2015 年下半年 网络工程师 下午试卷答案解析

试题一

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】

某工业园区视频监控网络拓扑如图 1-1 所示。

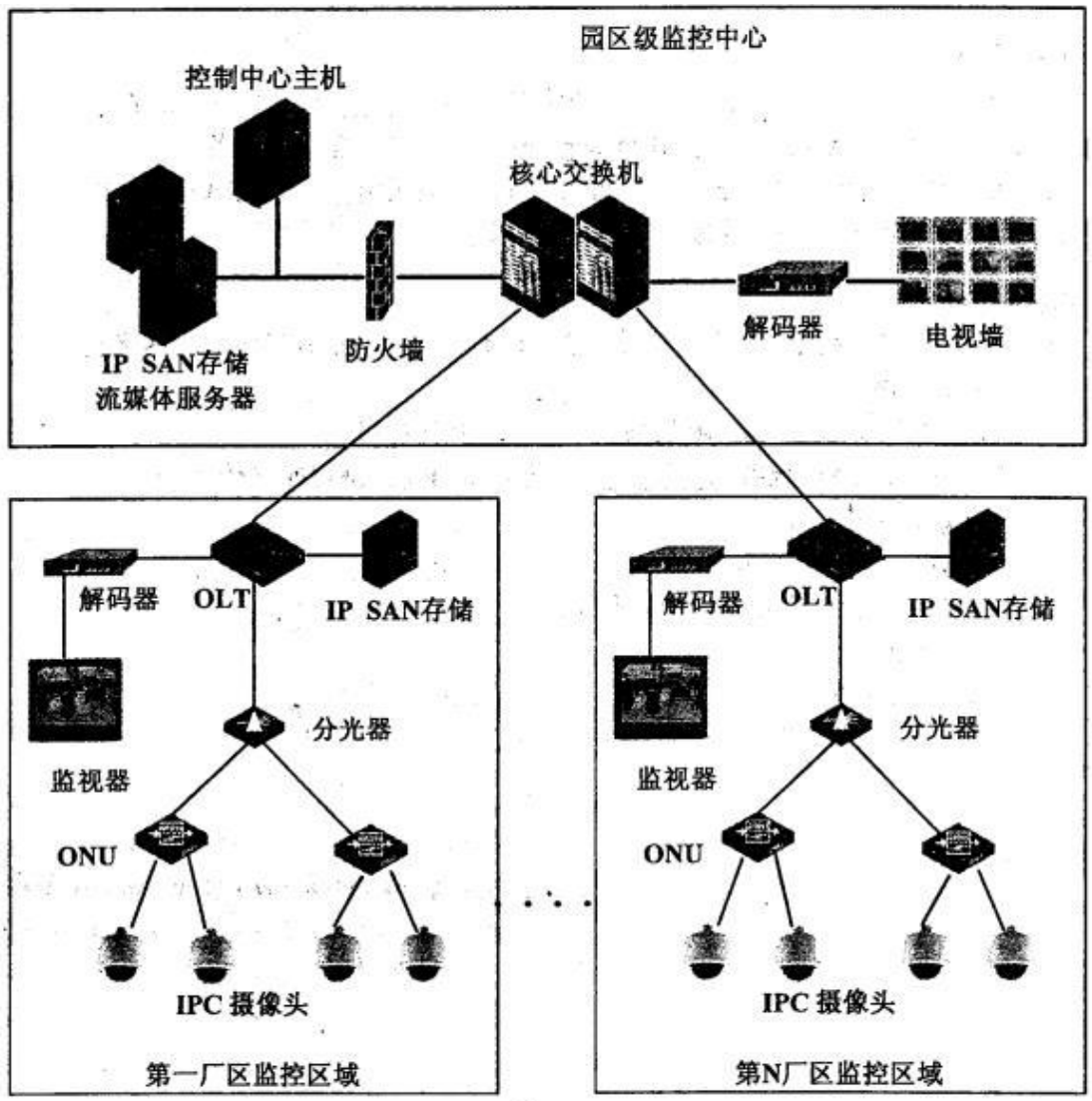

图 1-1

【问题 1】（4 分）

图 1-1 中使用了 SAN 存储系统，SAN 是一种连接存储管理子系统和（1）的专用网络。SAN 分为 FC SAN 和 IP SAN，其中 FC SAN 采用（2）互联；

IP SAN 采用 （3） 互联；SAN 可以被看作是数据传输的后端网络，而前端网络则负责正常的 （4） 传输。

（1）~（4）备选答案：

A. iSCSI　　B. TCP/IP　　C. 以太网技术　　D. SATA

E. 文件服务器　　F. 光纤通道技术　　G. 视频管理子系统　　H. 存储设备

（1）H

（2）F

（3）C

（4）B

本题通过视频监控网络的组网环境，考查 EPON 的特点与组网的相关知识。

此类题目要求考生熟悉网络系统的优化、网络存储和组网的基本技术，并且在工程实践中灵活运用。

SAN (Storage Area Network)存储区域网络，是一种高速的、专门用于存储操作的网络，通常独立于计算机局域网（LAN)。SAN 将主机和存储设备连接在一起，能够为其上的任意一台主机和任意一台存储设备提供专用的通信通道。SAN 将存储设备从服务器中独立出来，实现了服务器层次上的存储资源共享。SAN 将通道技术和网络技术引入存储环境中，提供了一种新型的网络存储解决方案，能够同时满足吞吐率、可用性、可靠性、可扩展性和可管理性等方面的要求。

SAN 分为 FCSAN 和[PSAN，其中 FC SAN 采用光纤通道技术互联；IP SAN 采用以太网技术互联；SAN 可以被看作是数据传输的后端网络，而前端网络则

负责正常的 TCP/IP 传输。

【问题 2】(4 分)

该网络拓扑是基于 EPON 的技术组网，与传统的基于光纤收发器的组网有所不同。请从组网结构复杂度、设备占用空间大小、设备投资多少、网络管理维护难易程度等几方面对两种网络进行比较。

对比内容	光纤收发器	EPON
组网结构	复杂	简单
占用空间	较多	较少
设备投资	较多	较少
管理维护	复杂	简单

EPON (Ethernet Passive Optical Network,以太网无源光网络）源于以太网的 PON 技术。它采用点到多点结构、无源光纤传输，在以太网之上提供多种业务。综合了 PON 技术和以太网技术的优点：低成本、高带宽、扩展性强、与现有以太网兼容、方便管理等。

光纤收发器，是一种将短距离的双绞线电信号和长距离的光信号进行互换的以太网传输媒体转换单元。一般应用在以太网电缆无法覆盖、必须使用光纤来延长传输距离的实际网络环境中，且通常定位于宽带城域网的接入层应用，成对使用。

【问题 3】(6 分)

1. 该系统采用 VLAN 来隔离各工厂和监控点，在 （5） 端进行 VLAN 配置，在（6）端采用 trunk 进行 VLAN 汇聚，使用 Manage VLAN 统一管理 OLT 设备。

2. OLT 的 IP 地址主要用于设备的网元管理，一般采用 （7） 方式分配，IPC 摄像机的地址需要统一规划，各厂区划分为不同的地址段。

5）ONU

（6）OLT

（7）静态或制定

在 ONU 设备上配置 VLAN 用户和业务，在 OLT 设备上将相同的 VLAN 配置在同 一个逻辑通道中。IP 地址的分配分为动态或静态，OLT 的地址用于设备的管理，应采用静态方式。

【问题 4】（6 分）

1. 在视频监控网络中，当多个监控中心同时查看一个点的视频时要求网络支持（8） 。

（8）备选答案：A. IP 广播　　B. IP 组播　　C. IP 任意播

2. 在组网时，ONU 设备的 （9） 接口通过 UTP 网线和 IPC 摄像机连接。

（9）备选答案：A. BNC　　B. RJ45　　C. USB

3. 该网络的网管解决方案中一般不包含 （10） 功能或组件。

（10）备选答案：A. 网元管理　　B. 防病毒模块　　C. EPON 系统管理　　D. 事件、告警管理

（8）B

（9）B

（10）B

TCP/IP 传输方式有 3 种：单播、广播、组播。单播在发送和每个接收主机之间需要单独的数据信道，如果有多个主机希望获得数据包的同一份拷贝将导致发送端负担沉重、延迟长、网络拥塞。组播是允许一个或多个主机发送一个数据包到多个主机的网络技术。组播源把数据包发送到特定组播组，只有属于该组播组地

址的主机才能接收到数据包。 广播是指在 IP 子网内广播数据包，所有在子网内部的主机都将收到这些数据包。

UTP 网线由一定长度的双绞线和 RJ-45 水晶头组成。双绞线由 8 根不同颜色的线分成 4 对绞合在一起，成对扭绞的作用是尽可能减少电磁辐射与外部电磁干扰的影响。

防病毒模块属于网络安全防护的范畴，随着网络病毒特征的变化需要不断地升级病毒库。该模块与具体的网络设备的配置管理、运行维护和故障监控之间密切度不高， 一般不作为特定网络管理解决方案的组成部分。

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】

某企业的网络结构如图 2-1 所示。

该企业通过一台路由器接入到互联网，企业内部按照功能的不同分为 6 个 VLAN。分别是网络设备与网管（VLAN1）、内部服务器（VLAN2）、Internet 连接（VLAN3）、财务部（VLAN4）、市场部（VLAN5）、研发部门（VLAN6）。

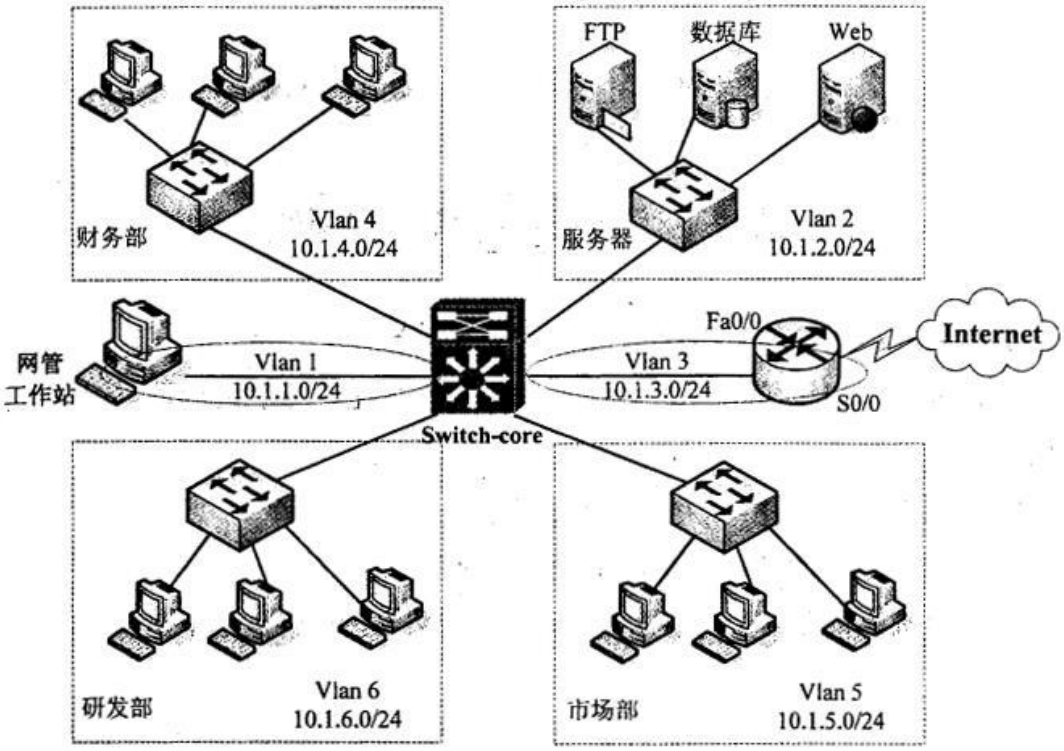

图 2-1 某企业网络拓扑图

【问题 1】(7 分)

1. 访问控制列表 ACL 是控制网络访问的基本手段，它可以限制网络流量，提高网络性能。ACL 使用（1）技术来达到访问控制目的。 ACL 分为标准 ACL 和扩展 ACL 两种，标准访问控制列表的编号为 （2） 和 1300～1999 之间的数字，标准访问控制列表只使用（3）进行过滤，扩展的 ACL 的编号使用（4）以及 2000～2699 之间的数字。

2. 每一个正确的访问列表都至少应该有一条 （5） 语句，具有严格限制条件的语句应放在访问列表所有语句的最上面，在靠近 （6） 的网络接口上设置扩展 ACL，在靠近 （7） 的网络接口上设置标准 ACL。

（1）对数据包进行过滤

（2）1-99

（3）源地址

（4）100-199

（5）允许

（6）出口（数据源地址）

（7）入口（数据目的地址）

本题考查网络层访问权限控制技术 ACL 的使用配置。

此类题目要求考生不但具有较高的网络配置理论水平，而且必须具备较强的动手配置能力。

本问题主要考查考生对 ACL 基本概念的掌握和应用。

信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，为了保证内网的安全性，需要通过安全策略来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。访问控制列表（Access Control List, ACL）是路由器和交换机接口的指令列表，用来控制端口进出的数据包。配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。如可以配置 ACL,禁止局域网内的设备访问外部公共网络，或者只能使用 FTP 服务。

ACL 使用包过滤技术，在路由器上读取第 3 层及第 4 层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 分为标准 ACL 和扩展 ACL 两种，标准访问控制列表的编号为 1～99 和 1300～1999 之间的数字，标准访问控制列表只使用源地址进行过滤，扩展的 ACL 的编号使用 100～199 以及 2000～2699 之间的数字。在实施 ACL 的过程中，应当遵循如下两个基本原则：最小特权原则，只给受控对象完成任务所必须的最小的权限；最靠近受控对象原则，所有的网络层访问权

限控制每一个正确的访问列表都至少应该有一条允许语句，具有严格限制条件的语句应放在访问列表所有语句的最上面，在靠近源地址的网络接口上设置扩展ACL，在靠近目的地址的 网络接口上设置标准 ACL。

【问题 2】（5 分）

网管要求除了主机 10.1.6.66 能够进行远程 telnet 到核心设备外，其它用户都不允许进行 tehet 操作。同时只对员工开放 Web 服务器（10.1.2.20）、FTP 服务器（10.1.2.22）和数据库服务器（10.1.2.21:1521），研发部除 IP 为 10.1.6.33 的计算机外，都不能访问数据库服务器，按照要求补充完成以下配置命令。

```
…
Switch-core#conf t
Switch-core(config)#access-list 1 permit host __(8)__
Switch-core(config)#line __(9)__ 0 4
Switch-core(config-line)#access-class 1 __(10)__
…
Switch-core(config)#ip access-list extend server-protect
Switch-core(config-ext-nacl)#permit tcp host __(11)__ host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#deny tcp __(12)__ 0.0.0.255 host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.20 eq www
Switch-core(config-ext-nacl)#permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.22 eq ftp
…
```

（8）10.1.6.66

（9）vty

（10）in

（11）10.1.6.33

（12）10.1.6.0

本问题主要考查考生对 ACL 基本配置命令的掌握和应用。

```
…
Switch-core#conf t
//进入全局配置模式
Switch-core(config)#access-list 1 permit host 10.1.6.66
//配置标准 acl1 允许源地址为 10.1.6.66 的包通过
Switch-core(config)#line vty 0 4
//进入 VTY 端口，对 VTY 端口进行配置
Switch-core(config-line)#access-class 1 in
//只允许 acl1 进入
…
Switch-core(config)#ip access-list extend server-protect
//定义扩展 ACL server-protect
Switch-core(config-ext-nacl)#permit tcp host 10.1.6.33 host 10.1.2.21 eq
1521
//允许主机 10.1.6.33 访问 10.1.2.21 的 1521 端口
Switch-core(config-ext-nacl)#deny tcp 10.1.6.0  0.0.0.255 host 10.1.2.21
eq 1521
//不允许 10.1.6.0 子网主机访问 10.1.2.21 的 1521 端口
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.21 eq 1521
//允许 10.1.0.0 子网的主机访问 10.1.2.21 的 1521 端口
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.20 eq www
//允许 10.1.0.0 子网的主机访问 10.1.2.20 的 www 端口
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.22 eq ftp
//允许 10.1.0.0 子网的主机访问 10.1.2.22 的 ftp 端口
…
```

【问题 3】（4 分）

该企业要求在上班时间内（9:00-18:00）禁止内部员工浏览网页（TCP 80 和 TCP 443 端口），禁止使用 QQ（TCP/UDP 8000 端口以及 UDP 4000）和 MSN（TCP 1863 端口）。另外在 2015 年 6 月 1 日到 2 日的所有时间内都不允许进行上述操作。除过上述限制外。在任何时间都允许以其它方式访问 Internet。为了防止利用代理服务访问外网，要求对常用的代理服务端口 TCP 8080、TCP 3128 和 TCP 1080 也进行限制。按照要求补充完成（或解释）以下配置命令。

```
…
Switch-core(config)#time-range TR1
Switch-core(config-time-range)#absolute start 00:00 1 June 2015 end 00:00 3 June 2015
Switch-core(config-time-range)#periodic weekdays start __(13)__
Switch-core(config-time-range)#exit
…
Switch-core(config)#ip access-list extend internet_limit
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 80 time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 443 time-range TR1
//__(14)__
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1863 time-range TR1
//__(15)__
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8000 time-range TR1
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 8000 time-range TR1
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 4000 time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 3128 time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8080 time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1080 time-range TR1
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int__(16)__
Switch-core(config-if)#ip access-group internet_limit out
…
```

（13）9:00 18:00

（14）禁止以安全方式浏览网页

（15）禁止使用 MSN

（16）VLAN3

本问题主要考查考生使用 ACL 技术对网络访问进行精细化控制的能力。

```
…
Switch-core(config)#time-range TR1
//定义一个新的时间范围 TR1
Switch-core(config-time-range)#absolute start 00:00 1 June 2015 end 00:00
3 June 2015
//绝对时间范围为 2015 年 6 月 1 日到 2 日
Switch-core(config-time-range)#periodic weekdays start 9:00 18:00
//定义周期性重复使用的时间范围周一至周五 9:00-18:00
Switch-core(config-time-range)#exit
…
Switch-core(config)#ip access-list extend internet_limit
//定义扩展 ACL internet_limit
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 80
time-range TR1
//禁止以 http 浏览网页
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 443
time-range TR1
//禁止以安全方式浏览网页
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1863
time-range TR1
//禁止使用 MSN
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
//禁止使用 QQ
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
//禁止使用 QQ
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 4000
time-range TR1
//禁止使用 QQ
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 3128
time-range TR1
//禁止使用代理端口 3128
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8080
time-range TR1
//禁止使用代理端口 8080
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1080
time-range TR1
//禁止使用代理端口 1080
Switch-core(config-ext-nacl)#permit ip any any
//允许所有数据通过
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int s0/0
//进入端口 s0/0 配置子模式
Switch-core(config-if)#ip access-group internet_limit out
//将 ACL internet_limit 应用在 s0/0 出口上
…
```

【问题 4】（4 分）

企业要求市场和研发部门不能访问财务部 Vlan 中的数据，但是财务部门做为公司的核心管理部门，又必须能访问到市场和研发部门 Vlan 内的数据。按照要求补充完成（或解释）以下配置命令。

```
…
Switch-core(config)#ip access-list extend fi-main
Switch-core(config-ext-nacl)#permit tcp any 10.1.0.0 0.0.255.255 reflect r-main timeout 120
Switch-core(config-ext-nacl)#permit udp any 10.1.0.0 0.0.255.255 reflect r-main timeout 200
Switch-core(config-ext-nacl)#permit icmp any 10.1.0.0 0.0.255.255 reflect r-main timeout 10
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int __(17)__
Switch-core(config-if)#ip access-group fi-main in
…
Switch-core(config)#ip access-list extend fi-access-limit
Switch-core(config-ext-nacl)#evaluate r-main
Switch-core(config-ext-nacl)#deny ip any __(18)__
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int __(19)__
Switch-core(config-if)#ip access-group fi-access-limit in
Switch-core(config-if)#int __(20)__
Switch-core(config-if)#ip access-group fi-access-limit in
```

（17）vlan4

（18）10.1.4.0 0.0.0.255

（19）vlan5

（20）vlan6

注：（19）（20）答案可互换

本问题主要考查考生使用 IP ACL 实现单向访问控制的命令。

```
...
Switch-core(config)#ip access-list extend fi-main
//定义扩展 ACL fi-main
Switch-core(config-ext-nacl)#permit tcp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 120
//允许 tcp 流量，建立自反访问控制列表 r-main，没有流量的情况下 120 秒消失
Switch-core(config-ext-nacl)#permit udp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 200
//允许 udp 流量，建立自反访问控制列表 r-main，没有流量的情况下 200 秒消失
Switch-core(config-ext-nacl)#permit icmp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 10
//允许 icmp 流量，建立自反访问控制列表 r-main，没有流量的情况下 10 秒消失
Switch-core(config-ext-nacl)#permit ip any any
//允许所有流量通过
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int vlan 4
//进入 VLAN4 子接口配置模式
Switch-core(config-if)#ip access-group fi-main in
//把 acl fi-main 应用在入口
...
Switch-core(config)#ip access-list extend fi-access-limit
//定义扩展 ACL fi-access-limit
Switch-core(config-ext-nacl)#evaluate r-main
//有符合 r-main 这个 reflect 组中所定义的 acl 条目的流量发生时，在 evaluate 语句所
在的当前位置动态生成一条反向的 permit 语句
Switch-core(config-ext-nacl)#deny ip any 10.1.4.0 0.0.0.255
//禁止访问 10.1.4.0 网段
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int vlan 5
//进入 VLAN5 子接口配置模式
Switch-core(config-if)#ip access-group fi-access-limit in
//把 acl fi-access-limit 应用在入口
Switch-core(config-if)#int vlan 6
//进入 VLAN6 子接口配置模式

Switch-core(config-if)#ip access-group fi-access-limit in
//把 acl fi-access-limit 应用在入口
```

试题三

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】

某企业采用 Windows Server 2003 配置了 Web、FTP 和邮件服务。

【问题 1】(4 分)

Web 的配置如图 3-1 和图 3-2 所示。

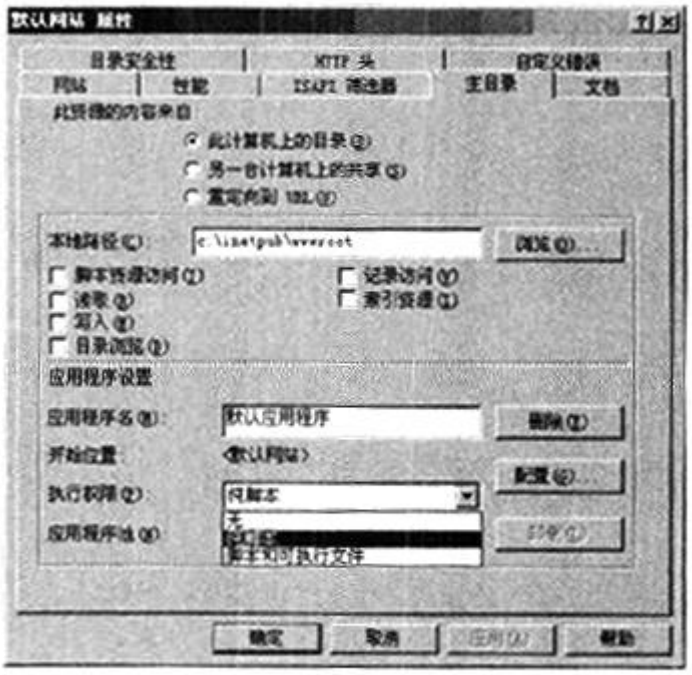

图 3-1

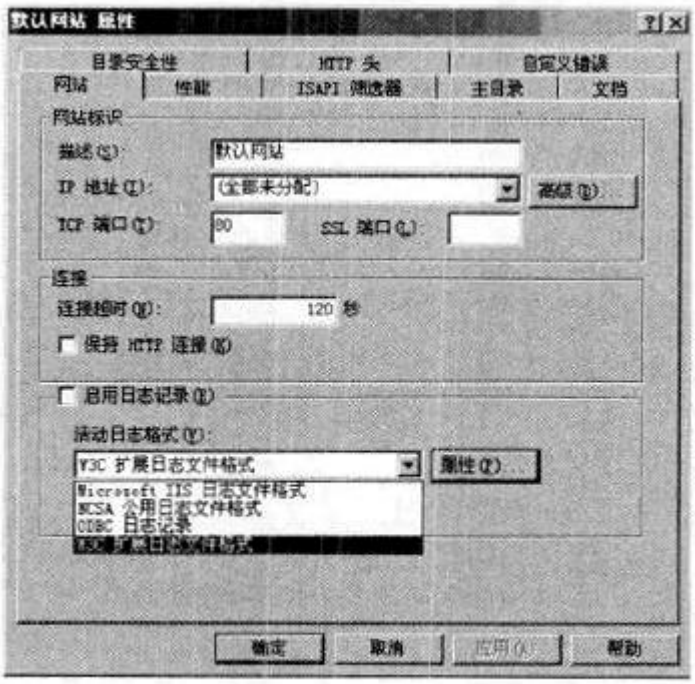

图 3-2

1. 如果要记录用户访问历史，需（1）。

（1）备选答案

A. 同时勾选图 3-1 中“写入”复选框和图 3-2 中“启用日志记录”复选框

B. 同时勾选图 3-1 中“记录访问”复选框和图 3-2 中“启用日志记录”复选框

C. 同时勾选图 3-1 中“记录访问”复选框和“索引资源”复选框

D. 同时勾选图 3-1 中“记录访问”复选框和图 3-2 中“保持 HTTP 连接”复选框

2. 在图 3-2 所示的 4 种活动日志格式中，需要提供用户名和密码的是（2）。

（1）B

（2）ODBC 日志记录

IIS 是微软推出的架设 WEB、FTP、SMTP 服务器的一整套系统组件，集成在

NT 核心的服务器系统中。本题考查 Windows 环境下 Web 服务、FTP 服务及邮件服务的安装与配置。

此类题目要求考生熟悉 Windows 环境提供的网络服务。了解安装网络服务时相关参数设置的含义和配置目的。

在对 Web 的配置时，“默认网站属性”页面是配置网站的主要页面。本题“记录用户访问历史”的作用是获得（IIS)日志记录，该记录可提供比 Windows Server 2003 的事件日志记录或性能监视功能更详细的信息。IIS 日志包括以下信息：访问网站的用户、 他们查看的内容以及最后一次查看信息的时间等内容。需要注意的是必须同时选中“网站” 选项卡上的“启用日志记录”和“主目录”选项卡上的“记录访问”才能启用日志记录。

如果选择了“ODBC 日志记录”，请单击“属性”，并提供 ODBC 数据源名称(DSN)、 表、用户名和密码，然后单击“确定”。

【问题 2】(4 分)

根据图 3-1 判断正误。(正确的答“对”，错误的答“错”)

A. 勾选“读取”是指禁止客户下载网页文件及其他文件。 (3)

B. 不勾选“写入”是指禁止客户以 HTTP 方式向服务器写入信息。(4)

C. 勾选“目录浏览”是指当客户请求的文件不存在时，将显示服务器上的文件列表。(5)

D. 当网页文件是 CGI 文件时，“执行权限”中选择“纯脚本”。(6)

(3)错

(4)对

(5)对

（6）错

IIS Web 服务器的权限设置有两个方面，一个是 NTFS 文件系统本身的权限设置，另一个是“默认网站属性”页面的“主目录”选项卡的设置。在“主目录”选项卡中选中“读取”、“写入”、“目录浏览”等设置都代表“允许”的含义。在“执行权限”的选项中，网页文件是 CGI 文件时，需要选择“纯脚本和可执行程序”。

【问题 3】（6 分）

FTP 的配置如图 3-3 所示。

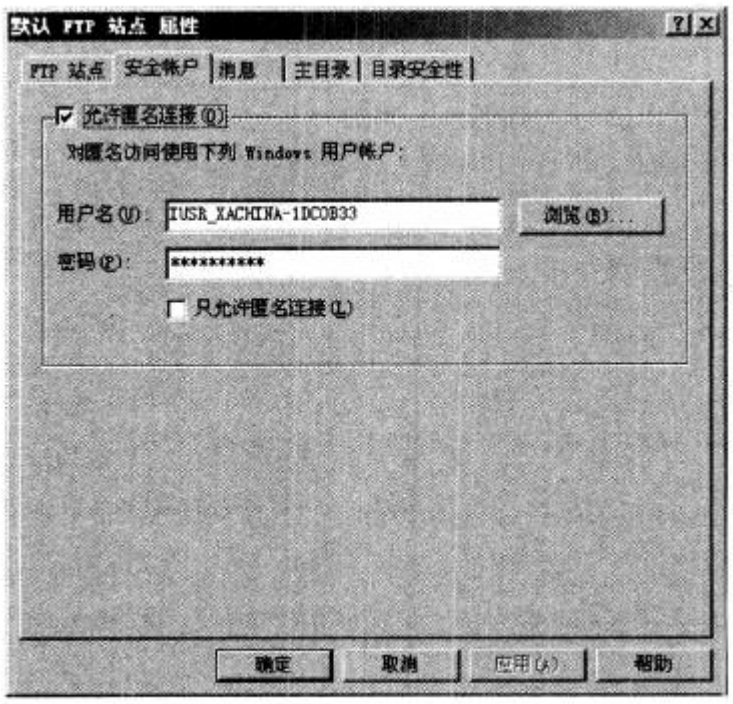

图 3-3

匿名用户的权限与在“本地用户和组”的权限（7），FTP 可以设置（8）虚拟目录。FTP 服务器可以通过 （9） 访问。

（9）备选答案：

A. DOS、客户端方式

B．客户端、浏览器方式

C．DOS、浏览器、客户端方式

（7）相同

（8）多个

（9）C

在进行 FTP 的设置时，匿名用户使用的用户名和密码都来自“本地用户和组”，并且与“本地用户和组”中的权限一致。FTP 可以设置多个虚拟目录为不同的用户提供服务。FTP 可以通过命令行、浏览器、客户端方式访问。

【问题 4】（6 分）

邮件服务器的配置如图 3-4 所示。

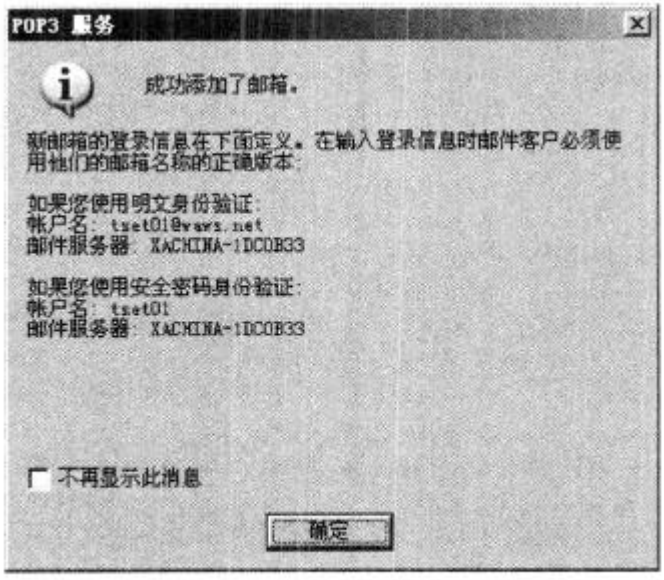

图 3-4

若图 3-4 所示 waws.net 域已经在 Internet 上注册，那么在 DNS 服务器中应配置邮件服务器的 （10） 记录。POP3 是 （11） 邮件协议，配置 POP3 服务器的步骤包含 （12） （多选）。

（11）备选答案：

A．接收　　B．发送　　C．存储　　D．转发

（12）备选答案：

A．创建邮件域　　B．设置服务器最大连接数

C．安装 POP3 组件　　D．添加邮箱

（10）MX

（11）A

（12）A、C、D

MX (Mail Exchanger)记录是邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。例如，当 Internet 上的某用户要发一封信给 user@mydomain.com 时，该用户的邮件系统通过 DNS 查找 mydomain.com 这个域名的 MX 记录，如果 MX 记录存在，用户计算机就将邮件发送到 MX 记录所指定的邮件服务器上。

POP 是一种电子邮件传输协议，3 代表该协议第 3 个版本，规定了怎样将个人计算机连接到 Internet 邮件服务器和下载电子邮件的电子协议。配置 POP 包括安装组件、创建域、添加邮件等内容。“设置服务器最大连接数”是配置 SMTP 服务时配置的参数。

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】

某公司网络拓扑结构图如图 4-1 所示。公司内部的用户使用私有地址段 192.168.1.0/24 。

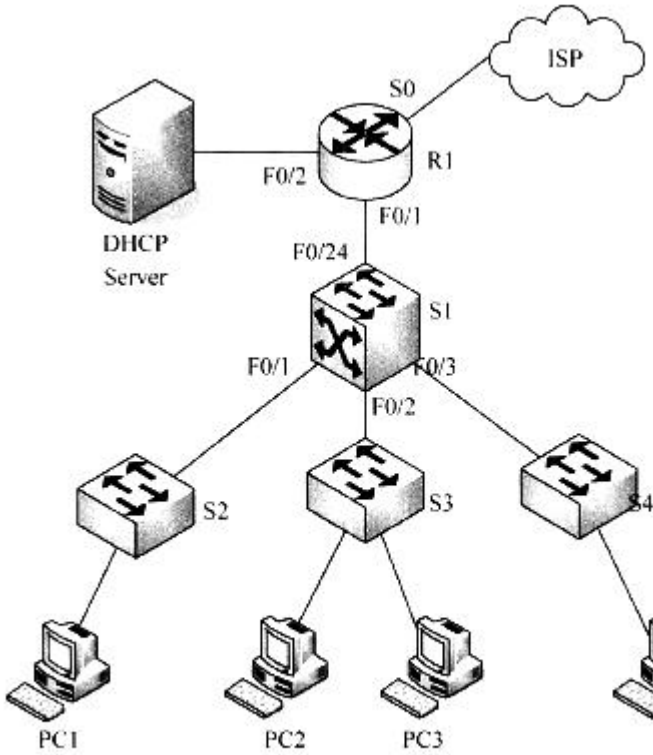

图 4-1

【问题 1】(2 分)

为了节省 IP 地址，在接口地址上均使用 30 位地址掩码，请补充下表中的空白。

设备	接口	IP 地址	设备	接口	IP 地址
S1	F0/24	192.168.1.253	R1	F0/1	(1)
DHCPServer	Eth0	192.168.1.249		F0/2	(2)

(1) 192.168.1.254

(2) 192.168.1.250

本题考查交换机的配置以及三层交换机中实现 VLAN 间路由的基本配置方法。

该类题目首先要求考生能够认真阅读题目，领会题目的要求，并熟悉相关设备的基本配置命令和配置逻辑。

问题 1 的说明中，已明确表示使用 30 位掩码作为设备之间连接时接口的 IP 地

址根据问题 1 中表格所示，已给出了对端的 IP 地址，并使用的是 30 位掩码，通过 IP 地址计算，可得路由器对应接口上的 IP 地址。

【问题 2】（9 分）

将公司内部用户按照部门分别划分在 3 个 vlan 中：vlan 10，vlan 20 和 vlan 30。均连接在交换机 S1 上，并通过 S1 实现 vlan 间通信，所有内网主机均采用 DHCP 获取 IP 地址。按照要求补充完成（或解释）以下配置命令。

```
Switch>en
Switch#（3）
Switch(config)#hostname （4）
S1(config)#interface fastEthernet 0/1
S1(config-if)#（5） mode trunk
S1(config)#interface vlan 10          //（6）
S1(config-if)#ip address 192.168.1.206 255.255.255.240
S1(config-if)#no shutdown
S1(config-if)#ip helper-address （7）
S1(config-if)#（8）
S1(config)#
.....
S1(config)#router （9）
S1(config-router)#version （10）
S1(config-router)#network 192.168.1.192
S1(config-router)#network 192.168.1.208
S1(config-router)#network 192.168.1.224
S1(config-router)#（11）
S1#
```

（3）config terminal

（4）S1

（5）switchport

（6）进入 vlan10 接口配置

（7）192.168.1.249

（8）exit

（9）rip

（10）2

（11）end

根据问题 2 的描述可知，对交换机 S1 需要完成 VLAN 间路由、DHCP 中继和 RIP 协议的配置。其中，DHCP 中继需指明 DHCP 服务器的 IP 地址。在 RIP 协议的配置中，由于局域网地址均使用的是非主类地址，需要使用 RIPv2 版本才可以正确宣告路由。

【问题 3】（2 分）

在 S1 上将 F0/1 接口配置为 trunk 模式时，出现了以下提示：

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

应采取 （12） 方法解决该问题。

（12）选项：

A. 在该接口上使用 no shutdown 命令后再使用该命令

B. 在该接口上启用二层功后能再使用该命令

C. 重新启动交换机后再使用该命令

D. 将该接口配置为 access 模式后再使用该命令

（12）D

在三层交换机上，当交换机接口模式为“auto”模式时，无法直接将该接口模式配置为中继“trunk”模式，需先将该接口的模式手动调整为“access”模式后，再使用中继配置命令，将接口模式配置为中继模式。

【问题 4】（2 分）

在 S1 上配置的三个 SVI 接口地址分别处在 192.168.1.192，192.168.1.208 和 192.168.1.224 网段，它们的子网掩码是 （13） 。

（13）255.255.255.240

为了在交换机上实现 VLAN 间路由，需在交换机上设置 SVI(Switch Visual Interface）接口，3 个 SVI 接口处在 192.168.1.192，192.168.1.208 和 192.168.1.224 网段，将最后一个字节使用二进制表示后为：

192： 11000000

208： 11010000

224： 11100000

可知，其子网掩码为 28 位掩码。