的 IP 地址
（10）使用相同的 IP 地址、不同的 TCP 端口
（11）使用相同的 IP 地址和 TCP 端口、不同的主机头

试题解析：

问题 1 ：A、B、C
内网用户去往外网需要部署 NAT，安全设备 1 部署防火墙。看图安全设备 2 旁挂，部署 IDS 对网络流量进行检测不影响网络。在安全设备 3 处部署 IPS 可以对服务器进行防护。
问题 2：
访问 WEB 服务器的流量都要经过 IPS，IPS 是入侵防御系统，IPS 会对数据包做重组，会对数据的传输层，网络层，应用层中各字段做分析并与签名库做比对，如果没有问题，才转发出去。IPS 规划在这个位置会加大网络的延迟。同时，网络中部署一个 IPS 会存在有单点故障，还会存在误报。
问题 3：
WEB 服务器所使用的软件主要是 Windows server 平台的 IIS 组件和 Linux 平台上的 Apache 组件。Windows Server 2008 R2 的 IIS 版本为 IIS 7.5,并且默认没有安装 IIS 服务 。
【问题 4】（5 分）
在 IIS7.5 中集成了一些常见错误代码的提示页。其中
404 错误：服务器找不到请求的网页。
505 错误 ：服务器不支持请求中所用的 HTTP 协议版本。
虚拟目录：实现将一个网站的文件分散存储在同一计算机的不同路径和其他计算机中。如图所示，目前已经为 www.educity.cn 网站添加了如下的虚拟目录，并指定端口为 8080，请写出访问改虚拟目录的 URL： www.educity.cn:8080/csaiweb1 。
请写出实现虚拟主机 3 种方式使用不同的 IP 地址、使用相同的 IP 地址、不同的 TCP 端口、使用相同的 IP 地址和 TCP 端口、不同的主机头。

3、

某网络的结构如下图所示，阅读以下说明和参考需求，回复相关问题。



1、PC1 的数据从 ISP1 出,PC2 的数据从 ISP2 出。
2、两条线路互相冗余备份。
3、使用 NAT 地址转换。

问题内容：

问题一（5 分）：
在同一台路由器上如果配置了策略、静态、OSPF 动态三种路由。路由器接口首先对入站的数据包匹配（1）路由，如果没有匹配的话然后再匹配（2）路由，最后匹配（3）路由。策略路由分为基于（4）地址策略路由和基于（5）地址策略路由。
（1）、（2）、（3）的选型如下：
A、策略路由
B、静态路由
C、OSPF 动态路由
问题二，完成部分下列配置以及解释相关命令（10 分）：
路由器 AR3 的配置：

acl number 2000
rule 5 permit source 192.168.1.0 0.0.0.255
acl number 2001
rule 5 permit source 192.168.2.0 0.0.0.255
acl number 2002
rule 5 permit source 192.168.1.0 0.0.0.255//用于 NAT 转换
rule 10 permit source 192.168.2.0 0.0.0.255
#
traffic classifier c2000 operator or //基于流分类
if-match acl 2000
traffic classifier c2001 operator or
if-match acl 2001
#
traffic behavior b2001 //创建流行为
redirect ip-nexthop（1）
traffic behavior b2000
redirect ip-nexthop（2）
#
traffic policy PBR //创建流策略，关联数据流和流行为
classifier c2000 behavior b2000
classifier c2001 behavior b2001
#
interface GigabitEthernet0/0/0
ip address 192.168.1.254 255.255.255.0
ip address 192.168.2.254 255.255.255.0（3）
traffic-policy PBR （4）//调用策略路由。
#
interface （5）
ip address 10.10.10.10 255.255.255.0
nat outbound （6） //NAT 转换
#
interface （7）
ip address 10.10.20.20 255.255.255.0
nat outbound （8） //NAT 转换
#
ip route-static 0.0.0.0 0.0.0.0 10.10.10.11
ip route-static 0.0.0.0 0.0.0.0 （9） preference 70 //（10）

试题答案：

问题一（5 分）：
（1）A
（2）C
（3）B
（4）源

（5）目的
问题二（10 分）：
（1）10.10.20.22
（2）10.10.10.11
（3）sub
（4）inbound
（5）GigabitEthernet0/0/1
（6）2002
（7）GigabitEthernet0/0/2
（8）2002
（9）10.10.20.22
（10）配置浮动默认路由

试题解析：

问题一（5 分）：
在同一台路由器上如果配置了策略、静态、OSPF 动态三种路由。路由器接口首先对入站的数据包匹配策略路由，如果没有匹配的话然后再匹配 OSPF 路由，最后匹配静态路由。策略路由分为基于源地址策略路由和基于目的地址策略路由。
问题二（10 分）：
接口策略路由：只对转发的报文起作用，对本机下发的报文（比如本地的 ping 报文）不起作用。
实现原理:接口策略路由通过在流行为中配置重定向实现，只对接口入方向的报文生效。缺省情况下，设备按照路由表的下一跳进行报文转发，如果配置了接口策略路由，则设备按照接口策略路由指定的下一跳进行转发。
在按照接口策略路由指定的下一跳进行报文转发时，如果设备上没有该下一跳 IP 地址对应的 ARP 表项，设备会触发 ARP 学习，如果一直学习不到下一跳 IP 地址对应的 ARP 表项，则报文按照路由表指定的下一跳进行转发。如果设备上有或者学习到了此 ARP 表项，则按照接口策略路由指定的下一跳 IP 地址进行报文转发。
配置过程：
二、 配置接口 PBR 的步骤（华为）
配置思路：（思路步骤不是依据案例拓扑）
1、 抓取感兴趣的流量
使用 acl 抓取感兴趣的流量
[R1]acl 2001
[R1-acl-basic-2001]rule 10 permit source 192.168.20.0 0.0.0.255
2、 创建 流量分类
[R1]traffic classifier HAHA(流名称)
[R1-classifier-VLAN20] if-match acl 2001
3、 创建 流量分类处理行为
[R1]traffic behavior HEHE（行为名称）
[R1-behavior-VLAN20]redirect ip-nexthop 20.20.20.21
4、 创建 流量策略，将匹配的流量和处理行为结合。
[R1]traffic policy VLAN20 （策略名称）
[R1-trafficpolicy-vlan20]classifier HAHA behavior HEHE

流名称 行为名称
5、 调用流量策略
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]traffic-policy VLAN20 inbound

4、

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】
某单位网络内部部署有 IPv4 主机和 IPv6 主机，该单位计划采用 ISATAP 隧道技术实现两类主机的通信，其网络拓扑结构如图 5-1 所示，路由器 R1、R2、R3 通过串口经 IPv4 网络连接，路由器 R1 连接 IPv4 网络，路由器 R3 连接 IPv6 网段。通过 ISATAP 隧道将 IPv6 的数据包封装到 IPv4 的数据包中，实现 PC1 和 PC2 的数据传输。

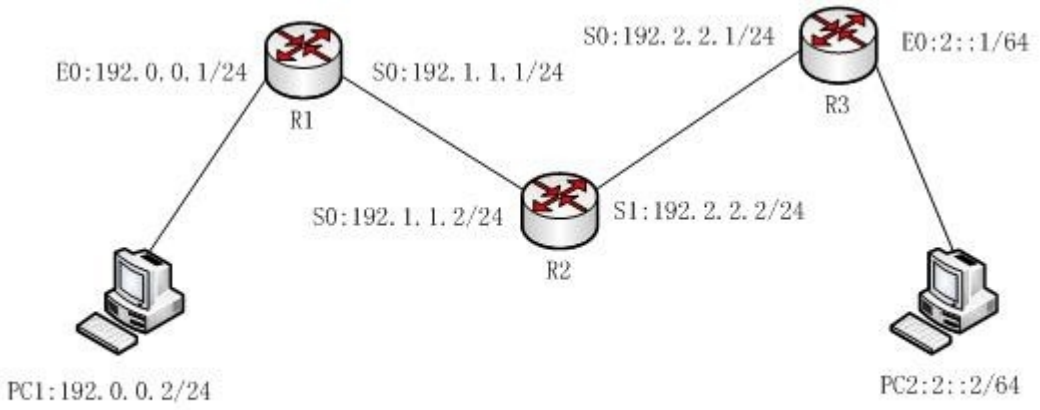


图 5-1 网络拓扑图

问题内容：

【问题 1】（4 分）
在 IPV6 的基本的过渡方案中除了隧道技术以外，还有（1）、（2）两种基本过渡技术。
【问题 2】（4 分）
主机使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。在 ISATAP 地址中，前 64 位是向 ISATAP 路由器发送请求得到的，后 64 位中由两部分构成，其中前 32 位是（3），后 32 位是（4）。
（3）备选答案：
A．0:5EFE B．5EFE:0 C．FFFF:FFFF D．0:0
（4）备选答案：
A．IPv4 广播地址 B．IPv4 组播地址 C．IPv4 单播地址
【问题 3】（4 分）
根据网络拓扑和需求说明，完成路由器 R1 的配置。
[R1] interface Serial 0
[R1- Serial0] ip address （5）//设置串口地址
[R1- Serial0]quit

[R1] interface FastEthernet 0
[R1- FastEthernet0] ip address（6）//设置以太口地址
[R1- FastEthernet0]quit
[R1] ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 192.0.0.1（7）
[R1-ospf-1-area-0.0.0.0]network 192.1.1.1（8）
【问题 4】（6 分）
根据网络拓扑和需求说明，解释路由器 R3 的 ISATAP 隧道地址。
[R3] interface Serial 0
[R3- Serial 0] ip address 192.2.2.1
[R3] interface FastEthernet 0
[R3- FastEthernet 0] ipv6 address （9）
[R3] interface tunnel 0
[R3- tunnel 0] ipv6 address 1::5EFE:202:202 64
[R3- tunnel 0] undo ipv6 nd ra halt
[R3- tunnel 0] source S0//（10）
[R3- tunnel 0]tunnel-protocal（11）
[R3- tunnel 0] quit
【问题 5】（2 分）
在配置 ISATAP 隧道的时候，主机 PC1 的设置 ISATAP 路由器地址的配置命令是 net interface ipv6 isatap>（13）

试题答案：

【问题 1】（4 分）
（1）双协议栈
（2）NAT-PT
【问题 2】（4 分）
（3）A
（4）C
【问题 3】（4 分）
（5）192.1.1.1 24
（6）192.0.0.1 24
（7）0.0.0.255
（8）0.0.0.255
【问题 4】（6 分）
（9）2::1 64
（10）指定 tunnel 源地址为 S0 口的地址
（11）ipv6-ipv4 isatap
【问题 5】（2 分）
（12）set router 192.2.2.1

试题解析：

【问题 1】（4 分）

IPv6 和 IPv4 互通包括 3 个层面：IPv6 与 IPv4 终端或服务器互通，IPv6 与 IPv4 网互通以及通过骨干 IPv4 网与对端 IPv6 网连接。针对不同的互通需求，已经有不同的技术标准出现。IPv4 终端或服务器互通采用双协议栈技术（设备上同时启用 IPv4 和 IPv6 的协议栈）来实现，对于需要跨越 IPv4 设备的 IPv6 网络之间的互联可以采用隧道技术，单一的 IPv6 网络需要访问 IPv4 网络，可以采用协议转换技术 NAT/PT 技术。

【问题 2】（4 分）

ISATAP 不但是一种自动隧道技术，同时还能对地址的自动配置。ISATAP 隧道的地址有自己特定的格式，它的接口 ID 必须如下：0000:5EFE:w.x.y.z。在这里，0000:5EFE 是规定的格式，w.x.y.z 是单播 IPv4 地址，嵌入到 IPv6 地址的最后 32 位。ISATAP 地址的前 64 位前缀是通过向 ISATAP 路由器发送请求得到的。

【问题 3\4\5】

略。