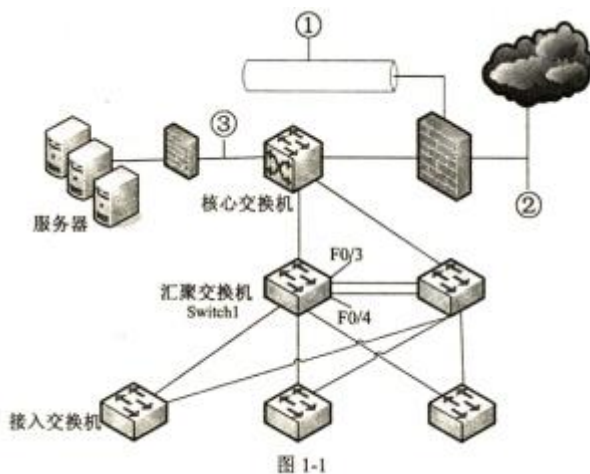


试题一

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】

某企业网络拓扑图如图 1-1 所示。



工程师给出了该网络的需求：

1. 用防火墙实现内外网地址转换和访问控制策略；
2. 核心交换机承担数据转发，并且与汇聚层两台交换机实现 OSPF 功能；
3. 接入层到汇聚层采用双链路方式组网；
4. 接入层交换机对地址进行 VLAN 划分；
5. 对企业的核心资源加强安全防护。

【问题 1】(4 分)

该企业计划在①、②或③的位置部署基于网络的入侵检测系统(NIDS)，将 NIDS 部署在①的优势是 (1)；将 NIDS 部署在②的优势是 (2)、(3)；将 NIDS 部署在③的优势是 (4)。

(1) ~ (4) 备选答案:

- A.检测外部网络攻击的数量和类型
- B.监视针对 DMZ 中系统的攻击
- C.监视针对关键系统、服务和资源的攻击
- D. 能减轻拒绝服务攻击的影响

(1) C

(2) A

(3) D

(4) B

本题考查网络规划以及组网的相关基础知识。包括入侵检测系统部署的技术规范，企业组网中路由协议的选用、线路聚合、生成树协议等相关知识。

入侵检测系统 (IDS)可以基于主机部署也可以基于网络进行部署，将 IDS 部署在网络中不同的位置区域可以达到对网络中异常行为和攻击的识别，对特定网络区域的资源进行保护。例如，将 IDS 部署在网络出口常用于监测外部网络攻击的数量和类型。

【问题 2】(4 分)

OSPF 主要用于大型、异构的 IP 网络中，是对 (5) 路由的一种实现。若网络规模较小，可以考虑配置静态路由或 (6) 协议实现路由选择。

(5) 备选答案: A. 链路状态 B. 距离矢量 C. 路径矢量

(6) 备选答案: A. EGP B. RIP C. BGP

(5) A

(6) B

路由器提供了异构网互联的机制，实现将一个网络的数据包发送到另一个网络。

而路由就是指导 IP 数据包发送的路径信息。路由协议就是在路由指导 IP 数据包发送过程中事先约定好的规定和标准。常见的路由协议分为分为动态路由和静态路由，而动态路由协议又距离矢量路由协议和链路状态路由协议。

OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态來建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。

【问题 3】(4 分)

对汇聚层两台交换机的 F0/3、F0/4 端口进行端口聚合，F0/3、F0/4 端口默认模式是 (7)，进行端口聚合时应配置为 (8) 模式。

(7)、(8) 备选答案：

A. multi B.trunk C.access

(7) C

(8) B

端口聚合也叫做以太通道 (Ethernet Channel),主要用于交换机之间连接。由于两个交换机之间有多条冗余链路的时候，STP 会将其中的几条链路关闭，只保留一条，这样可以避免二层的环路产生。

同一个汇聚组中端口的的基本配置应该保持一致，即如果某端口为 trunk 端口，则其他端口也配置为 trunk 端口；如该端口的链路类型改为 access 端口，则其他端口的链路类型也改为 access 端口。

【问题 4】(6 分)

为了在汇聚层交换机上实现虚拟路由冗余功能，需配置 (9) 协议，可以采用竞

争的方式选择主路由设备，比较设备优先级大小，优先级大的为主路由设备。若备份路由设备长时间没有收到主路由设备发送的组播报文，则将自己的状态转为（10）。

为了避免二层广播风暴，需要在接入与汇聚设备上配置（11）。

（10）、（11）备选答案：

A. Master B.Backup C.VTP Server D.MSTP

（9）VRRP 或者 HSRP

（10）A

（11）D

汇聚交换机采用虚拟路由冗余，目的是当一台汇聚交换机出现故障时，启用备份线路的措施。根据设备情况可以采用虚拟路由器冗余协议（VRRP）或热备份路由器协议（HSRP）。

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

【问题5】（2分）

阅读汇聚交换机 Switch 1 的部分配置命令，回答下面的问题。

```
Switch 1(config)#interface vlan 20
```

```
Switch 1 (config-if)#ip address 192.168.20.253 255.255.255.0
```

```
Switch 1 (config-if)#standby 2 ip 192.168.20.250
```

```
Switch 1 (config-if)#standby 2 preempt
```

```
Switch 1 (config-if)#exit
```

VLAN20standby 默认优先级的值是（12）。

VLAN20 设置 preempt 的含义是 (13)。

(12) 100

(13) 设置为抢占模式，或交换机故障恢复后抢占 vlan20 的控制权。

HSRP 协议利用优先级决定哪个路由器成为活动路由器。如果一个路由器的优先级比其他路由器的优先级高，则该路由器成为活动路由器，路由器的默认优先级是 100。

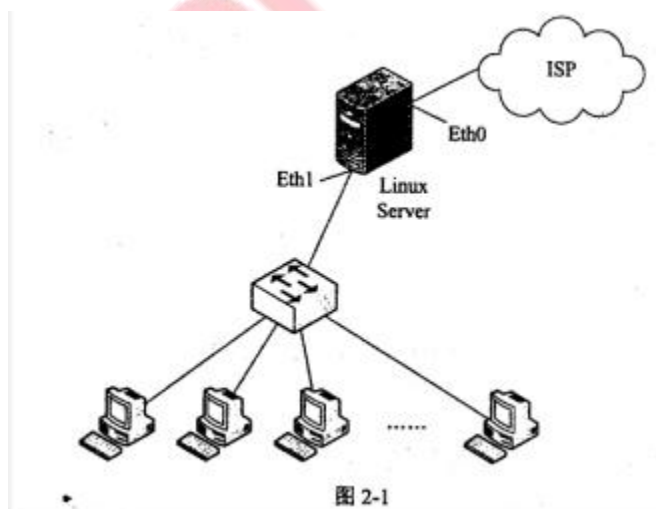
当在交换机上配置链路冗余或负载均衡后，保证故障设备恢复后正常工作，需要设置 preempt 模式。

试题二

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】

某公司内部搭建了一个小型的局域网，拓扑图如图 2-1 所示。公司内部拥有主机约 120 台，用 C 类地址段 192.168.100.0/24。采用一台 Linux 服务器作为接入服务器，服务器内部局域网接口地址为 192.168.100.254，ISP 提供的地址为 202.202.212.62。



【问题1】(2分)

在Linux中，DHCP的配置文件是(1)。

(1) dhcpd.conf

本题考查Linux服务器下DHCP服务器的配置。

DHCP服务是一种动态的为客户端主机分配IP地址的服务，在Linux服务器中，该服务的配置文件是dhcpd.conf。

【问题2】(8分)

内部邮件服务器IP地址为192.168.100.253，MAC地址为01:A8:71:8C:9A:BB；内部文件服务器IP地址为192.168.100.252，MAC地址为01:15:71:8C:77:BC。公司内部网络分为4个网段。

为方便管理，公司使用DHCP服务器为客户机动态配置IP地址，下面是Linux服务器为192.168.100.192/26子网配置DHCP的代码，将其补充完整。

Subnet (2) netmask (3)

{ option routers 192.168.100.254;

option subnet-mask (4);

option broadcast-address (5);

option time-offset -18000;

range (6)(7);

default-lease-time 21600;

max-lease-time 43200;

host servers

{Hardware ethernet (8);

```
fixed-address 192.168.100.253;  
hardware ethernet 01:15:71:8C:77:BC;  
fixed-address ( 9 ) ;}}
```

(2) 192.168.100.192

(3) 255.255.255.192

(4) 255.255.255.192

(5) 192.168.100.255

(6) 192.168.100.193

(7) 192.168.100.251

(8) 01:A8:71:8C:9A:BB

(9) 192.168.100.252

问题中给出了该公司所使用的 IP 地址所在子网为 192.168.100.192/26，网络号为 192.168.100.192，子网掩码为 255.255.255.192。本网的广播地址是将本网段中所有主机部分的二进制位数全部变为 1 得到，为 192.168.100.255。

空(6)和空(7)是要求计算该子网的 IP 地址范围，其有效的 IP 地址为 192.168.100.193 -192.168.100.254。

空(8)和空(9)按照问题的描述，要求填写对应的硬件地址和 IP 地址。

【问题 3】(2 分)

配置代码中 “ option time-offset -18000 ” 的含义是 (10) 。

“default-lease-time 21600” 表明，租约期为 (11) 小时。

(10) 备选答案:

A. 将本地时间调整为格林威治时间 B. 将格林威治时间调整为本地时间 C. 设

置最长租约期

(10) B

(11) 6

option time-offset -18000 的配置项,是为了使得本地的 DHCP 服务器时间采用本地的时间进行计时,将从时间服务器中获取的格林威治时间调整到与本地时间同步的目的。default-lease-time 21600 的配置项是设置 IP 地址分配给客户端后的失效时间,改时间以秒为单位,即时间为 12600 秒,将其换算为小时的方法是 $216000 \text{ 秒} / 3600 \text{ 秒} = 6 \text{ 小时}$ 。

【问题 4】(3 分)

在一台客户机上使用 ipconfig 命令输出如图 2-2 所示,正确的说法是 (12)。

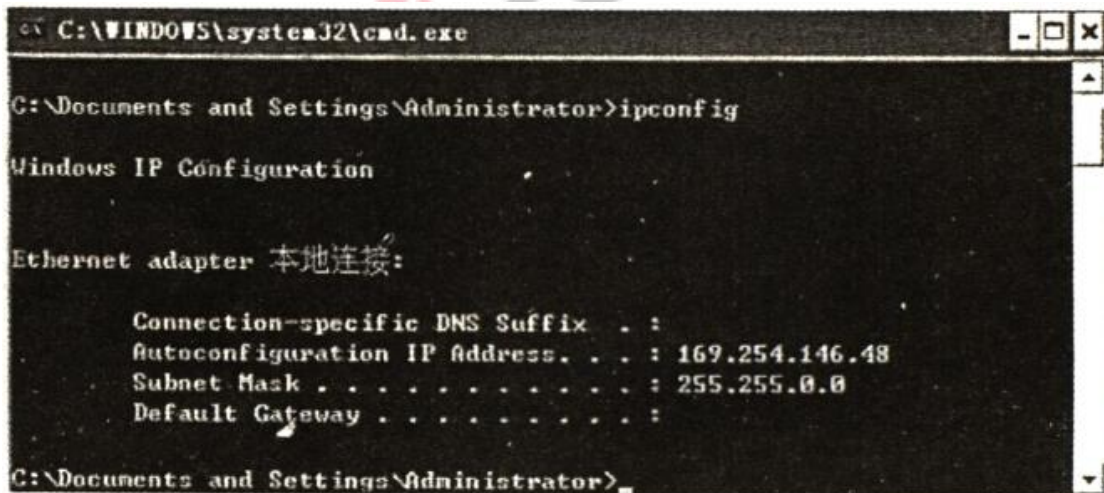


图 2-2

此时可使用 (13) 命令释放当前 IP 地址,然后使用 (14) 命令向 DHCP 服务器重新申请 IP 地址。

(12) 备选答案:

- A.本地网卡驱动未成功安装
- B.未收到 DHCP 服务器分配的地址
- C.DHCP 服务器分配给本机的 IP 地址为 169.254.146.48
- D.DHCP 服务器的 IP 地址为 169.254.146.48

(12) B

(13) ipconfig/release

(14) ipconfig/renew

图中所示的故障,是由于该客户端并未接收到系统的 DHCP 服务器所发来的 IP 地址配置信息,而有 TCP/IP 协议集为该客户端分配的 169.254.x.x 段的地址。169.254.x.x 地址是 IANA 组织规定的保留地址,为了未采用 DHCP 服务器动态分配 IP 地址的用户,当未获取 DHCP 分配的 IP 地址时,自动使用该段地址,该段地址一般不能使网络正常运行。

试题三

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】

某企业在采用 Windows Server 2003 配置了共享打印、FTP 和 DHCP 服务。

【问题 1】(8 分)

1. Internet 共享打印使用的协议是 (1)。(1 分)

(1) 备选答案:

- A. PPI B. IPP C. TCP D. IP

2. Internet 共享打印配置完成后,需在如图 3-1 所示的 Web 服务扩展选项卡中将“Active Server Pages”设置为“允许”,其目的是 (2)。(2 分)

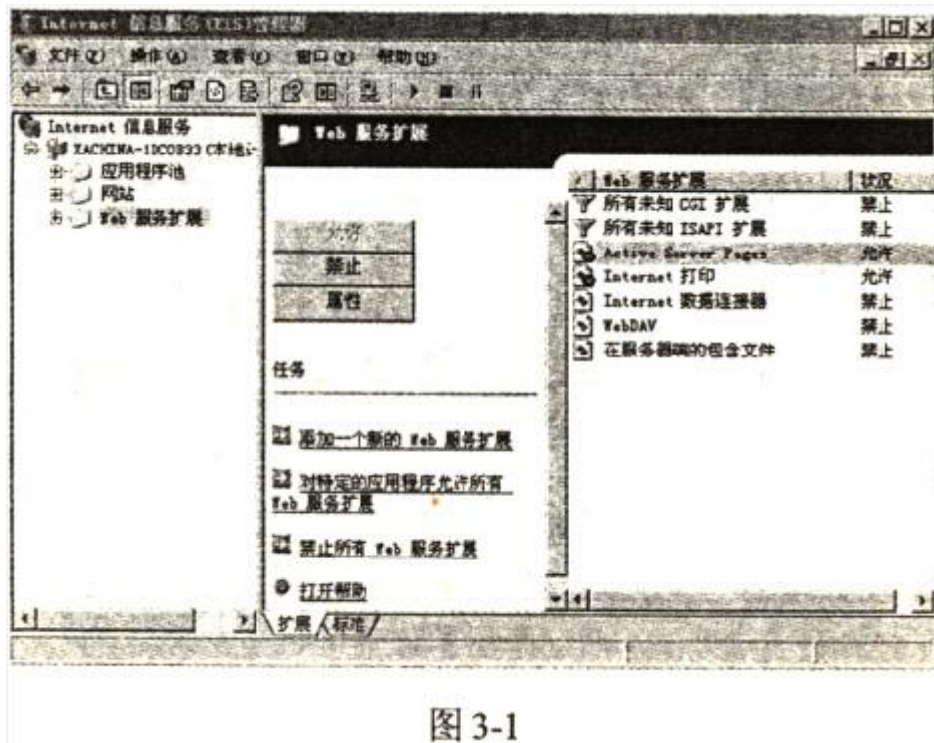


图 3-1

3. 检验 Internet 打印服务是否安装正确的方法是在 Web 浏览器的地址栏输入 URL 是 (3)。(2分)

(3) 备选答案:

- A. HTTP://127.0.0.1/PRINTERS
- B. FTP://127.0.0.1/PRINTERS
- C. HTTP://PRINTERS
- D. FTP://PRINTERS

4. 使用 Internet 共享打印流程为 6 个步骤:

- ①在终端上输入打印设备的 URL
- ②服务器向用户显示打印机状态信息
- ③客户端向打印服务器发送身份验证信息
- ④用户把要打印的文件发送到打印服务器
- ⑤打印服务器生成一个 cabinet 文件，下载到客户端

⑥通过 Internet 把 HTTP 请求发送到打印服务器

对以上步骤进行正确的排序（4）。（3分）

（1）B

（2）可采用页面显示打印机状态信息

（3）A

（4）①⑥③②⑤④

本题考查 Windows Server 2003 配置共享打印、FTP 和 DHCP 服务等相关知识。

IPP 协议是一个基于 Internet 应用层的协议，它面向终端用户和终端打印设备。IPP 基于常用的 Web 浏览器向终端设备传送打印机的属性和状态信息需要将 Web 服务扩展选项卡中将“Active Server Pages”设置为“允许”。

Internet 打印流程如下：

①用户输入打印设备的 URL (统一资源定位符),通过 Internet 连接到打印服务器。

②HTTP 请求通过 Internet 发送到打印服务器。

③打印服务器要求客户端提供身份验证信息。这样能够确保只有经过授权的用户才能在打印服务器上打印文件。

④当用户获得授权可以访问打印服务器后，服务器使用活动服务器页（Active Server Pages, ASP)向用户显示状态信息，其中包括有关当前空闲打印机的信息。

⑤当用户连接 Internet 打印网页上的任何打印机时，客户端计算机首先尝试在本地寻找该打印机的驱动程序。如果没有找到适合的驱动程序，打印服务器将会

生成一个 Cabinet 文件（.cab 文件，又称为 Setup 文件），其中包含正确的打印机驱动程序文件。打印服务器把.cab 文件下载到客户端计算机上。客户端计算机提示用户允许下载该.cab 文件。

⑥当用户连接到 Internet 打印机后,他们可以使用 Internet 打印协议(Internet Printing Protocol, IPP)把文件发送到打印服务器。

【问题 2】(8 分)

FTP 的配置如图 3-2、图 3-3 所示。

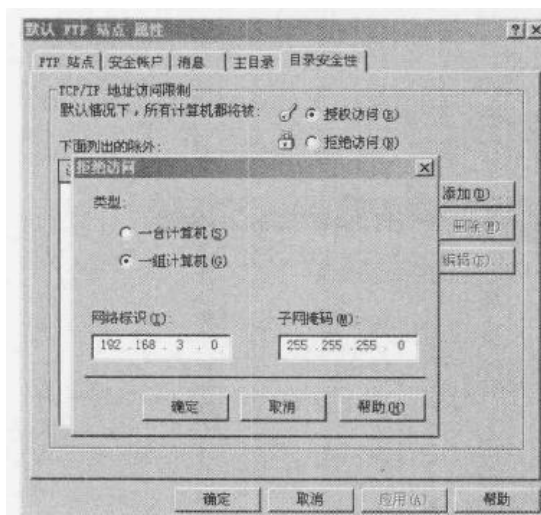


图 3-2

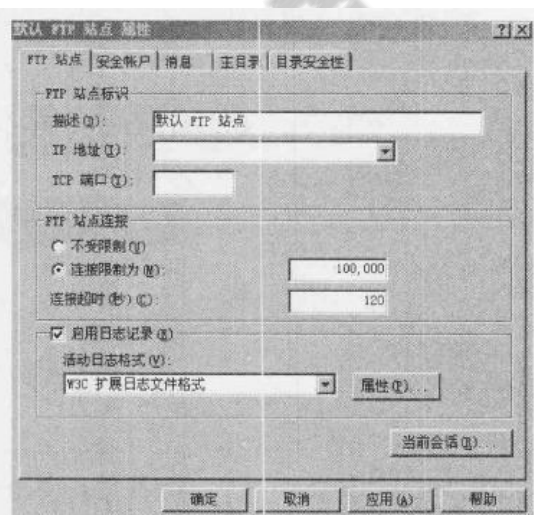


图 3-3

1. 默认情况下,用户登录 FTP 服务器时,服务器端建立的 TCP 端口号为(5)。
2. 如果只允许一台主机访问 FTP 服务器,参考图 3-2 给出具体的操作步骤(6)。
3. 参考图 3-3,在一台服务器上搭建多个 FTP 站点的方法是(7)。
4. 如点击图 3-3 中“当前会话”按钮,显示的信息是(8)。

(5) 21

(6) 在“目录安全性”页面选中“拒绝访问”,单击“添加”,在弹出的“授权

访问”页面，选中“一台计算机”，填入允许访问的主机 IP

(7) 增加 IP 地址或修改 TCP 端口

(8) 连接 FTP 的用户或主机的信息

在 Windows Server 2003 环境下安装 FTP 服务需要在“Internet 信息服务”组件中添加“文件传输协议 (FTP)”功能模块。该功能模块的配置可以实现特定用户对 FTP 的访问、建立多个 FTP 站点、显示用户连接 FTP 状态等功能。

FTP 服务器端建立的 TCP 端口号是 21。

【问题 3】(4 分)

DHCP 的配置如图 3-4 和 3-5 所示。

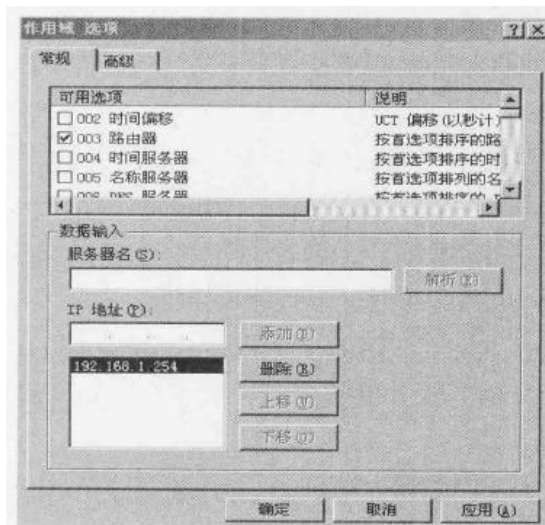


图 3-4

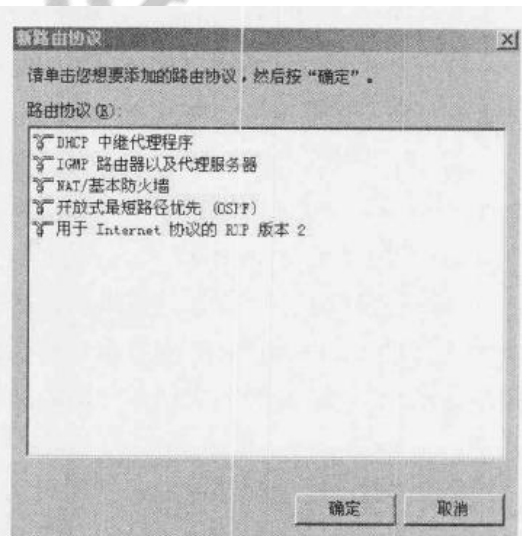


图 3-5

1. 图 3-4 中填入的 IP 地址是 (9) 。
2. 图 3-5 中配置 DHCP 中继代理程序，可以实现 (10)。

(9) 备选答案：

A. 分配给客户端的 IP 地址

B. 默认网关的 IP 地址

C. DHCP 服务器的 IP 地址

(10) 备选答案:

A. 使普通客户机获取 IP 等信息

B. 跨网段的地址分配

C. 特定用户组访问特定网络

(9) B

(10) B

动态主机分配协议 (DHCP) 是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 Windows Server 2003 提供的组件进行 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作。在进行 DHCP 服务器配置时需要填入待分配的 IP 段以及默认网关等信息。

在大型的网络中, 可能会存在多个子网。DHCP 客户机通过网络广播消息获得 DHCP 服务器的响应后得到 IP 地址。但广播消息是不能跨越子网的。如果 DHCP 客户机和服务器在不同的子网内, 就要用到 DHCP 中继代理。

试题四

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】

某企业的网络拓扑结构如图 4-1 所示。

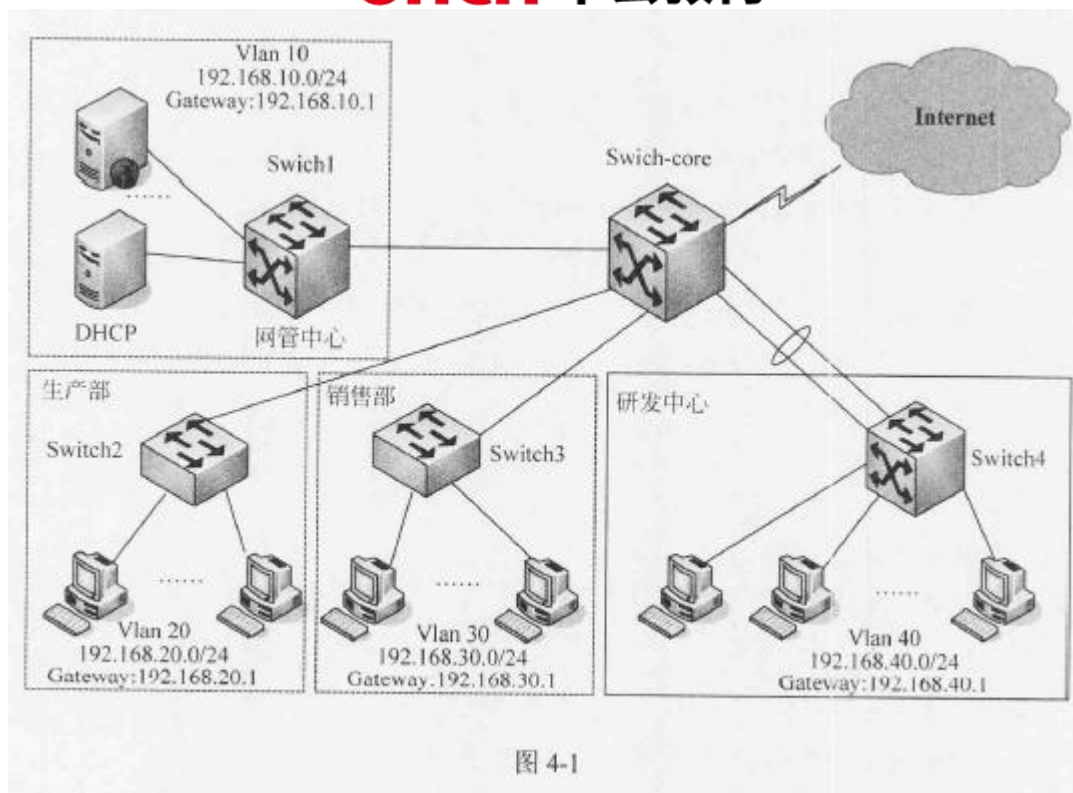


图 4-1

由于该企业路由设备数量较少，为提高路由效率，要求为企业构建基于静态路由的多层安全交换网络。根据要求创建 4 个 VLAN 分别属于网管中心、生产部、销售部以及研发中心，各部门的 VLAN 号及 IP 地址规划如图 4-1 所示。该企业网采用三层交换机 Switch-core 为核心交换机，Switch-core 与网管中心交换机 Switch1 和研发中心交换机 Switch4 采用三层连接，Switch-core 与生产部交换机 Switch2 及销售部交换机 Switch3 采用二层互联。各交换机之间的连接以及接口 IP 地址如表 4-1 所示。

表 4-1 各交换机之间的连接以及接口 IP 地址表

交换机	上联端口			下联端口			
	端口	描述	IP 地址	交换机	端口	描述	IP 地址
Switch-core	G0/1	scsw-g1/1		Switch2	G1/1	core-g0/1	
	G0/2	wgsw-g0/1	192.168.101.1/24	Switch1	G0/1	core-g0/2	192.168.101.2/24
	F0/1	yfsw-f0/1	192.168.102.1/24	Switch4	F0/1	core-f0/1	192.168.102.2/24
	F0/2	yfsw-f0/2			F0/2	core-f0/2	
	F0/3	yfsw-f0/3			F0/3	core-f0/3	
	F0/4	yfsw-f0/4			F0/4	core-f0/4	
F0/5	xssw-f0/1		Switch3	F0/1	ccre-f0/5		

【问题 1】(4 分)

随着企业网络的不断发展,研发中心的上网计算机数急剧增加,在高峰时段研发中心和核心交换机之间的网络流量非常大,在不对网络进行大的升级改造的前提下,网管人员采用了以太信道(或端口聚合)技术来增加带宽,同时也起到了(1)和(2)的作用,保证了研发中心网络的稳定性和安全性。

在两台交换机之间是否形成以太信道,可以用协议自动协商。目前有两种协商协议:一种是(3),是 Cisco 私有的协议;另一种是(4),是基于 IEEE 802.3ad 标准的协议。

(3)、(4) 备选答案:

- A. 端口聚合协议(PAgP)
- B. 多生成树协议(MSTP)
- C. 链路聚合控制协议(LACP)

(1) 负载均衡

(2) 链路冗余

(3) A

(4) C

本题考查使用三层交换机实现 VLAN 间路由的相关知识点和配置命令。

本问题主要考查以太信道(或端口聚合)技术。

EtherChannel 是由 Cisco 研发的,应用于交换机之间的多链路捆绑技术。它的基本原理是:将两个设备间多条相同特性的快速以太或千兆位以太物理链路捆绑在一起组成一条逻辑链路,从而达到带宽倍增的目的。除了增加带宽外,EtherChannel 还可以在多条链路上均衡分配流量,起到负载均衡的作用;当

一条或多条链路故障时，只要还有链路正常，流量将转移到其他的链路上，整个过程在几毫秒内完成，从而起到链路冗余的作用，增强了网络的稳定性和安全性。

在 EtherChannel 中，负载在各个链路上的分布可以根据源 IP 地址、目的 IP 地址、源 MAC 地址、目的 MAC 地址、源 IP 地址和目的 IP 地址组合，以及源 MAC 地址和目的 MAC 地址组合等来进行分布。

两台交换机之间是否形成 EtherChannel 也可以用协议自动协商。目前有两个协商协议：PAgP 和 LACP，PAgP（端口汇聚协议 Port Aggregation Protocol）是 Cisco 私有的协议，而 LACP（链路汇聚控制协议 Link Aggregation Control Protocol）是基于 IEEE 802.3ad 的国际标准。语法为：
channel-group [num] mode [auto | on | desirable]

其中，auto:被动协商；on:不协商；desirable:主动协商。

on 只能和 on 起 channel,两个 auto 不能起 channel。

【问题 2】(7 分)

核心交换机 Switch-core 与网管中心交换机 Switch1 通过静态路由进行连接。

根据需求，完成或解释 Switch-core 与 Switch1 的部分配置命令。

1.配置核心交换机 Switch-core

```
Switch-core#config terminal
```

```
Switch-core(config)#interface gigabitEthernet 0/2
```

```
Switch-core(config-if)#description wgs-wg0/1 // (5)
```

```
Switch-core(config-if)#no switchport // (6)
```

```
Switch-core(config-if)#ip address (7)
```

```
Switch-core(config-if)#no shutdown
```

```
Switch-core(config)#ip route 192.168.10.0 255.255.255.0
```

```
192.168.101.2
```

```
Switch-core(config)#exit
```

```
...
```

2.配置网管中心交换机 Switch1

```
Switch1#config terminal
```

```
Switch1(config)#no ip domain lookup // ( 8 )
```

```
Switch1(config)#interface gigabitEthernet 0/1
```

```
Switch1(config-if)#description core-g0/2
```

```
Switch1(config-if)#no switchport
```

```
Switch1(config-if)#ip address ( 9 )
```

```
Switch1(config-if)#exit
```

```
Switch1(config)#vlan 10
```

```
Switch1(config-vlan)#name wgl0
```

```
Switch1(config-vlan)#exit
```

```
Switch1(config)#interface vlan 10 //创建 VLAN10
```

```
Switch1(config-if)#ip address ( 10 )
```

```
Switch1(config-if)#exit
```

```
Switch1(config)#interface range f0/2-20
```

```
Switch1(config-if-range)#switchport mode access //设置端口模为  
access 模式
```

```
Switch1(config-if-range)#switchport access ( 11 ) //设置端口所属的
```

VLAN

```
Switch1(config-if-range)#no shutdown
```

```
Switch1(config-if-range)#exit
```

```
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
```

```
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
```

...

- (5) 描述该端口或者给该端口做备注
- (6) 关闭二层交换功能，启用三层路由模式
- (7) 192.168.101.1 255.255.255.0
- (8) 关闭域名解析功能
- (9) 192.168.101.2 255.255.255.0
- (10) 192.168.10.1 255.255.255.0
- (11) VLAN 10

本问题主要考查三层交换机使用静态路由进行路由选择的配置方法。

(1)配置核心交换机 Switch-core

```
Switch-core#config terminal
```

```
Switch-core(config)#interface gigabitEthernet 0/2
```

```
//进入核心交换机三层网络接口
```

```
Switch-core(config-if)#description wgs-wg0/1
```

```
//描述该端口或者给该端口做备注
```

```
Switch-core(config-if)#no switchport //
```

关闭二层交换功能，启用三层路由模式

```
Switch-core(config-if)#ip address 192.168.101.1 255.255.255.0
```

```
//配置三层网络接口的IP地址
```

```
Switch-core(config-if)#no shutdown
```

```
//激活接口
```

```
Switch-core(config)#ip route 192.168.10.0 255.255.255.0
```

```
192.168.101.2
```

```
//配置核心交换机到 192.168.10.0 网段的静态路由
```

```
Switch-core(config)#exit
```

```
...
```

(2)配置网管中心交换机 Switch1

```
Switch1#config terminal
```

```
Switch1(config)#no ip domain lookup
```

```
//关闭域名解析功能
```

```
Switch1(config)#interface gigabitEthernet 0/1
```

```
//进入 gigabitEthernet 0/1 接口
```

```
Switch1(config-if)#description core-g0/2
```

```
//描述该接口
```

```
Switch1(config-if)#no switchport
```

```
//关闭二层交换功能，启用三层路由模式
```

```
Switch1(config-if)#ip address 192.168.101.2 255.255.255.0
```

```
//配置三层网络接口的IP地址和子网掩码
```

```
Switch1(config-if)#exit
```



```
Switch1(config)#vlan 10
Switch1(config-vlan)#name wg10
Switch1(config-vlan)#exit
Switch1(config)#interface vlan 10
//进入 VLAN10 接口
Switch1(config-if)#ip address 192.168.10.1 255.255.255.0
//配置该接口的 IP 地址和子网掩码
Switch1(config-if)#exit
Switch1(config)#interface range f0/2-20
//选择接口范围为 f0/2-20
Switch1(config-if-range)#switchport mode access
//设置端口模式为 access 模式
Switch1(config-if-range)#switchport access vlan 10
//设置端口所属的 VLAN
Switch1(config-if-range)#no shutdown
Switch1(config-if-range)#exit
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
//配置 switch1 到 192.168.20.0 及 192.168.30.0 网段的静态路由
...
```

【问题3】(7分)

为确保研发中心网络的稳定性,在现有条件下尽量保证带宽,要求实现核心交换

机 Switch-core 与研发中心交换机 Switch4 的三层端口聚合，然后通过静态路由进行连接。根据需求，完成或解释以下配置命令。

1.继续配置核心交换机 Switch-core

```
Switch-core#config terminal
```

```
Switch-core(config)#interface port-channel 10 // (12)
```

```
Switch-core(config-if)#no switchport
```

```
Switch-core(config-if)#ip address (13)
```

```
Switch-core(config-if)#no shutdown
```

```
Switch-core(config-if)#exit
```

```
Switch-core(config)#interface range fastEthernet0/1-4 //选择配置的物理接口
```

```
Switch-core(config-if-range)#no switchport
```

```
Switch-core(config-if-range)#no ip address //确保该物理接口没有指定的IP地址
```

```
Switch-core(config-if-range)#switchport //改变该端口为2层接口
```

```
Switch-core(config-if-range)#channel-group 10 mode on // (14)
```

```
Switch-core(config-if-range)#no shutdown
```

```
Switch-core(config-if-range)#exit
```

```
Switch-core(config)#ip route 192.168.40.0 255.255.255.0  
192.168.102.2
```

...

2.配置研发中心交换机 Switch4

```
Switch4#config terminal
Switch4(config)#interface port-channel 10
Switch4(config-if)#no switchport
Switch4(config-if)#ip address ( 15 )
Switch4(config-if)#no shutdown
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/1-4 //选择配置的物理接
□
Switch4(config-if-range)#no switchport
Switch4(config-if-range)#no ip address
...
Switch4(config-if-range)#no shutdown
Switch4(config-if-range)#exit
Switch4(config)# ( 16 ) //配置默认路由
Switch4(config)#vlan 40
Switch4(config-vlan)#name yf10
Switch4(config-vlan)#exit
Switch4(config)# ( 17 ) //开启该交换机的三层路由功能
Switch4(config)#interface vlan 40
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/5-20
```

```
Switch4(config-if-range)#switchport mode access
```

...

```
Switch4(config-if-range)# (18) //退回到特权模式
```

```
Switch4#
```

...

(12) 创建编号为 10 的 port-channel 接口

(13) 192.168.102.1 255.255.255.0

(14) 分配接口并指定 PAgP 模式

(15) 192.168.102.2 255.255.255.0

(16) ip route 0.0.0.0.0.0.0.0 192.168.102.1

(17) ip routing

(18) end 或者 Ctrl+Z

本问题主要考查冗余链路汇聚的相关配置知识。

(1)继续配置核心交换机 Switch-core

```
Switch-core#config terminal
```

```
Switch-core(config)#interface port-channel 10
```

```
//创建编号为 10 的 port-channel 接口
```

```
Switch-core(config-if)#no switchport
```

```
//关闭二层交换功能，启用三层路由模式
```

```
Switch-core(config-if)#ip address 192.168.102.1 255.255.255.0
```

```
//为该接口分配 IP 地址和子网掩码
```

```
Switch-core(config-if)#no shutdown
```

```
Switch-core(config-if)#exit
```

```
Switch-core(config)#interface range fastEthernet0/1-4
```

```
//选择配置的物理接口
```

```
Switch-core(config-if-range)#no switchport
```

```
//关闭二层交换功能，启用三层路由模式
```

```
Switch-core(config-if-range)#no ip address
```

```
//确保该物理接口没有指定的 IP 地址
```

```
Switch-core(config-if-range)#switchport
```

```
//改变该端口为 2 层接口
```

```
Switch-core(config-if-range)#channel-group 10 mode on
```

```
//分配接口并指定为 PAgP 模式
```

```
Switch-core(config-if-range)#no shutdown
```

```
Switch-core(config-if-range)#exit
```

```
Switch-core(config)#ip route 192.168.40.0 255.255.255.0
```

```
192.168.102.2
```

```
//配置核心交换机到 192.168.40.0 网段的静态路由
```

```
...
```

(2)配置研发中心交换机 Switch4

```
Switch4#config terminal
```

```
Switch4(config)#interface port-channel 10
```

```
//创建编号为 10 的 port-channel 接口
```

```
Switch4(config-if)#no switchport
```

```
//关闭二层交换功能，启用三层路由模式

Switch4(config-if)#ip address 192.168.102.2 255.255.255.0

//为该接口分配 IP 地址和子网掩码

Switch4(config-if)#no shutdown

Switch4(config-if)#exit

Switch4(config)#interface range fastEthernet0/1-4

//选择配置的物理接口范围为 f0/1-4

Switch4(config-if-range)#no switchport

//关闭二层交换功能，启用三层路由模式

Switch4(config-if-range)#no ip address

//确保该物理接口没有指定的 ip 地址

...

Switch4(config-if-range)#no shutdown

Switch4(config-if-range)#exit

Switch4(config)# ip route 0.0.0.0 0.0 . 0 . 0 192.168.102.1

//配置默认路由

Switch4(config)#vlan 40

Switch4(config-vlan)#name yf10

Switch4(config-vlan)#exit

Switch4(config)# ip routing

//开启该交换机的三层路由功能

Switch4(config)#interface vlan 40
```



```
//进入 VLAN40 接口
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
//配置该接口的 IP 地址和子网掩码
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/5-20
//选择接口范围为 f0/5-20
Switch4(config-if-rang)#switchport mode access
//设置端口模式为 access 模式
...
Switch4 (config-if-range) #end 或 Ctrl+Z
//在该接口模式下使用 end 或 Ctrl+Z 可直接退回到特权模式
Switch4#
...
```

【问题 4】(2 分)

为了保障局域网用户的网络安全，防范欺骗攻击，以生产部交换机 Switch2 为例，配置 DHCP 侦听。根据需求完成或解释 Switch2 的部分配置命令。

```
Switch2#config terminal
Switch2(config)#ip dhcp snooping // ( 19 )
Switch2(config)#ip dhcp snooping vlan 20
Switch2(config)#interface gigabitEthernet0/24
Switch2(config-if)#ip dhcp snooping trust // ( 20 )
Switch2(config-if)#exit
```

...

(19) 启用 DHCP 探测

(20) g1/1 端口为信任端口

问题主要考查交换机利用 DHCP 探测防范欺骗攻击的相关配置知识。

```
Switch2#config terminal
```

```
Switch2(config)#ip dhcp snooping
```

```
//启用 DHCP 探测
```

```
Switch2(config)#ip dhcp snooping vlan 20
```

```
//指定要实现 DHCP 探测的 VLAN
```

```
Switch2(config)#interface gigabitEthernet1/1
```

```
Switch2(config-if)#ip dhcp snooping trust
```

```
//配置端口信任，g1/1 端口为信任端口
```

```
Switch2(config-if)#exit
```

...