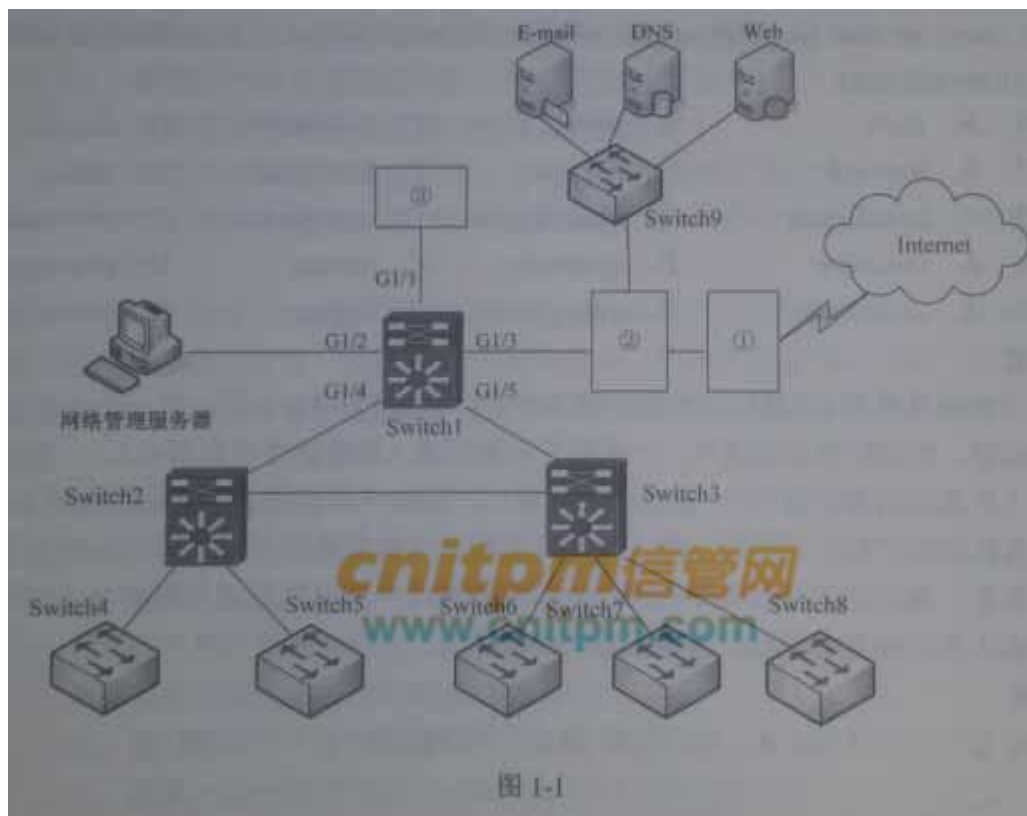


1、试题一

阅读以下说明，根据要求回答下面问题。

[说明]

某企业的网络结构如下图所示。



【问题 1】图中的网络设备①应为（1），网络设备②应为（2），从网络安全角度出发，switch9 所组成的网络一般称为（3）区。

2. 图中③处的网络设备的作用是检测流经内网的信息，提供对网络系统的安全保护。该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。网络设备③应为（4），其连接的 switch1 的 g1/1 端口称为（5）端口，这种连接方式一般称为（6）。

【问题 2】随着企业用户的增加，要求部署上网行为管理设备，对用户的上网行为进行安全分析、流量管理、网络访问控制等，以保证正常的上网需求。部署上网行为管理设备的位置应该在上图中的（7）和（8）之间比较合理。

2. 网卡的工作模式有直接、广播、多播和混杂四种模式，默认的工作模式为（9）和（10），即它只接收广播帧和发给自己的帧。网络管理机在抓包时，需要把网卡置于（11），这时网卡将接受同一子网内所有站点所发送的数据包，这样就可以达到对网络信息监视的目的。

【问题 3】针对上图中的网络结构，各台交换机需要运行（12）协议，以建立一个无环路的树状网络结构。按照该协议，交换机的默认优先级值为（13），根交换机是根据（14）来选择的，值小的交换机为根交换机；如果交换机的优先级相同，再比较（15）。

当上图中的 switch1~switch3 之间的某条链路出现故障时，为了使阻塞端口直接进入转发状态，从而切换到备份链路上，需要在 switch1~switch3 上使用（16）功能。

【问题 4】根据层次化网络的设计原则，从上图中可以看出该企业网络采用了由（17）层和（18）层组成的两层架构。其中，mac 地址过滤和 ip 地址绑定等功能是由（19）完成的，分组的高速转发是由（20）完成的。

信管网参考答案（最终答案以信管网题库为准）：

查看解析：www.cnitpm.com/st/2389720783.html

2、阅读以下说明，根据要求回答下面问题。

[说明]

某中学为两个学生课外兴趣小组提供了建立网站的软硬件环境。网站环境的基本配置方案如下：

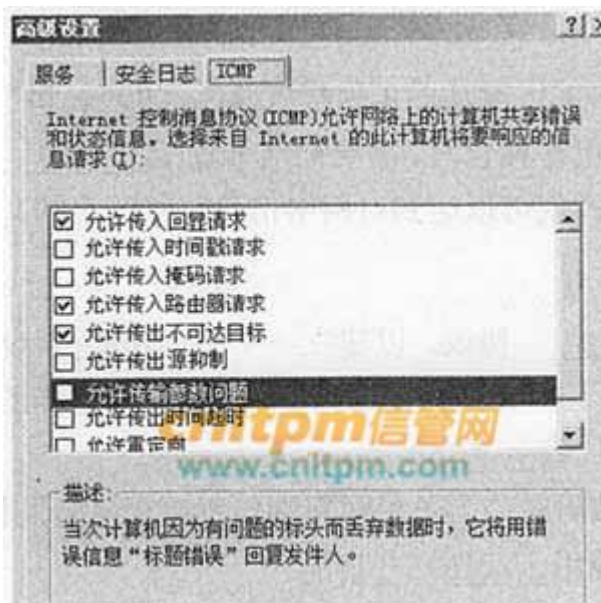
1. 两个网站配置在同一台服务器上，网站服务由 win 2003 环境下的 iis 6.0 提供；
2. 网站的管理通过 win 2003 的远程桌面实现，并启用 win 2003 的防火墙组件；
3. 为兴趣小组建立各自独立的文件夹作为上传目录和网站的主目录，对用户使用磁盘空间大小进行了设定；
4. 通过不同的域名分别访问课外兴趣小组各自的网站。

按照方案，学校的网络工程师安装了 win 2003 服务器，使用 iis6.0 建立 web 及 ftp 服务器，配置了远程桌面管理、防火墙，在服务器上为两个课外兴趣小组分配了不同的用户名，进行了初步的权限配置。

【问题 1】

windows 2003 远程桌面服务的默认端口是（1），对外提供服务使用（2）协议。

在下图中，若要拒绝外部设备 ping 服务器，在防火墙的 icmp 配置界面上应该如何操作？



【问题 2】

在下图中，web 服务扩展选项中“所有未知 cgi 扩展禁止”的含义是什么？

2. 在上图中，如何配置 web 服务扩展，网站才能提供对 asp.net 或 asp 程序的支持。

【问题 3】

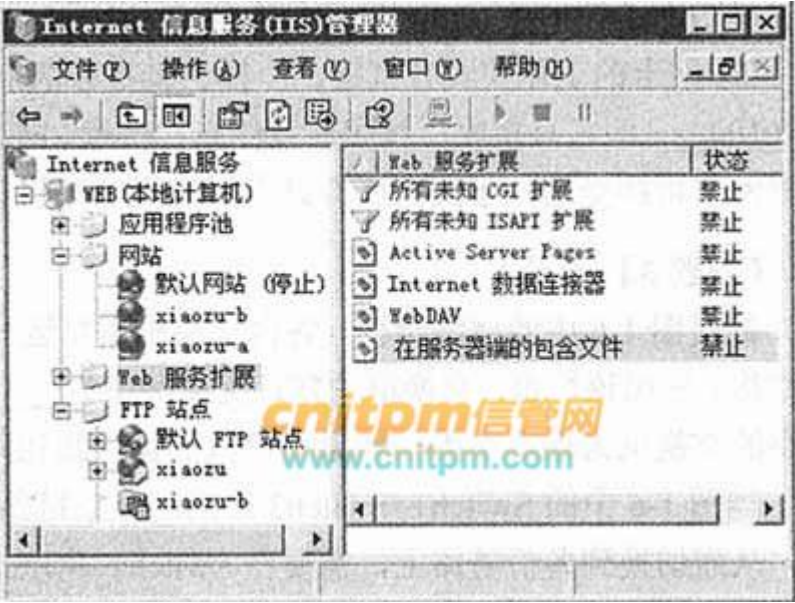
在上图中，选择 iis 管理器中的“ftp 站点→新建→虚拟目录”，分别设置 ftp 用户与（3）、（4）的对应关系。由于 iis 内置的 ftp 服务不支持（5），因此 ftp 用户密码是以明文方式在网络上传输，安全性较弱。

【问题 4】

在 iis 6.0 中，每个 web 站点都具有唯一的、由三部分组成的标识符，用来接收和响应请求，分别是（6）、（7）和（8）。网络工程师通过单击网站属性→网站→高级选项，通过添加（9）的方式在一个 ip 地址上建立多个网站。

【问题 5】

在（10）文件系统下，为了预防用户无限制的使用磁盘空间可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是（11）和（12）。

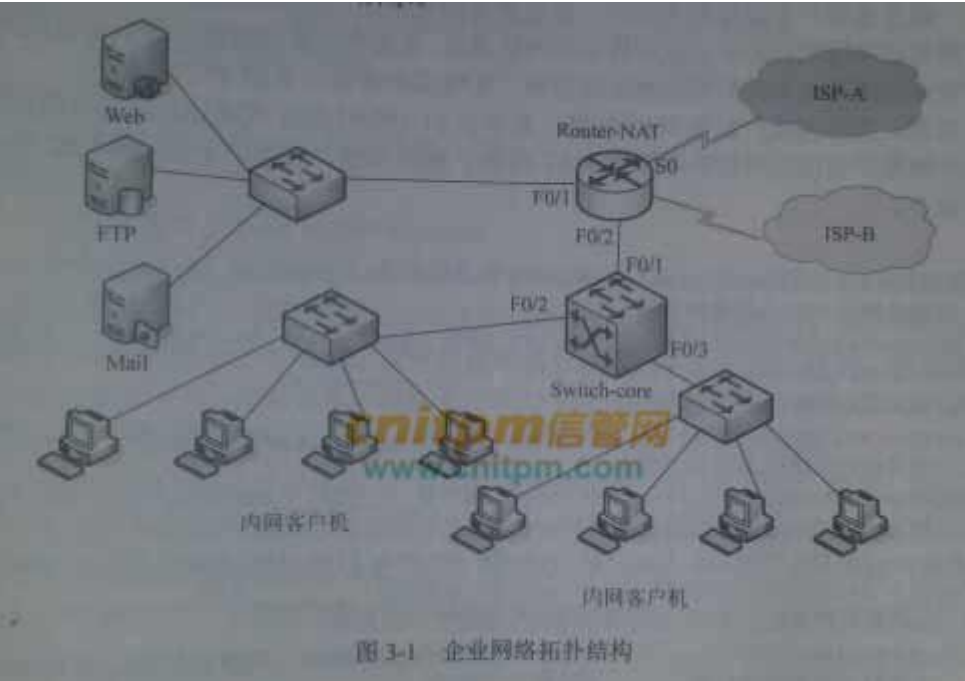


信管网参考答案（最终答案以信管网题库为准）：
查看解析：www.cnitpm.com/st/2389817838.html

3、阅读以下说明，根据要求回答下面问题。

[说明]

某企业的网络结构如下图所示。



按照网络拓扑结构为企业网络进行网络地址配置，地址分配如下表所示。

某企业网络地址分配表	
设备	地址
Router-NAT	F0/1: 192.168.1.1/24 S0: 61.192.93.100/24 S1: 202.102.100.100/24
Web服务器	192.168.1.100
ISP-A	61.192.93.200/24
ISP-B	202.102.100.200/24
ISP-A地址池	61.192.93.100~61.192.93.102
ISP-B地址池	202.102.100.100~202.102.100.102

【问题 1】

企业网络中使用私有地址，如果内网用户要访问互联网，一般使用（1）技术将私有网路地址转换为公网地址。在使用该技术时，往往是用（2）技术指定允许转换的内部主机地址范围。

一般来说，企业内服务器需要被外部用户访问，就必须对其做地址变换，内部服务器映射的公共地址不能随意更换，需要使用（3）nat 技术。但是对于企业内部用户来讲，使用一一映射的技术为每个员工配置一个地址很不现实，一般使用（4）nat 技术以提高管理效率。

【问题 2】

一般企业用户可能存在于任何一家运营商的网络中，为了确保每个运营商网络中的客户都可以高效地访问本企业所提供的网络服务，企业有必要同时接入多个运营商网络。根据企业网络的拓扑图和网络地址规划表，实现该企业出口的双线接入。

首先，为内网用户配置 nat 转换，其中以 61.192.93.0/24 代表 isp-a 所有网段；其次为外网用户访问内网服务器配置 nat 转换。根据需求，完成以下 route-nat 的有关配置命令。

```
route-switch (config) #access-list 100 permit ip any 61.192.93.0 0.0.0.255
```

```
//定义到达 isp-a 所有网段的 acl
```

```
route-switch (config) #access-list 101 (5) ip any 61.192.93.0 0.0.0.255
```

```
route-switch (config) #access-list 101 (6)
```

```
//定义到达 isp-b 所有网段的 acl
```

```
route-switch (config) #ip nat pool isp-a (7) netmask 255.255.255.0
```

```
//定义访问 isp-a 的合法地址池
```

```
route-switch (config) #ip nat pool isp-b (8) netmask 255.255.255.0
```

```
//定义访问 isp-b 的合法地址池
```

```
route-switch (config) #ip nat inside source list100 pool isp-a overload
```

```
route-switch (config) #ip nat inside source (9)
```

```
//为内网用户实现区分目标运营商网络进行匹配的 nat 转换
```

```
route-switch (config) #ip nat inside source static tcp (10) extendable
```

```
//为内网 web 服务器配置 isp-a 的静态 nat 转换
```

```
route-switch (config) #ip nat inside source static tcp (11) extendable
```

```
//为内网 web 服务器配置 isp-b 的静态 nat 转换
```

【问题 3】

在路由器的内部和外部接口启用 nat，同时为了确保内网可以访问外部网络，在出口设备配置静态路由。根据需求，完成(或解释)route-nat 的部分配置命令。

```
route-switch (config) #int s0
```

```
route-switch (config) # (12) //指定 nat 的外部转换接口
```

```
route-switch (config) #int s1
```

```
route-switch (config) # (13) //指定 nat 的外部转换接口
```

```
route-switch (config) #int f0/1
```



```
route-switch (config) # (14)          //指定 nat 的内部转换接口
route-switch (config) # (15)          //配置到达 isp-a 的流量从 s0 口转发
route-switch (config) # (16)          //配置默认路由指定从 s1 口转发
route-switch (config) #ip route 0.0.0.0 0.0.0.0 s0 120      //(17)
```

常用的网络流量控制技术除了 acl（访问控制列表）外还有 qos（服务质量）。qos 是网络的一种安全机制，主要用来解决网络延迟和阻塞等问题，它主要有三种工作模式，分别为（18）模型、integrated service（或集成服务）模型及（19）模型，其中使用比较普遍的方式是（20）模型。

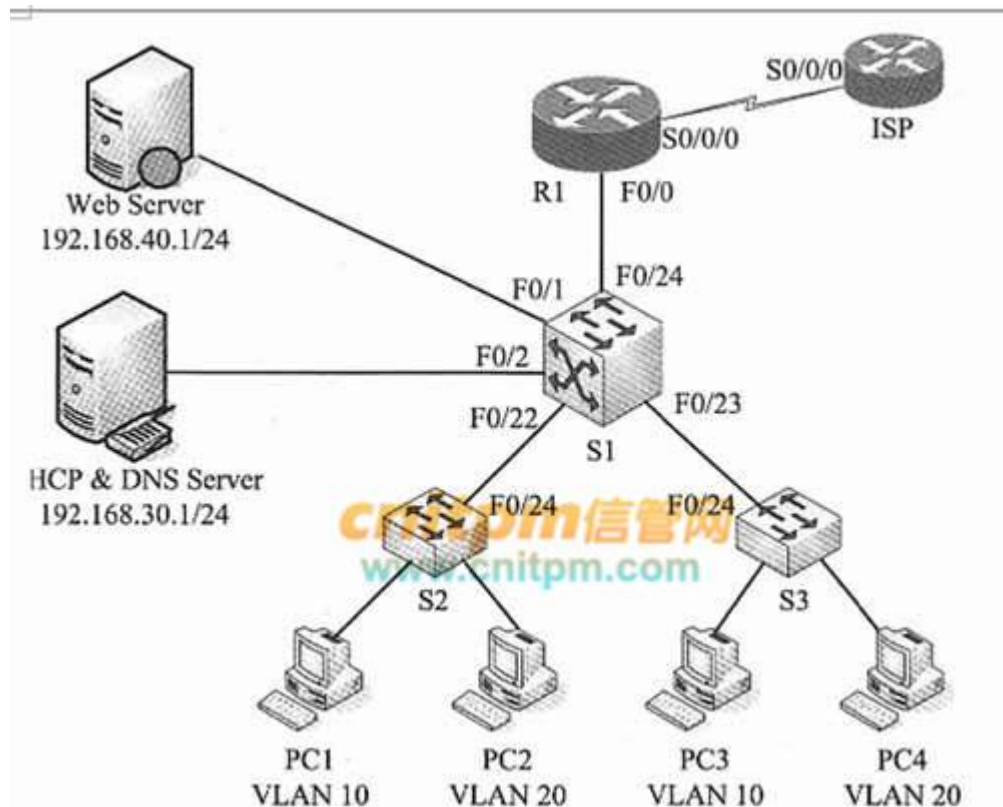
信管网参考答案（最终答案以信管网题库为准）：

查看解析：www.cnitpm.com/st/2389913040.html

4、阅读以下说明，根据要求回答下面问题。

[说明]

某公司网络拓扑结构如下图所示。公司内部使用 c 类私有 ip 地址，其中公司两个部门分别处于 vlan10 和 vlan20，vlan10 采用 192.168.10.0/24 网段，vlan20 采用 192.168.20.0/24 网段，每段最后一个地址作为网关地址。



【问题 1】公司使用 vtp 协议规划 vlan，三层交换机 s1 为 vtp sever，其他交换机为 vtp client，并通过 s1 实现 vlan 间通信。请根据网络拓扑和需求说明，完成交换机 s1 和 s2 的配置。

```
s1>enable
s1#configure terminal
s1 (config) #vtp mode (1)
s1 (config) #vtp domain shx
s1 (config) #vtp password shx
s1 (config) #vlan 10
s1 (config-vlan) #exit
s1 (config) #vlan 20
s1 (config-vlan) #exit
```

```
s1 (config) #interface vlan 10
s1 (config-if) #ip address (2) (3)
s1 (config-if) #exit
s1 (config) #interface vlan 20
s1 (config-if) #ip address 192.168.20.254 255.255.255.0
s1 (config-if) #exit
s1 (config) #intetrace (4) fastethernet 0/22-23
s1 (config-if-range) #switchport mode access
s1 (config-if-range) #switchporm mode (5)
s1 (config-if-range) #exit
s1 (config) #interface fastethernet 0/1
s1 (config-if) # (6) //关闭二层功能
s1 (config-if) #ip add 192.168.40.254 255.255.255.0
s1 (config-if) #exit
.....
s1 (config) # (7) (8) //开启路由功能
s1 (config) #
s2>enable
s2#configure terminal
s2 (config) #vtp mode (9)
s2 (config) #vtp domain shx
s2 (config) #vtp password shx
s2 (config) #intererce fastethernet 0/24
s2 (config-if) #switchport mode (10) //设定接口模式
s2 (config-if) #end
s2#
```

【问题 2】

公司申请了 202.165.200.0/29 地址段，使用 nat-pt 为用户提供 internet 访问，外部全局地址为 202.165.200.1，web 服务器使用的外部映射地址为 202.165.200.3。请根据网络拓扑和需求说明，完成路由器 r1 的配置。

```
r1>enable
r1#config terminal
r1 (config) #access-list 1 (11) 192.168.10.0 255.255.255.0
r1 (config) #interface serial 0/0/0
r1 (config-if) #ip address 202.165.200.1 255.255.255.248
r1 (config-if) #no shutdown
r1 (config-if) #clock rate 4000000
r1 (config-if) #ip address 192.168.50.254 255.255.255.0
r1 (config-if) #no shutdown
r1 (config-if) #exit
r1 (config) #ip nat inside source (12) 1 interface s0/0/0 overload
r1 (config) #ip nat inside source static (13) 202.165.200.3
r1 (config) #interface fastethernet 0/0
r1 (config-if) #ip nat (14)
r1 (config-if) #interface serial 0/0/0
r1 (config-if) #ip nat (15)
r1 (config-if) #end
```

rl#

信管网参考答案（最终答案以信管网题库为准）：

查看解析：www.cnitpm.com/st/23900656.html