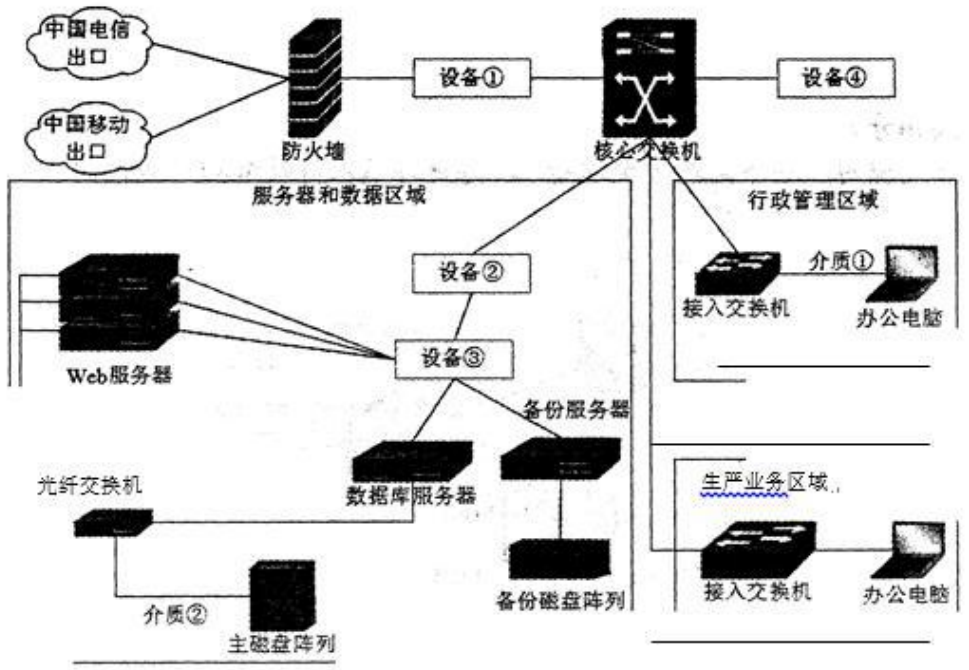
2017 年上半年网络工程师下午真题+答案

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】某企业网络拓扑如图 1-1 所示，中国电信和中国移动双链路接入，采用硬件设备实现链路负载均衡:主磁盘阵列的数据通过备份服务器到备份磁盘阵列。请结合下图，回答相关问题。



问题：1.1

图 1-1 中，设备①处部署（1），设备②处部署(2)，设备③处部署(3)。

(1)~(3)备选答案（每个选项限选一次):

入侵防御系统(IPS) B. 交换机 C. 负载均衡

问题：1.2

图 1-1 中，介质①处应采用(4)，介质②处应采用(5)

(4)~(5) 备选答案(每个选项限选一次):

双绞线 B. 同轴电缆 C. 光纤

问题：1.3

图 1-1 中，为提升员工的互联网访问速度，通过电信出口访问电信网络，移动出口访问移动网络，则需要配置基于(6)地址的策略路由:运行一段时间后，网络管理员发现电信出口的用户超过 90% 以上，网络访问速度缓慢，为实现负载均衡，网络管理员配置基于 (7)一地址的策略路由，服务器和数据区域访问互联网使用电信出口，行政管理区域员工访问互联网使用移动出口，生产业务区域员工使用电信出口。

问题：1.4

1. 图 1-1 中，设备④处应为（8），该设备可对指定计算机系统进行安全脆弱性扫描和检测，发现其安全漏洞，客观评估网络风险等级。

2. 图 1-1 中，（9）设备可对恶意网络行为进行安全检测和分析。

3. 图 1-1 中，（10）设备可实现内部网络和外部网络之间的边界防护，依据访问规则，允许或者限制数据传输。

答案解析：问题一（共 6 分）

（1）C

（2）A

（3）B

综合分析，设备 3 是交换机，那么设备 2 是 IPS，而设备 1 选择负载均衡。

问题二（共 4 分）

（4）A

（5）C

介质 1 连接接入交换机和用户，为双绞线，而介质 2 连接 FC 交换机和磁盘阵列，所以是光纤。

问题三（共 4 分）

（6）目的

（7）源访问电信网络走电信出口，访问移动网络走移动出口，所以是基于目的地址的策略路由。而后来根据需求改为基于源地址的策略路由。

问题四（共 6 分）

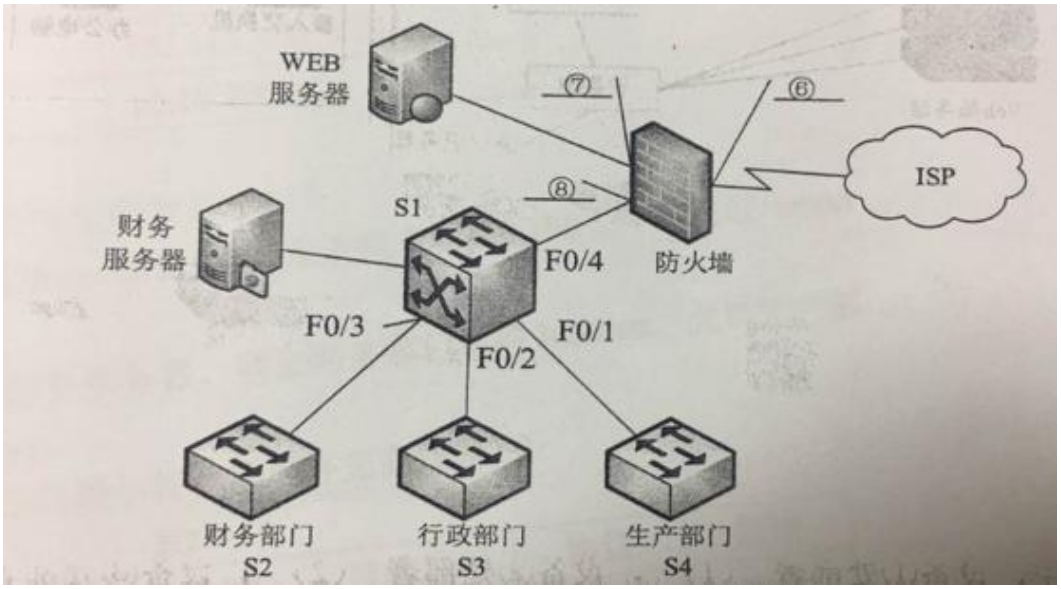
（8）漏洞扫描设备

（9）IPS

（10）防火墙

漏洞扫描通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的 一种安全检测（渗透攻击）行为。漏洞扫描技术是一类重要的网络安全技术。所以这里是漏洞扫描设备。在图中，IPS 设备对恶意网络行为进行分析。防火墙设备实现内外网之间的安全保护。

第 2 题：阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。【说明】某公司的网络拓扑结构图如图 2-1 所示



问题：2.1 为了保障网络安全，该公司安装了一款防火墙，对内部网络、服务期以及外部网络

进行逻辑隔离，其网络结构如图 2-1 所示。

包过滤防火墙使用 ACL 实现过滤功能，常用的 ACL 分为两种，编号为（1）的 ACL 根据 IP 报文的（2）域进行过滤，称为（3）；编号为（4）的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为（5）

(1)~(5) 备选项:

A.标准访问控制列表

B.扩展访问控制列表

C.基于时间的访问控制列表

D.1-99

E.0-99

F.100-199

G.目的的 IP 地址

H.源 IP 地址 .

I. 源端口

J.目的端口问题

2.2 如图 2-1 所示，防头墙的三个端口，端口⑥是（6）、端口⑦是（7）、端口⑧（8）。

(6）~（8) 是备选项

A. 外部网络 B. 内部网络 C. 非军事区问题

2.3 公司内部 E 地址分配如下

表2-1

部门/服务器	IP地址段
财务部门	192.168.9.0/24
生产部门	192.168.10.0/24
行政部门	192.168.11.0/24
财务服务器	192.168.100.1/24
Web服务器	10.10.200.1/24

1.为保护内网安全，防火墙的安全配置要求如下

(1)内外网用户均可访问 Web 服务器，特定主机 200.120.100.1 可以通过 Telnet 访问 Web 服务器。

(2)禁止外网用户访问财务服务器，禁止财务部门访问 Intemet ，允许生 产部门和行政部门访问

Intemet 。根据以上需求，请按照防火墙的最小特权原则补充完成表 2-2:

表2-2

序号	源地址	源端口	目的地址	目的端口	协议	规则
1	Any	Any	（9）	（10）	WWW	允许
2	（11）	Any	10.10.200.1	（12）	telnet	允许
3	（13）	Any	Any	Any	Any	（14）
4	Any	Any	Any	Any	Any	（15）

2.若调换上面配置中的第 3 条和第 4 条规则的顺序，则（16）（16）备选项：

安全规则不发生变化
财务服务器将受到安全威胁
Web 服务器将受到安全威胁
内网用户将无法访问 Intemet
3. 在上面的配置中，是否实现了"禁止外网用户访问财务服务器"这条规则?
答案解析：
问题一：
（1）D
（2）H
（3）A
（4）F
（5）B
问题 1：
访问控制列表用来限制使用者或设备，达到控制网络流量，解决拥塞，提高安全性等。在 IP 网络中，可以使用的访问列表有标准访问列表（值为 1~99、1300-1999）、扩展访问列表（标号为 100~199、2000-2699）两种。
标准访问列表：基于源 IP 地址进行判定是否允许或拒绝数据包通过。
扩展的访问列表是在标准访问列表的基础上增加更高层次的控制，它能够基于目的地址、端口号码、协议来控制数据包。
问题二：
（6）A
（7）C
（8）B
问题 2：
防火墙通常具有至少 3 个接口，使用防火墙时，就至少产生了 3 个网络，描述如下：
内部区域（内网）。内部区域通常就是指企业内部网络或者是企业内部网络的一部分。它是互连网络的信任区域，即受到了防火墙的保护。
外部区域（外网）。外部区域通常指 Internet 或者非企业内部网络。它是互连网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务，通过防火墙，就可以实现有限制的访问。
非军事区（DMZ，又称停火区）。是一个隔离的网络，或几个网络。位于区域内的主机或服务器被称为堡垒主机。一般在非军事区内可以放置 Web、Mail 服务器等。停火区对于外部用户通常是可以访问的，这种方式让外部用户可以访问企业的公开信息，但却不允许它们访问企业内部网络。
答案解析：
问题三：
（9）10.10.200.1（10）80（11）200.120.100.1（12）23
（13）192.168.10.0（14）允许（15）拒绝（16）D（17）已经实现，除开允许的，其余均已经禁止

问题 3：

配置略，请查看答案。

访问控制列表就是用来在路由技术的网络中，决定这些数据流量是应该被转发还是被丢弃的技术。同时访问控制列表成为实现防火墙实现的重要手段。

设置 ACL 的一些规则：

1，按顺序进行比较，先比较第一行，再比较第二行，直到最后一行；

从第一行起，直到找到 1 个符号条件的行；符合之后，其余的行就可以不用继续比较下去；

3，默认在每个 ACL 中最后一行都隐藏有拒绝所有，如果之前没找到一条允许（permit）语句，意味着包将会被丢弃，所以每个 ACL 必须至少有一行 Permit 语句，除非用户想把所有的数据包丢弃。

如果 3、4 条规则顺序交换， 会导致内网用户无法访问互联网。

另外禁止外网访问财务服务器已经实现，因为配置中除开允许的，其余均已经禁止

第 3 题：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】

请根据 Windows 服务器的安装与配置，回答下列问题。

问题：3.1

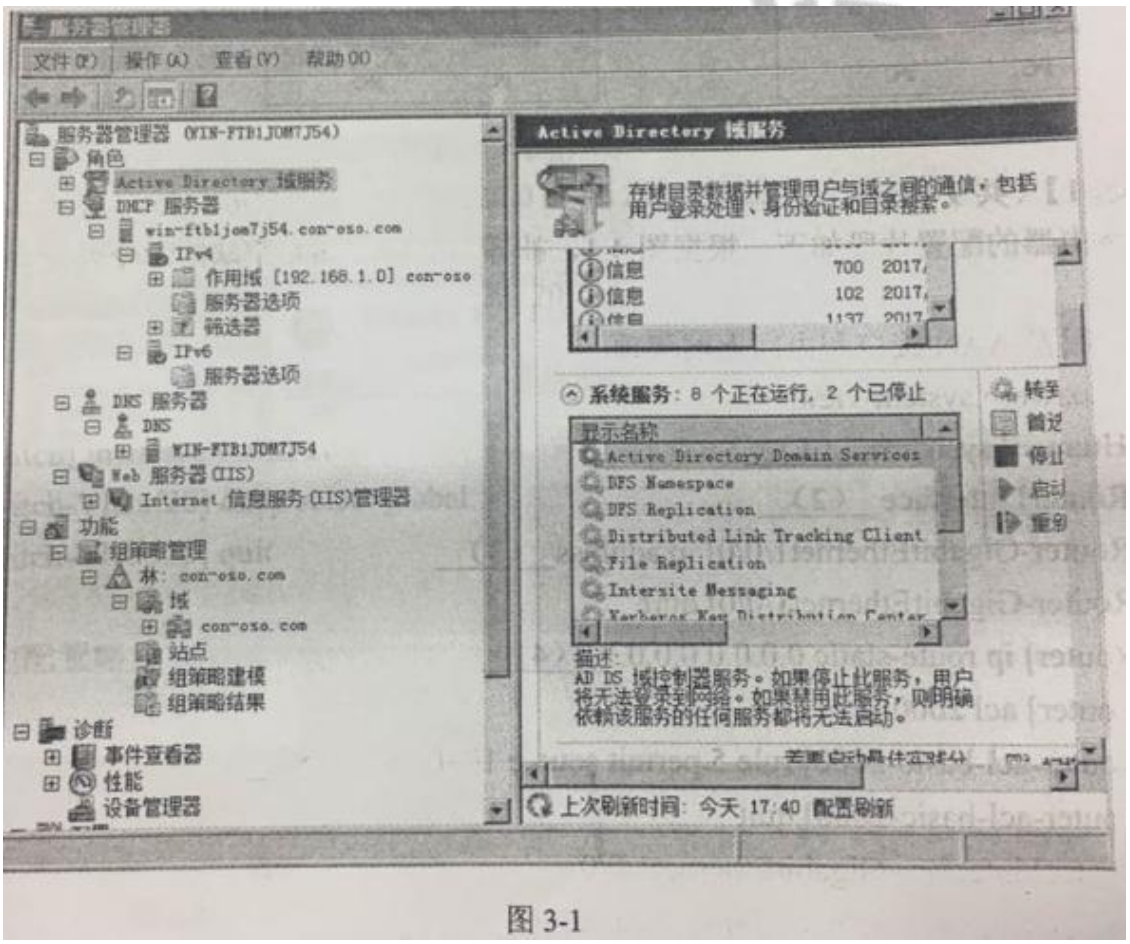


图 3-1

图 3-1 是安装好的服务器管理器界面，在当前配置下，根域的名称是(1)。

图示中角色服务配置时，建立域控制器 DC(Domain Controller),需要通过命令行方式运行(2) 命令；域中的 DC 和 DNS 配置在同一设备时，需要将独立服务器的首个 DNS 与 DC 的 IP

地址配置为（3）；DHCP 服务加入 DC 需要（4），否则服务报错。

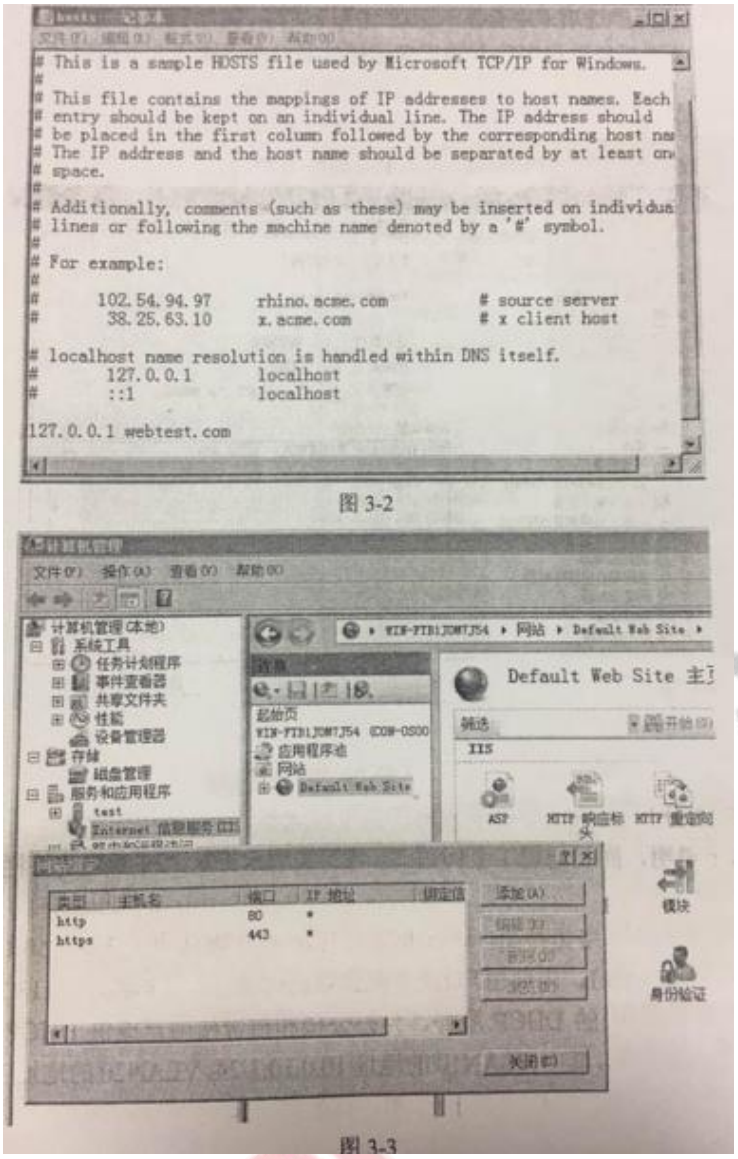


图 3-2

图 3-3

（2）备选答案：

A.dcomcnfg B.dcpromo 问题：3.2

3-2 是 hosts 文件内容，图 3-3 是配置安全站点 https://webtest.com 的界面。

3-2 中，127.0.0.1 webtest.com 的含义是(5)。在建立安全站点时，需要在 WEB 服务器上启用（6）功能，并且绑定创建好的证书。

备选答案: A:SSL B. 代理

若将图 3-3 中 https 的端口号改为 8000，访问站点的 URL 是(7)

问题：3.3

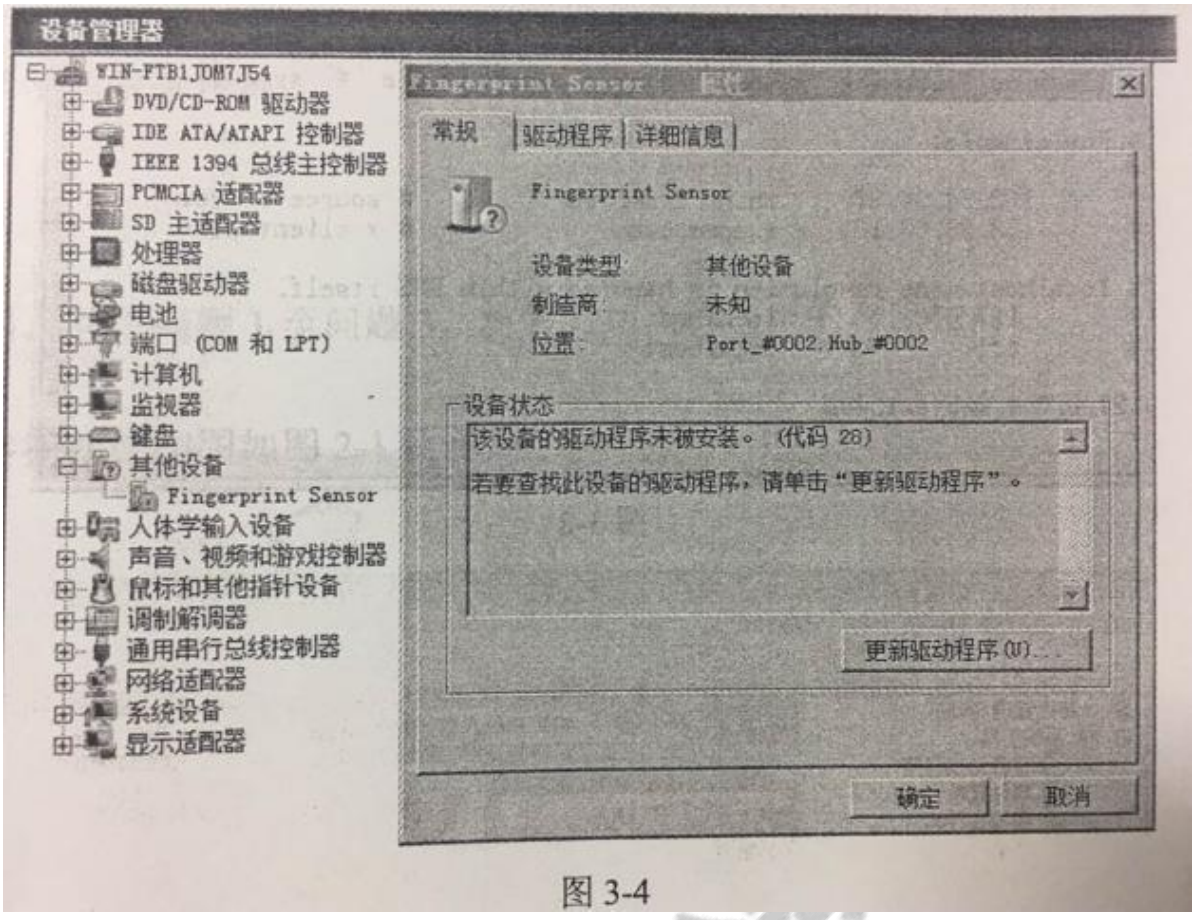


图 3-4

图 3-4 是通过设备管理器查看到的信息，未安装驱动程序的设备提供（8）功能。

在"驱动程序" 选项卡中会显示驱动程序提供商、驱动程序日期、 驱动程序版本和（9）信息。若更新驱动程序后无法正常运行，可以在该选项卡页面通过（10）操作将以前的驱动程序恢复。

(9)备选答案:

A. 数字签名 B.硬件类型

答案解析：问题一：

（1）con-oso.com

（2）B（3）一样（4）授权

答案解析：问题二：

（5）在主机 HOSTS 表中建立 webtest.com 和 127.0.0.1 的对应关系（6）A

（7）https://webtest.com:8000

问题二：（5）在主机 HOSTS 表中建立 webtest.com 和 127.0.0.1 的对应关系

SSL 可以对万维网客户与服务器之间传送的数据进行加密和鉴别。在双方握手阶段，对将要使用的加密算法和双方共享的会话密钥进行协商，完成客户与服务器之间的鉴别。在握手完成后，所传送的数据都使用会话密钥进行传输。

答案解析：问题三：

（8）更新驱动程序（9）A（10）回退驱动程序

第 4 题：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。【说明】

图 4-1 为某学校网络拓扑图，运营商分配的公网 IP 地址为 113.201.60.1/29，运营商网关地址为 113.201.60.1，内部用户通过路由器代理上网，代理地址为 113.201.60.2.核心交换机配置基于全局的 DHCP 服务，在办公楼和宿舍楼用户提供 DHCP 服务。内部网络划分为 3 个 VLAN,其中 VLAN10 的地址 10.0.10.1/24，VLAN20 的地址 10.0.20.1/24，VLAN30 的地址 10.0.30.1/24，请结合下图，回答相关问题

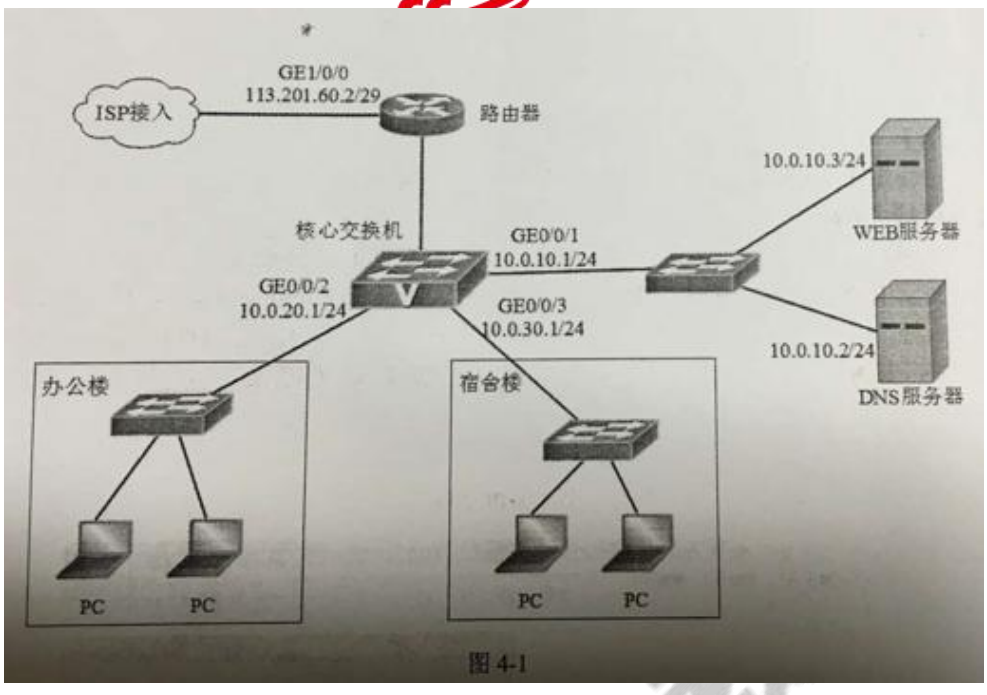


图 4-1

问题：4.1 路由器的配置片段如下，根据图 4-1，补齐(1) ~(6) 空缺的命令。

#配置 WAN 接口和内网上网代理

<Huawei>system-view [Huawei] sysname（ ）[Router] interface（ ）

[Router-GigabitEthernet1/0/0] ip address

[Router-GigabitEthernet1/0/0] quit [Router] ip route-static 0.0.0.0

0.0.0（ ） [Router-acl-basic-2000]

[Router-acl-basic-2000] rule 5 permit source 10.0.0 （ ）

[Router-acl-basic-2000] quit

[Router] interface GigabitEthernet1/0/0 [Router-GigabitEthernet1/0/0]

nat outbound（ ） [Router-GigabitEthernet1/0/0] quit

……

其他配置略问题：4.2 核心交换机的配置片段如下，根据图 4-1，补齐 (7)~(10)

空缺的命令。

#配置 GEO/0/2 接口加入 VLAN20，并配置对应 VLAN 接口地址

[Switch]vlanbatch20

[Switch]inlterface GigabitEthernet0/0/2

[Switch-GigabitEthernet0/0/2]port link-type( )

[Switch-GigabitEthernet0/0/2]port hybrid pvid vlan20

[Switch-GigabitEthernet0/0/2]port hybrid untagged vlan20

[Switch-GigabitEthernet0/0/2]quit

[Switch] interface vlanif 20 [Switch-Vlanif20] ip address( )

[Switch-Vlanif20] quit

.....

其他配置略

#配置 DHCP 服务，租期 3 天 [Switch] dhcp( ) [Switch] ip pool pooll

[Switch-ip-pool-pooll] network 10.0.20.0 mask 225.225.255.0

[Switch-ip-pool-pooll] dns-list 10.010.2 [Switch-ip-pool-pooll]

gateway-list 10.0.20.1 [Switch-ip-pool-pooll] lesae day( )

[Switch-ip-pool-pooll] quit [Switch] interface vlanif 20

[Switch-Vlanif20] dhcp select global [Switch-Vlanif20] quit

.....

其他配置略

答案解析：问题一：（共 9 分）

（1）Router

（2）GigabitEthernet 1/0/0

（3）113.201.60.2 255.255.255.248 （4）113.201.60.1（5）0.0.255.255

（6）2000

问题一：（共 9 分）

（1）对设备进行重命名。（2）进入端口子模式（3）给端口配置 IP 和掩码。

（4）配置默认路由，下一跳指向 ISP 地址。（5）配置反掩码（6）把符合 ACL2000 的地址做 NAT 转换

答案解析：问题二：（共 6 分）

（7）hybird（8）10.10.20.1 255.255.255.0 （9）enable（10）3

问题二：（共 6 分）

（7）除了 Access 类型和 Trunk 类型外，交换机还支持第三种 Hybrid 类型端口。这种接口可以接收和发送多个 VLAN 数据帧，同时还能指定对任何 VLAN 帧进行剥离标签操作。

（8）配置接口 IP 和掩码（9）dhcp enable：开启 DHCP 配置。

lease day 3：配置租约期间为 3 天。