

CPU 是在(1)结束时响应 DMA 请求的。

- (1) A. 一条指令执行 B. 一段程序 C. 一个时钟周期 D. 一个总线周期

【答案】D

【解析】本题考查计算机组成基础知识。

DMA 控制器在需要的时候代替 CPU 作为总线主设备，在不受 CPU 干预的情况下，控制 I/O 设备与系统主存之间的直接数据传输。DMA 操作占用的资源是系统总线，而 CPU 并非在整个指令执行期间即指令周期内都会使用总线，故 DMA 请求的检测点设置在每个机器周期也即总线周期结束时执行，这样使得总线利用率最高。

虚拟存储体系是由(2)两级存储器构成。

- (2) A. 主存-辅存 B. 寄存器-Cache C. 寄存器-主存 D. Cache-主存

【答案】A

【解析】本题考查计算机组成基础知识。

计算机中不同容量、不同速度、不同访问形式、不同用途的各种存储器形成的是一种层次结构的存储系统。所有的存储器设备按照一定的层次逻辑关系通过软硬件连接起来，并进行有效的管理，就形成了存储体系。不同层次上的存储器发挥着不同的作用。一般计算机系统中主要有两种存储体系：Cache 存储体系由 Cache 和主存储器构成，主要目的是提高存储器速度，对系统程序员以上均透明；虚拟存储体系由主存储器和在线磁盘存储器等辅存构成，主要目的是扩大存储器容量，对应用程序员透明。

在机器指令的地址字段中，直接指出操作数本身的寻址方式称为(3)。

- (3) A. 隐含寻址 B. 寄存器寻址 C. 立即寻址 D. 直接寻址

【答案】C

【解析】本题考查计算机组成基础知识。

随着主存增加，指令本身很难保证直接反映操作数的值或其地址，必须通过某种映射方式实现对所需操作数的获取。指令系统中将这种映射方式称为寻址方式，即指令按什么方式寻找（或访问）到所需的操作数或信息（例如转移地址信息等）。可以被指令访问到的数据和信息包括通用寄存器、主存、堆栈及外设端口寄存器等。

指令中地址码字段直接给出操作数本身，而不是其访存地址，不需要访问任何地址的寻址方式被称为立即寻址。

内存按字节编址从 B3000H 到 DABFFH 的区域，其存储容量为(4)。

- (4) A. 123KB B. 159KB C. 163KB D. 194KB

【答案】B

【解析】本题考查计算机组成基础知识。

直接计算 16 进制地址包含的存储单元个数即可。

$DABFFH - B3000H + 1 = 27C00H = 162816 = 159K$, 按字节编址，故此区域的存储容量为 159KB。

在软件项目管理中，以下关于人员管理的叙述，正确的是(5)。

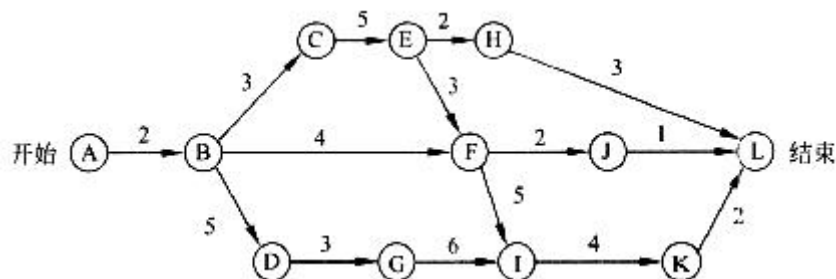
- (5) A. 项目组成员的工作风格也应该作为组织团队时要考虑的一个要素
B. 鼓励团队的每个成员充分地参与开发过程的所有阶段
C. 仅根据开发人员的能力来组织开发团队
D. 若项目进度滞后于计划，则增加开发人员一定可以加快开发进度

【答案】A

【解析】本题考查软件项目管理的基础知识。

人员管理是软件项目管理的一个重要部分，在组织开发团队时，应该考虑开发人员的工作能力、知识背景、工作风格、兴趣爱好等多方面的因素。每个成员的工作任务分配清楚，不应该参与所有阶段的工作。当项目进度滞后于项目计划时，增加开发人员不一定可以加快开发进度。

某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示该活动所需的天数，则完成该项目的最少时间为(6)天。活动 BD 最多可以晚(7)天开始而不会影响整个项目的进度。



- | | | | |
|----------|-------|-------|-------|
| (6) A. 9 | B. 15 | C. 22 | D. 24 |
| (7) A. 2 | B. 3 | C. 5 | D. 9 |

【答案】D A

【解析】本题考查软件项目管理的基础知识。

根据上图计算出关键路径为 A-B-C-E-F-I-K-L, 其长度为 24, 关键路径上的活动均为关键活动。活动 BD 不在关键路径上, 包含该活动的最长路径为 A-B-D-G-I-K-L, 其长度为 22, 因此松弛时间为 2。

在 Windows 系统中, 设 E 盘的根目录下存在 document1 文件夹, 用户在该文件夹下已创建了 document2 文件夹, 而当前文件夹为, document1。若用户将 test.docx 文件存放 document2 文件夹中, 则该文件的绝对路径为 (8); 在程序中能正确访问该文件且效率较高的方式为 (9)。

- | | |
|-----------------------------|--------------------------------------|
| (8) A. \document1\ | B. E:\document1\ document2 |
| C. document2\ | D. E:\document2\ document1 |
| (9) A. \document1\test.docx | B. document1\ document2\test.docx |
| C. document2\test.docx | D. E:\document1\ document2\test.docx |

【答案】B C

【解析】

按查找文件的起点不同可以将路径分为: 绝对路径和相对路径。从根目录开始的路径称为绝对路径; 从用户当前工作目录开始的路径称为相对路径, 相对路径是随着当前工作目录的变化而改变的。

在 Windows 操作系统中, 绝对路径是从根目录开始到文件所经过的文件夹名构成的, 并以开始, 表示根目录; 文件夹名之间用符号 “\” 分隔。按题意, “test.docx” 的绝对路径表示为: E:\document1\ document2。相对路径是从当前文件夹开始到文件所经过的文件夹名。编程时采用相对路径名 document2\test.docx, 不仅能正确地访问该文件而且效率也更高。

软件设计师王某在其公司的某一综合信息管理系统软件开发工作中承担了大部分程序设计工作。该系统交付用户, 投入试运行后, 王某辞职离开公司, 并带走了该综合信息管理系统源程序, 拒不交还公司。王某认为, 综合信息管理系统源程序是他独立完成的, 他是综合信息管理系统源程序的软件著作权人。王某的行为 (10)。

- (10) A. 侵犯了公司的软件著作权 B. 未侵犯公司的软件著作权
C. 侵犯了公司的商业秘密权 D. 不涉及侵犯公司的软件著作权

【答案】A

【解析】

王某的行为侵犯了公司的软件著作权。因为王某作为公司的职员，完成的某一综合信息管理系统软件是针对其本职工作中明确指定的开发目标而开发的软件。该软件应为职务作品，并属于特殊职务作品。公司对该软件享有除署名权外的软件著作权的其他权利，而王某只享有署名权。王某持有该软件源程序不归还公司的行为，妨碍了公司正常行使软件著作权，构成对公司软件著作权的侵犯，应承担停止侵权法律责任，交还软件源程序。

集线器与网桥的区别是(11)。

- (11) A. 集线器不能检测发送冲突，而网桥可以检测冲突
B. 集线器是物理层设备，而网桥是数据链路层设备
C. 网桥只有两介端口，而集线器是一种多端口网桥
D. 网桥是物理层设备，而集线器是数据链路层设备

【答案】B

【解析】

集线器是物理层设备，相当于在 10BASE2 局域网中把连接工作站的同轴电缆收拢在一个盒子里，这个盒子只起到接收和发送的功能，可以检测发送冲突，但不能识别数据链路层的帧。网桥是数据链路层设备，它可以识别数据链路层 MAC 地址，有选择地把帧发送到输出口，网桥也可以有多个端口，如果网桥端口很多，并配置了加快转发的硬件，就成为局域网交换机。

根据 STP 协议，网桥 ID 最小的交换机被选举为根网桥，网桥 ID 由(12)字节的优先级和 6 字节的(13)组成。

- (12) A. 2 B. 4 C. 6 D. 8
(13) A. 用户标识 B. MAC 地址 C. IP 地址 D. 端口号

【答案】A B

【解析】

根据 STP 协议，网桥 ID 由 2 字节的网桥优先级和 6 字节的网桥 MAC 地址组成，取值范

围为 0~65535，默认值为 32768。

关于 ICMP 协议，下面的论述中正确的是 (14)。

- (14) A. 通过 ICMP 可以找到与 MAC 地址对应的 IP 地址
B. 通过 ICMP 可以把全局 IP 地址转换为本地 IP 地址
C. ICMP 用于动态分配 IP 地址
D. ICMP 可传送 IP 通信过程中出现的错误信息

【答案】D

【解析】

ICMP 与 IP 同属于网络层协议，用于传送有关通信问题的消息，例如数据报不能到达目标，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。支持 IPv6 地址的 ICMPv6 协议增加的邻居发现功能代替了 ARP 协议，ICMPv6 还支持 IPv6 中的路由优化、IP 组播、移动 IP 等增加了一些新的报文类型。

设信号的波特率为 500Baud，采用幅度-相位复合调制技术，由 4 种幅度和 8 种相位组成 16 种码元，则信道的数据速率为 (15)。

- (15) A. 500 b/s B. 1000 b/s C. 2000 b/s D. 4800 b/s

【答案】C

【解析】

根据尼奎斯特定理，若信道带宽为 W，则最大码元速率为

$$B=2W \text{ (Baud)}$$

尼奎斯特定理指定的信道容量也叫做尼奎斯特极限，这是由信道的物理特性决定的。码元携带的信息量由码元取的离散值个数决定。若码元取两个离散值，则一个码元携带 1 比特 (bit) 信息。若码元可取 4 种离散值，则一个码元携带 2 比特信息。总之一码元携带的信息量 n (比特数) 与码元的种类个数 N 有如下关系：

$$n=\log_2 N \quad (N=2^n)$$

单位时间内在信道上传送的信息量 (比特数) 称为数据速率。在一定的波特率下提高速率的途径是用一个码元表示更多的比特数。如果把 2 比特编码为一个码元，则数据速率可成倍提高，公式为

$$R=B\log_2 N=2W\log_2 N \text{ (b/s)}$$

在本题中 $B=500\text{Baud}$, $N=16$, 所以 $R=B\log_2 N=500 \times \log_2 16=2000\text{b/s}$

E1 载波的数据速率是 (16)。E3 载波的数据速率是 (17)。

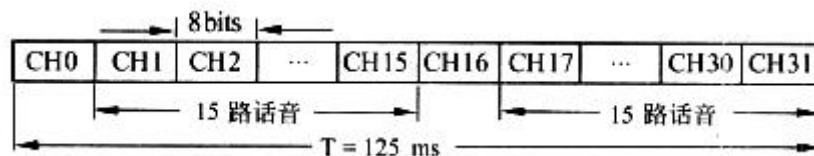
(16) A. 64kb/s B. 2.048Mb/s C. 34.368Mb/s D. 139.26Mb/s

(17) A. 64kb/s B. 2.048Mb/s C. 34.368Mb/s D. 139.26Mb/s

【答案】B C

【解析】

ITU-T E1 信道的数据速率是 2.048 Mb/s (见下图)。这种载波把 32 个 8 位一组的数据样本组装成 $125 \mu\text{s}$ 的基本帧, 其中 30 个子信道用于语音传送数据, 2 个子信道(CH0 和 CH16)用于传送控制信令, 每 4 帧能提供 64 个控制位。除了北美和日本外, E1 载波在其他地区得到广泛使用。



按照 ITU-T 的多路复用标准, E2 载波由 4 个 E1 载波组成, 数据速率为 8.448Mb/s。E3 载波由 4 个 E2 载波组成, 数据速率为 34.368 Mb/s。E4 载波由 4 个 E3 载波组成, 数据速率为 139.264 Mb/s。E5 载波由 4 个 E4 载波组成, 数据速率为 565.148 Mb/s。

ADSL 采用 (18) 技术把 PSTN 线路划分为语音、上行和下行三个独立的信道, 同时提供电话和上网服务。采用 ADSL 联网, 计算机需要通过 (19) 和分离器连接到电话入户接线盒。

(18) A. 对分复用 B. 频分复用 C. 空分复用 D. 码分多址

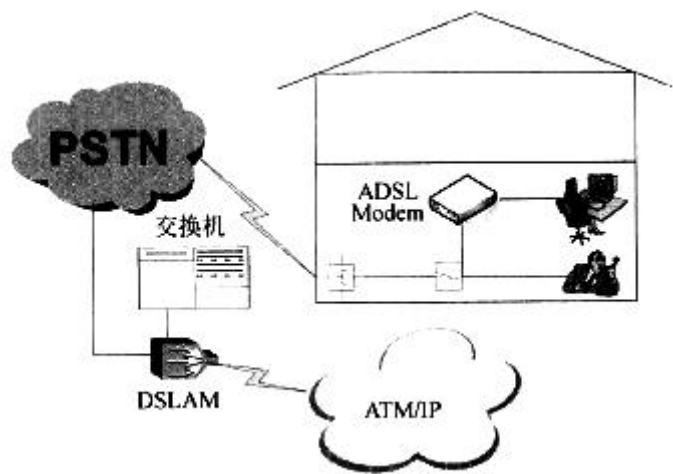
(19) A. ADSL 交换机 B. Cable Modem C. ADSL Modem D. 无线路由器

【答案】B C

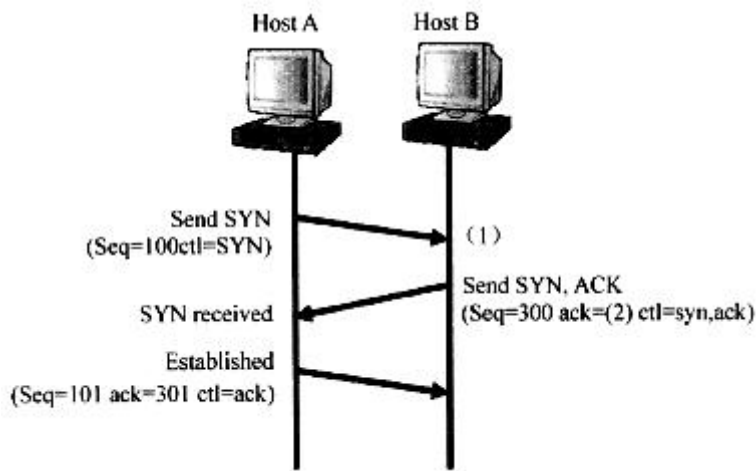
【解析】

数字用户线路 (Digital Subscriber Line, DSL) 是以铜质电话线为传输介质的通信技术组合, 采用频分复用技术把 PSTN 线路划分为语音、上行和下行三个独立的信道。非对称 DSL (Asymmetric DSL, ADSL) 在一对铜线上支持上行速率 640Kb/s~1Mb/s、下行速率 1Mb/s~8Mb/s, 有效传输距离在 3~5 公里范围以内。在提供语音服务的同时还可以满足网上冲浪

和视频点播等应用对带宽的要求。采用 ADSL 联网，计算机需要通过 ADSL Modem 和分离器连接到电话入户接线盒，如下图所示。



下图中主机 A 和主机 B 通过三次握手建立 TCP 连接，图中 (1) 处的状态是 (20)，图 (2) 处的数字是 (21)。

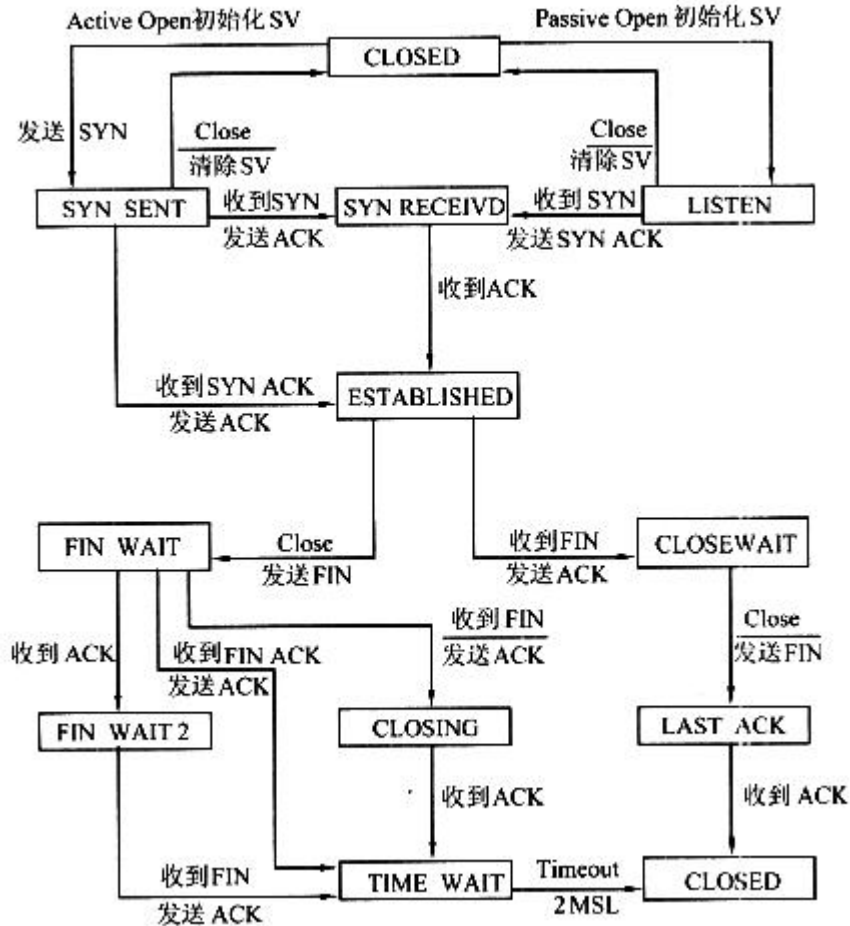


- (20) A. SYN received B. Established C. Listen D. FIN wait
- (21) A. 100 B. 101 C. 300 D. 301

【答案】 A B

【解析】

TCP 连接管理如下图所示。由于主机 A 发出了连接请求 (SendSYN)，所以主机 B 收到这个请求时的状态是 SYN received。又由于主机 A 发出的序列号是 100，所以主机 B 准备从 101 字节开始接收。



TCP 使用的流量控制协议是 (22)。

(22) A. 固定大小的滑动窗口协议

B. 可变大小的滑动窗口协议

C. 后退 N 帧 ARQ 协议

D. 停等协议

【答案】B

【解析】

TCP 的流量控制采用了可变大小的滑动窗口协议，由接收方指明接收缓冲区的大小（字节数），发送方发送了规定的字节数后等待接收方的下一次请求。固定大小的滑动窗口协议用在数据链路层的 HDLC 中。可变大小的滑动窗口协议可以应付长距离通信过程中线路延迟不确定的情况，而固定大小的滑动窗口协议则适合链路两端点之间通信延迟固定的情况。

下面 4 种路由中，哪一种路由的子网掩码是 255.255.255.255？ (23)。

(23) A. 远程网络路由

B. 主机路由

C. 默认路由

D. 静态路由

【答案】B

【解析】

主机路由的子网掩码是 255.255.255.255。网络路由要指明一个子网，所以不可能为全 1，默认路由是访问默认网关，而默认网关与本地主机属于同一个子网，其子网掩码也应该与网络路由相同，对静态路由也是同样的道理。

边界网关协议 BGP4 是一种动态路由发现协议，它的主要功能是 (24)。BGP 路由器之间传送的是 AS 路径信息，这样就解决了 (25) 问题。BGP4 报文封装在 (26)。

(24) A. 发现新的路由 B. 计算最短通路 C. 控制路由策略 D. 维护网络拓扑数据库

(25) A. 路由环路 B. 最短通路 C. 路由计算 D. 路由更新

(26) A. IP 数据报 B. 以太网帧 C. TCP 报文 D. UDP 报文

【答案】C A C

【解析】

外部网关协议 BGP 4 是一种动态路由发现协议，其主要功能是控制路由策略，例如是否愿意转发过路的数据包等。BGP 路由器之间传送的是 AS 路径信息，由一个目标网络地址后跟一串要经过的 AS 的编号组成，如果该串中出现了相同的 AS 编号，这就是出现了路由环路。BGP4 报文封装在 TCP 报文中传送，在封装层次上看似 TCP 的上层协议，但是从功能上理解它解决的是路由问题，所以仍然属于网络层协议。

在广播网络中，OSPF 协议要选定一个指定路由器 (DR)，指定路由器的功能是 (27)。

(27) A. 发送链路状态公告 B. 检查网络故障
C. 向其他路由器发送最新路由表 D. 发现新增加的路由器

【答案】A

【解析】

OSPF 是一种链路状态协议，用于在自治内部路由器之间交换路由信息。链路状态协议是从各个路由器收集链路状态信息，构造网络拓扑结构图，使用 Dijkstra 的最短通路优先 (SPF) 算法计算到达各个目标的最佳路由。

如果两个路由器都通过各自的接口连接到一个共同的网络上，则它们是邻居 (Neighboring) 关系。路由器可以在其邻居中选择需要交换链路状态信息的路由器，与之建立毗邻关系 (Adjacency)。并不是每一对邻居都需要交换路由信息，因而不是每一对邻居都要建立毗邻关系。在一个广播网络或 NBMA 网络中要选举一个指定路由器 (Designated

Router, DR), 其他的路由器都与 DR 建立毗邻关系, 把自己掌握的链路状态信息提交给 DR, 由 DR 代表这个网络向外界发布。可以看出, DR 的存在减少了毗邻关系的数量, 从而也减少了向外发布的路由信息量。

OSPF 路由器之间通过链路状态公告 (Link State Advertisement, LSA) 交换网络拓扑信息。LSA 中包含连接的接口、链路的度量值 (Metric) 等信息。

POP3 协议采用 (28) 模式, 客户端代理与 POP3 服务器通过建立 (29) 连接来传送数据。

(28) A. Browser/Server B. Client/Server C. Peer to Peer D. Peer to Server

(29) A. TCP B. UDP C. P2P D. IP

【答案】B A

【解析】 本题考查 POP3 协议及 POP3 服务器方面的基础知识。

POP3 协议是 TCP/IP 协议簇中用于邮件接收的协议。邮件客户端通过与服务器之间建立 TCP 连接, 采用 Client/Server 计算模式来传送邮件。

如果要将目标网络为 202.117.112.0/24 的分组经 102.217.115.1 接口发出, 需增加一条静态路由, 正确的命令是 (30)。

(30) A. Route add 202.117.112.0 255.255.255.0 102.217.115.1

B. Route add 202.117.112.0 0.0.0.255 102.217.115.1

C. add route 202.117.112.0 255.255.255.0 102.217.115.1

D. add route 202.117.112.0 0.0.0.255 102.217.115.1

【答案】A

【解析】 本题考查路由配置命令格式方面的基础知识。

route 命令的功能是显示和修改本地的 IP 路由表, 语法如下:

```
route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]]  
[if Interface]]
```

Command 命令值为 add, 表示添加路由。目标网络为 202.117.112.0/24, 且接口为 102.217.115.1, 故正确的命令为:

```
route add 202.117.112.0    255.255.255.0    102.217.115.1
```

在 Linux 系统中, 使用 ifconfig 设置接口的 IP 地址并启动该接口的命令是 (31)。

- (31)A. `ifconfig eth0 192.168.1.1 mask 255.255.255.0`
B. `ifconfig 192.168.1.1 mask 255.255.255.0 up`
C. `ifconfig eth0 192.168.1.1 mask 255.255.255.0 up`
D. `ifconfig 192.168.1.1 255.255.255.0`

【答案】C

【解析】本题目考查是在 Linux 系统下基本命令使用的基础知识。

在 Linux 系统下，设置接口 IP 地址，并将接口启动的命令格式是：

`ifconfig` 接口名称 IP 地址 mask 子网掩码 up/down

根据以上命令格式，据题意可知，C 为正确答案。

在 Linux 系统中，在 (32) 文件中查看一台主机的名称和完整域名。

- (32)A. `etc/dev` B. `etc/conf` C. `etc/hostname` D. `etc/network`

【答案】C

【解析】本题目考查是在 Linux 系统文件系统的基础知识。

在 Linux 操作系统中，TCP/IP 网络是通过若干个文本文件进行配置的。系统在启动时通过读取一组有关网络配置的文件和脚本参数内容，来实现网络接口的初始化和控制过程，这些文件和脚本大多数位于 `/etc` 目录下。

`/etc/hostname` 文件包含了 Linux 系统的主机名称，包括完全的域名。

`/etc/host.conf` 文件指定如何解析主机域名，Linux 通过解析器库来获得主机名对应的 IP 地址。

`/etc/sysconfig/network` 是一个用来指定服务器 h 的网络配署信息的文件，包含了控制和网络有关的文件和守护程序行为的参数。

在 Windows 客户端运行 `nslookup` 命令，结果如下图所示。为 `www.softwaretest.com` 提供解析的是 (33)。在 DNS 服务器中，`ftp.softwaretest.com` 记录通过 (34) 方式建立。

```
C:\Documents and Settings\user>nslookup www.softwaretest.com
Server: ns1.softwaretest.com
Address: 192.168.1.254
```

Non-authoritative answer:

```
Name: www.softwaretest.com
Address: 10.10.1.3
```

```
C:\Documents and Settings\user>nslookup ftp.softwaretest.com
Server: ns1.softwaretest.com
Address: 192.168.1.254
```

Non-authoritative answer:

```
Name: ns1.softwaretest.com
Address: 10.10.1.1
Aliases: ftp.softwaretest.com
```

(33) A. 192.168.1.254 B. 10.10.1.3 C. 10.10.1.1 D. 192.168.1.1

(34) A. 主机 B. 别名 C. 邮件交换器 D. PTR 记录

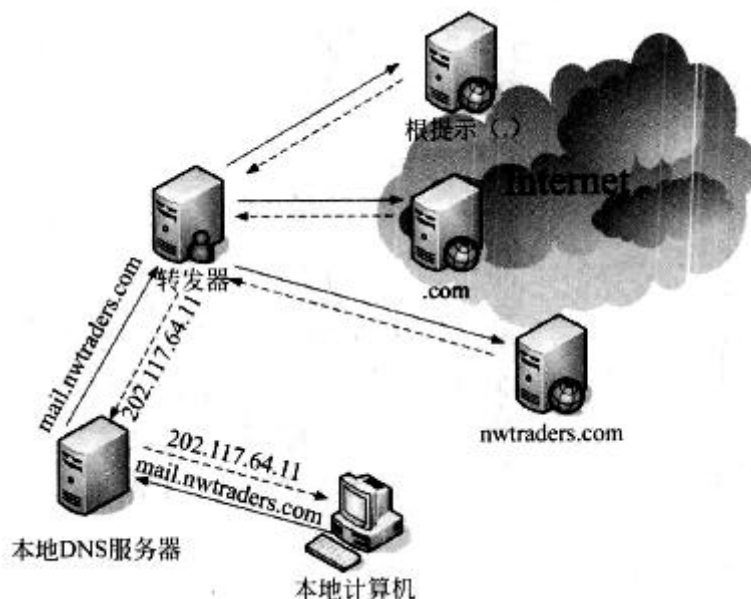
【答案】 A B

【解析】 本题考查 DNS 服务器方面的基础知识。

nslookup 命令显示的是为域名提供解析的服务器及相关资源记录。记录显示为 www.softwaretest.com 及 ftp. Softwaretest.com, 提供解析的服务器是 ns1.softwaretest.com, 其 IP 地址为 192.168.1.254。

又由记录显示 ftp.softwaretest.com 是 10.10.1.1 主机上通过别名建立的域名。

下图是 DNS 转发器工作的过程。采用迭代查询算法的是 (35)。



- (35) A. 转发器和本地 DNS 服务器 B. 根域名服务器和本地 DNS 服务器
C. 本地 DNS 服务器和 .com 域名服务器 D. 根域名服务器和 .com 域名服务器

【答案】D

【解析】本题考查 DNS 服务器递归算法和迭代算法方面的基础知识。

递归查询只发出一次查询请求,要求服务器彻底地进行名字解析。当需要进一步查询时,本域名服务器向上级域名服务器返回其他域名服务器发出请求,直到查到记录。

迭代查询可能发出多条请求,即上级域名服务器若返回的是其他域名服务器的地址,本域名服务器把这个地址发给用户,用户再进行深一级的查询。

从本题中可以看出,根域名服务器发回给转发器的是 .com 服务器地址,并不是结果,故采用的是迭代算法;.com 域名服务器发回给转发器的是授权域名服务器 nwtraders.com 服务器地址,也不是结果,采用的也是迭代算法;nwtraders.com 服务器尽管返回给转发器域名和 IP 的对应关系,但它是授权域名服务器,在其资源记录中已经找到了记录,故其采用的算法未知。本地域名服务器只向转发器发出了 1 条请求,转发器经过多次深层次查询,返回的是查到的记录,故转发器采用的是递归算法。本地域名服务器采用的算法未知。

下列域名中,格式正确的是 (36)。

- (36) A. -123456.com B. 123-456.com C. 123*456.com D. 123456-.com

【答案】B

【解析】本题目考查域名的基础知识。

以下关于域名查询的叙述中，正确的是(37)。

- 【答案】 D**

DNS 中的 PTR 记录是用来指定 IP 地址对应的主机名（或域名）记录。

下列地址中，(38) 不是 DHCP 服务器分配的 IP 地址。

- 【答案】B

下图是配置某邮件客户端的界面，图中 a 处应填写 (39)。b 处应填写 (40)。



(39) A. abc. com B. POP3. abc. com C. POP. com D. POP3. com

(40) A. 25 B. 52 C. 100 D. 110

【答案】B D

【解析】本题考查邮件客户端设置的基础知识。

在设置邮件客户端程序时，需设置相应的发送邮件服务器（SMTP 服务器）和接收邮件服务器（POP 服务器）。根据题意，邮件发送使用 SMTP 协议，因此服务器的地址是 SMTP. abc. com，其对应端口是 25 号端口；接收邮件使用 POP3 服务器，服务器的地址是 POP3. abc. com，对应端口是 110。

（41）不属于主动攻击。

(41) A. 流量分析 B. 重放 C. IP 地址欺骗 D. 拒绝服务

【答案】A

【解析】本题考查网络攻击的基础知识。

网络攻击有主动攻击和被动攻击两类。其中主动攻击是指通过一系列的方法，主动地向被攻击对象实施破坏的一种攻击方式，例如重放攻击、IP 地址欺骗、拒绝服务攻击等均属于攻击者主动向攻击对象发起破坏性攻击的方式。流量分析攻击是通过持续检测现有网络中的流量变化或者变化趋势，而得到相应信息的一种被动攻击方式。

下列算法中，可用于报文认证的是（42），可以提供数字签名的是（43）。

(42) A. RSA B. IDEA C. RC4 D. MD5

(43) A. RSA

B. IDEA

C. RC4

D. MD5

【答案】D A

【解析】本题考查报文认证和数字签名的基础知识。

报文认证是指在网络上对接收到的报文的完整性进行确认的过程。一般实现时使用一种散列函数，例如 MD5 或者 SHA-1，将任意长度的文本作为输入，产生长度为 L 的输出，作为报文认证信息与原报文一同发送给接收者，接收者接收到文本后，使用相同的散列函数进行计算，将计算结果与报文认证信息进行对比之后即可验证文本的完整性和真实性。而数字签名是使用公钥体制（如 RSA）产生的一对公钥和私钥，使用私钥对报文进行签名，使用公钥对文件的签名进行验证，起到保证文件的不可否认性的作用。

下列 (44) 不能提供应用层安全。

(44) A. S-HTTP

B. PGP

C. MIME

D. SET

【答案】C

【解析】本题考查应用层安全协议的基础知识。

以上 4 个选项中，S-HTTP 是安全的 HTTP，采用了超文本信息的协议，一般用于安全性要求较高的 Web 浏览环境，如电子商务网页浏览、通过网页支付等环境，它提供的是应用层的安全服务。HTTPS 是经过 SSL 加密的。

PGP 是传输安全电子邮件的协议，可对电子邮件进行加密、签名等操作，它提供的是应用层安全服务。

MIME (Multipurpose Internet Mail Extensions, 多用途互联网邮件扩展类型) 是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。它并未提供任何应用层安全服务。

SET (Secure Electronic Transaction, 简称 SET 协议) 主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份，以及可操作性。SET 中的核心技术主要有公开密钥加密、数字签名、电子信封、安全证书等，它提供的是应用层安全服务。

防火墙不具备 (45) 功能。

(45) A. 包过滤

B. 查毒

C. 记录访问过程

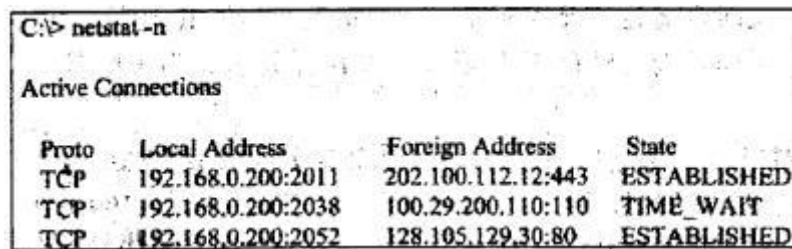
D. 代理

【答案】B

【解析】本题考查防火墙基础知识。

防火墙是一种放置在网络边界上，用于保护内部网络安全的网络设备。它通过对流经的数据流进行分析和检查，可实现对数据包的过滤、保存用户访问网络的记录和服务器代理功能。防火墙不具备检查病毒的功能。

如下图所示，从输出的信息中可以确定的是 (46)。



Proto	Local Address	Foreign Address	State
TCP	192.168.0.200:2011	202.100.112.12:443	ESTABLISHED
TCP	192.168.0.200:2038	100.29.200.110:110	TIME_WAIT
TCP	192.168.0.200:2052	128.105.129.30:80	ESTABLISHED

- (46) A. 本地主机正在使用的端口号是公共端口号
B. 192.168.0.200 正在与 128.105.129.30 建立连接
C. 本地主机与 202.100.112.12 建立了安全连接
D. 本地主机正在与 100.29.200.110 建立连接

【答案】C

【解析】本题考查网管命令 netstat -n 的含义。

从 netstat -n 的输出信息中可以看出，本地主机 192.168.0.200 使用的端口号 2011、2038、2052 都不是公共端口号。根据状态提示信息，其中已经与主机 128.105.129.30 建立了连接，与主机 100.29.200.110 正在等待建立连接，与主机 202.100.112.12 已经建立了安全连接。

为防止 www 服务器与浏览器之间传输的信息被窃听，可以采取 (47) 来防止该事件的发生。

- (47) A. 禁止浏览器运行 Active X 控件
B. 索取 WWW 服务器的 CA 证书
C. 将 WWW 服务器地址放入浏览器的可信站点区域
D. 使用 SSL 对传输的信息进行加密

【答案】D

【解析】本题考查利用 SSL 传输的相关知识。

SSL 是一个安全协议，它提供使用 TCP/IP 的通信应用程序间的隐私与完整性。因特网的超文本传输协议（HTTP）使用 SSL 来实现安全的通信。

SSL 协议位于 TCP 协议与各种应用层协议之间，为数据通讯提供安全支持。SSL 协议可分为两层。SSL 记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL 握手协议（SSL Handshake Protocol）：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。提供的服务如下：

- ①认证用户和服务，确保数据发送到正确的客户机和服务器；
- ②加密数据以防止数据中途被窃取；
- ③维护数据的完整性，确保数据在传输过程中不被改变。

某用户无法访问域名为 www.cisco.com 的网站，在用户主机上执行 tracert 命令得到提示如下：

```
Tracing route to www.cisco.com[119.188.155.27]
Over a maximum of 30 hops:
 0  <1ms  <1ms  <1ms  202.117.112.129
 1  202.117.112.129  reports:Destination net unreachable
```

根据提示信息，造成这种现象的原因可能是（48）。

- (48) A. 用户主机的网关设置错误
- B. 用户主机设置的 DNS 服务器工作不正常
- C. 路由器上进行了相关 ACL 设置
- D. 用户主机的 IP 地址设置错误

【答案】C

【解析】本题考查网管命令 tracert 的含义。

从 tracert 的输出信息中可以看出，DNS 解析正常，说明 DNS 服务器工作正常；第一跳到网关<1ms，说明网关设置正确；那么说明用户主机的 IP 地址设置也没有问题，由网关给出目标不可达信息，说明可能在路由器上进行了相关 ACL 设置，不允许访问。

下列网络管理软件中不需要 SNMP 支持的是（49）。

- (49) A. CiscoWorks
- B. Netview
- C. Solarwinds
- D. Wireshark

【答案】D

【解析】 本题考查网管命令网络管理软件的使用常识。

在这 4 个软件中，CiscoWorks、Netview 以及 Solarwinds 都是网络管理软件，都须得到 SNMP 的支持，而 Wireshark (前称 Ethereal) 是一个网络封包分析软件。网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料，并不要求 SNMP 的支持。

在 SNMPv2 错误类型中，表示管理对象不可访问的是 (50)。

(50) A. noAccess B. genErr C. wrongValue D. noCreation

【答案】 A

【解析】 本题考查 SNMPv2 的错误类型。

在 SNMPv2 错误类型中，表示管理对象不可访问的是 noAccess。而 genErr 表示某些其他的差错。若代理不执行该操作，则返回 wrongValue。noCreation 则表示对象不存在且无法建立。

通过 CIDR 技术，把 4 个主机地址 220.78.169.5、220.78.172.10、220.78.174.15 和 220.78.168.254 组织成一个地址块，则这个超级地址块的地址是 (51)。

(51) A. 220.78.177.0/21 B. 220.78.168.0/21
C. 220.78.169.0/20 D. 220.78.175.0/20

【答案】 B

【解析】

地址 220.78.169.5 的二进制表示是：1101 1100.0100 1110.1010 1001.0000 0101

地址 220.78.172.10 的二进制表示是：1101 1100.0100 1110.1010 1100.0000 1010

地址 220.78.174.15 的二进制表示是：1101 1100.0100 1110.1010 1110.0000 1111

地址 220.78.168.254 的二进制表示是：1101 1100.0100 1110.1010 1000.1111 1110

4 个地址共同的部分是：1101 1100.0100 1110.1010 1

所以取 220.78.168.0/21 作为超级地址块。1101 1100.0100 1110.1010 1000.0000 0000

采用可变长子网掩码可以把大的网络分成小的子网，例如把 A 类网络 60.15.0.0/16 分为两个子网，假设第一个子网为 60.15.0.0/17，则另一个子网为 (52)。

(52) A. 60.15.1.0/17 B. 60.15.2.0/17

C. 60. 15. 100. 0/17

D. 60. 15. 128. 0/17

【答案】D

【解析】

第一个子网为 60. 15. 0. 0/17

0011 1100. 0000 1111. 0000 0000. 0000 0000

则另一个子网为 60. 15. 128. 0/17

0011 1100. 0000 1111. 1000 0000. 0000 0000

假设用户 X 有 4000 台主机，则必须给他分配 (53) 个 C 类网络。如果为其分配的网络号为 196. 25. 64. 0，则给该用户指定的地址掩码为 (54)。

(53) A. 4

B. 8

C. 10

D. 16

(54) A. 255. 255. 255. 0

B. 255. 255. 250. 0

C. 255. 255. 248. 0

D. 255. 255. 240. 0

【答案】D D

【解析】

用户 X 有 4000 台主机，则必须给他分配 16 个 C 类网络， $253 \times 16 = 4048$ 。给该用户指定的地址掩码为 255. 255. 240. 0，其二进制表示形式为：

1111 1111. 1111 1111. 1111 0000. 0000 0000

第三个字节的前四位为子网掩码的一部分，第三个字节的后四位用于区分 16 个不同的 C 类网络。

如果在查找路由表时发现有多项匹配，那么应该根据 (55) 原则进行选择。假设路由表有 4 个表项如下所示，那么与地址 139. 17. 179. 92 匹配的表项是 (56)。

(55) A. 包含匹配

B. 恰当匹配

C. 最长匹配

D. 最短匹配

(56) A. 139. 17. 145. 32

B. 139. 17. 145 . 64

C. 139. 17. 147. 64

D. 139. 17. 177. 64

【答案】C D

【解析】

查找路由表时如发现有多个选项匹配，那么应该根据最长匹配原则进行选择。列出的 4 个表项中，与地址 139. 17. 179. 92 匹配的表项是 139. 17. 177. 64，参见下面的二进制表示。

路由表项 139. 17. 145. 32 的二进制表示为：1000 1011. 0001 0001. 1001 0001. 0010 0000

路由表项 139. 17. 145. 64 的二进制表示为：1000 1011. 0001 0001. 1001 0001. 0100 0000

路由表项 139.17.147.64 的二进制表示为：1000 1011.0001 0001.1001 0011.0100 0000

路由表项 139.17.177.64 的二进制表示为：1000 1011.0001 0001.1011 0001.0100 0000

地址 139.17.179.92 的二进制表示为：1000 1011.0001 0001.1011 0011.0100 0000

显然与最后一个表项为最长匹配。

配置路由器接口的提示符是 (57)。

(57) A. router (config)#

B. router (config-in)#

C. router (config-intf)#

D. router (config-if) #

【答案】D

【解析】

路由器的配置操作有 3 种模式，即用户执行模式、特权模式和配置模式。在用户执行模式下，用户只能发出有限的命令，这些命令对路由器的正常工作没有影响；在特权模式下，用户可以发出丰富的命令，以便更好地控制和使用路由器；在配置模式下，用户可以创建和更改路由器的配置，对路由器的管理和配置主要在配置模式下完成。配置模式又分为全局配置模式和接口配置模式、路由协议配置模式、线路配置模式等子模式。在不同的工作模式下，路由器有不同的命令提示状态。

- Router>路由器处于用户执行模式状态，这时用户可以看到路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

- Router#路由器处于特权模式状态，在 Router>提示符下输入 enable，可进入特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

- Router(config)#路由器处于全局配置模式状态，在 Router#提示符下输入 configure terminal，可进入全局设置状态，这时可以设置路由器的全局参数。

- Router(config-if)#，router(config-line)#，router(config-rcuter)#，…路由器处于局部设置状态，这时可以设置路由器某个局部的参数。

- >路由器处于 RXBOOT 状态，在开机后 60s 内按 Ctrl+Break 组合键可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。或者进行路由器口令恢复时要进入该状态。

- 设置对话状态这是一台新路由器开机时自动进入的状态，在特权命令状态使用 setup 命令也可进入此状态。用户可以通过“yes”或者“no”选择是否使用设置对话方式对路由器进行管理和配置。

如果想知道配置了哪种路由协议，应使用的命令是(58)。

- (58) A. router>show router protocol
B. Router (config)>show ip protocol
C. router (config)>#show router protocol
D. router >show ip protocol

【答案】D

【解析】

显示路由协议的命令是 router>show ip protocol。

如果在互联网中添加了一个局域网，要用手工方式将该局域网添加到路由表中，应使用的命令是(59)。

- (59) A. router (config) >ip route 2.0.0.0 255.0.0.0 via 1.0.0.2
B. router (config) #ip route 2.0.0.0 255.0.0.0 1.0.0.2
C. router (config) #ip route 2.0.0.0 via 1.0.0.2
D. router (config) #ip route 2.0.0.0 1.0.0.2 mask 255.0.0.0

【答案】B

【解析】

用手工方式将局域网添加到路由表中使用的命令是：

router (config) #ip route 2.0.0.0 255.0.0.0 1.0.0.2

IPv6 地址的格式前缀 (FP) 用于表示(60)。为实现 IP 地址的自动配置，IPv6 主机将(61)附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址，如果通过了邻居发现协议的验证，则表明自我配置的链路本地地址是有效的。

- (60) A. 地区号 B. 地址类型或子网地址 C. 网络类型 D. 播送方式或子网号
(61) A. 32 位二进制随机数 B. 主机名字
C. 网卡 MAC 地址 D. IPv4 地址

【答案】B C

【解析】

IPv6 地址的格式前缀 (FP) 用于表示地址类型或子网地址。为了实现 IP 地址的自动配

置，IPv6 主机将 MAC 地址附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址，如果通过了邻居发现协议的验证，则表明自我配置的链路本地地址是有效的。

以下关于 CSMA/CD 协议的叙述中，正确的是 (62)。

- (62) A. 每个结点按照逻辑顺序占用一个时间片轮流发送
B. 每个结点检查介质是否空闲，如果空闲则立即发送
C. 每个结点想发就发，如果没有冲突则继续发送
D. 得到令牌的结点发送，没有得到令牌的结点等待

【答案】B

【解析】

以太网 CSMA/CD 协议的工作原理如下。工作站在发送数据之前，先监听信道上是否有别的站发送的载波信号。若有，说明信道忙；否则信道是空闲的。即使信道空闲，若立即发送仍然会发生冲突。所以需要监听算法把冲突概率减到最小。有以下 3 种监听算法：

1. 非坚持型监听算法：当一个站准备好帧，在发送之前先监听信道。

①若信道空闲，立即发送，否则转②。

②若信道忙，则后退一个随机时间，重复①。

由于随机时延后退，从而减少了冲突的概率。然而，可能会因为后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

2. 1-坚持型监听算法：当一个站准备好帧，发送之前先监听信道。

①若信道空闲，立即发送，否则转②。

②若信道忙，继续监听，直到信道空闲后立即发送。

这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间。但是，多个站同时都在监听信道时必然发生冲突。

3. P-坚持型监听算法。这种算法汲取了以上两种算法的优点，但较为复杂：

①若信道空闲，以概率 P 发送，以概率 $(1 - P)$ 延迟一个时间单位。一个时间单位等于网络传输时延。

②若信道忙，继续监听直到信道空闲，转①。

③如果发送延迟一个时间单位，则重复①。

载波监听只能减小冲突的概率，不能完全避免冲突。当两个帧发生冲突后，若继续发送，将会浪费网络带宽。为了进一步改进带宽的利用率，发送站应采取边发边听的冲突检测方法，

即：

①发送期间同时接收，并把接收的数据与站中存储的数据进行比较。（或用其他办法检测冲突）

②若比较结果一致，说明没有冲突，重复①。

③若比较结果不一致，说明发生了冲突，立即停止发送，并发送一个简短的阻塞信号（Jamming），使所有站都停止发送。

④发送 Jamming 信号后，等待一段随机长的时间，重新监听，再试图发送。

以下关于交换机获取与其端口连接设备的 MAC 地址的叙述中，正确的是（63）。

- (63) A. 交换机从路由表中提取设备的 MAC 地址
B. 交换机检查端口流入分组的源地址
C. 交换机之间互相交换地址表
D. 由网络管理员手工输入设备的 MAC 地址

【答案】B

【解析】

交换机获取与其端口连接的设备的 MAC 地址的方法是检验端口流入分组的源地址，并将其记录在地址表中。

ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是（64），选定的多路复用技术是（65）。

- (64) A. 10Mb/s B. 100Mb/s C. 20Mb/s D. 1Gb/s
(65) A. OFDM B. QPSK C. MIMO D. 64-QAM

【答案】B A

【解析】

4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是 100Mb/s，选定的多路复用技术是 OFDM（正交频分多路复用）。

用来承载多个 VLAN 流量的协议组是（66）。

- (66) A. 802.11a 和 802.1q B. ISL 和 802.1q
C. ISL 和 802.3ab D. SSL 和 802.11b

【答案】B

【解析】

802.1q 是标准的 IEEE 协议，用于区分不同的 VLAN。802.1q 在以太网帧的源 MAC 地址和 Type 字段之间插入 4 个字节的 Tag 字段(最大帧长为 1522 字节)。Tag 字段里包括 priority (0~7)和 VLAN ID (0~4095)，其中 VLAN ID=0 用于识别优先级，VLAN ID=4095 保留未用，所以最多可配置 4094 个 VLAN。

ISL (Inter-Switch Link)是 Cisco 专有的 Trunk 封装方式，是在以太网帧的最前面加上 26 字节的帧头，在以太网帧的后面加上 4 字节的 CRC 校验(最大帧长为 1548 字节)。在新加的帧头里有 15 比特用来标识 VLAN，但目前只用到低 10 位，所以最多可以区分 1024 个 VLAN。

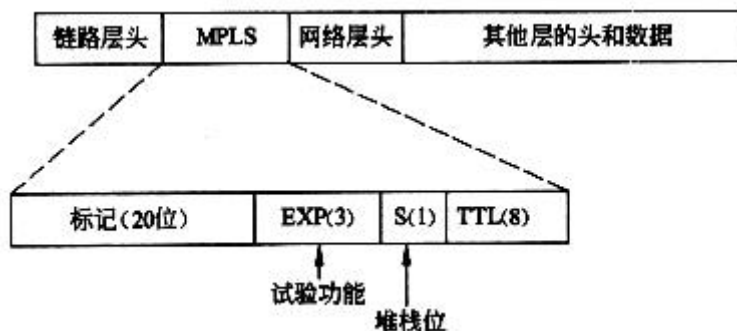
多协议标记交换 (MPLS) 是 IETF 提出的第三层交换标准，以下关于 MPLS 的叙述中，正确的是 (67)。

- (67)A. 带有 MPLS 标记的分组封装在 PPP 帧中传输
- B. 传送带有 MPLS 标记的分组之前先要建立对应的网络连接
- C. 路由器根据转发目标把多个 IP 流聚合在一起组成转发等价类
- D. MPLS 标记在各个子网中是特定分组的唯一标识

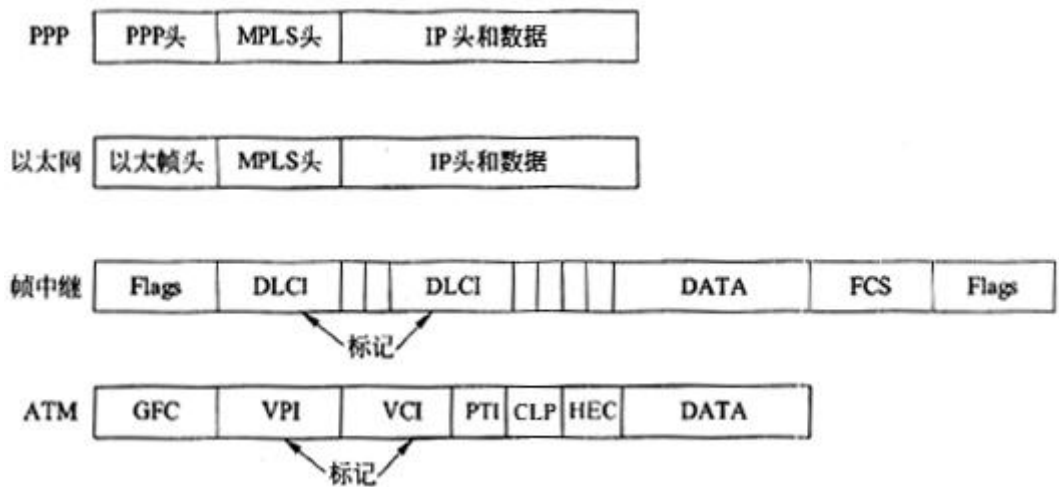
【答案】C

【解析】

IETF 开发的多协议标记交换 (MPLS)把第 2 层的链路状态信息(带宽、延迟、利用率等)集成到第 3 层的协议数据单元中，从而简化和改进了第 3 层分组的交换过程。理论上，MPLS 支持任何第 2 层和第 3 层协议。MPLS 包头的位置界于第 2 层和第 3 层之间，可称为第 2.5 层，标准格式如下图所示。



MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包甚至 ATM 信元等。可以承载 MPLS 的第 2 层协议可以是 PPP、以太帧、ATM 和帧中继等，如下图所示。



当分组进入 MPLS 网络时，标记边缘路由器（LER）就为其加上一个标记，这种标记不仅包含了路由表项中的信息（目标地址、带宽和延迟等），而且还引用了 IP 头中的源地址字段、传输层端口号和服务质量等。这种分类一旦建立，分组就被指定到对应的标记交换通路(LSP)中，标记交换路由器（LSR）将根据标记来处置分组，不再经过第 3 层转发，从而加快了网络的传输速度。

MPLS 可以把多个通信流汇聚成为一个转发等价类（FEC）。LER 根据目标地址和端口号把分组指派到一个等价类中，在 LSR 中只需根据等价类标记查找标记信息库 (LIB)，确定下一跳的转发地址。这样使得协议更具伸缩性。MPLS 标记具有局部性，一个标记只是在一定的传输域中有效。

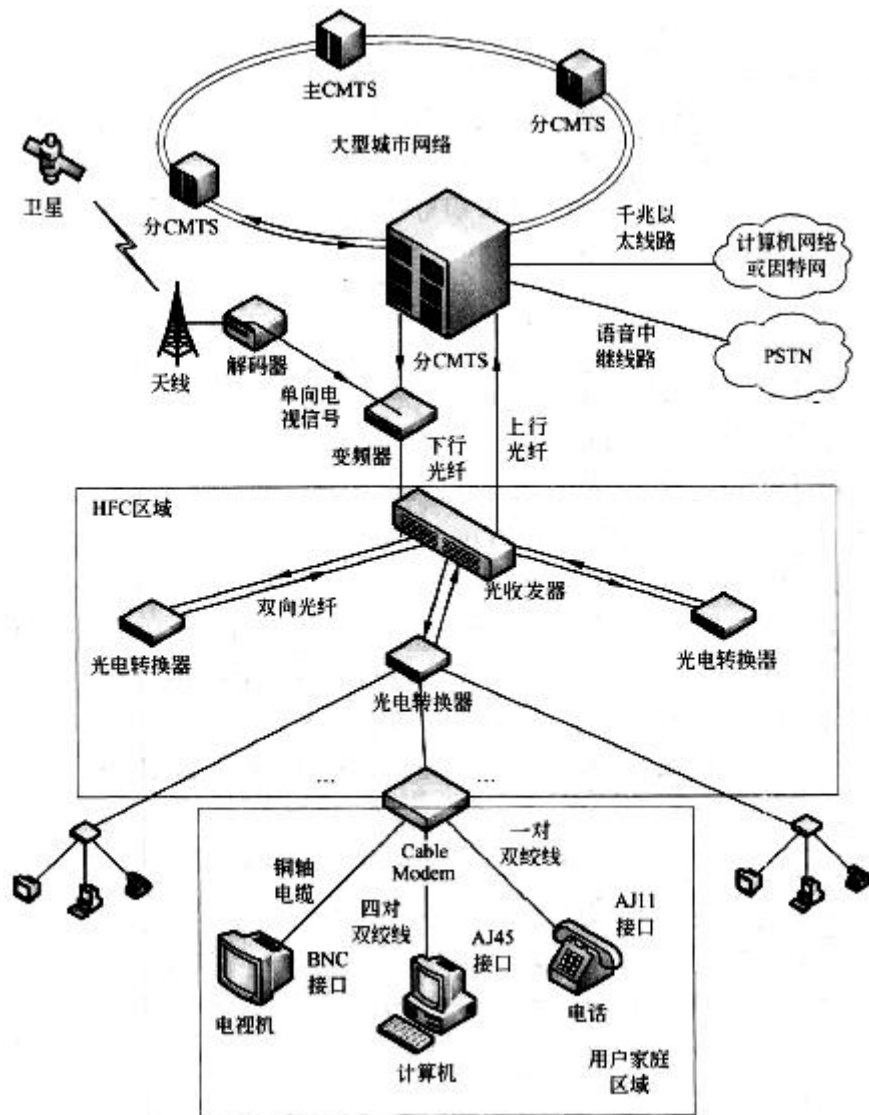
通过 HFC 网络实现宽带接入，用户端需要的设备是 (68)，局端用于控制和管理用户的设备是 (69)。

- (68) A. Cable Modem B. ADSL Modem C. OLT D. CMTS
- (69) A. Cable Modem B. ADSL Modem C. OLT D. CMTS

【答案】 A D

【解析】

通过 HFC 网络实现宽带接入，用户端需要的设备是 Cable Modem, 局端用于控制和管理用户的设备是 CMTS，如下图所示。



在层次化局域网模型中，以下关于核心层的叙述，正确的是 (70)。

- (70) A. 为了保障安全性，对分组要进行有效性检查
- B. 将分组从一个区域高速地转发到另一个区域
- C. 由多台二、三层交换机组成
- D. 提供多条路径来缓解通信瓶颈

【答案】B

【解析】

在层次化局域网模型中，核心层的主要功能是将分组从一个区域高速地转发到另一个区域。核心层是因特网络的高速骨干，由于其重要性，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能快速适应变化。在设计核心层设备的功能时，应尽量避免使用数据包

过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。汇聚层是核心层和接入层的分界点，应尽量将资源访问控制、核心层流量的控制等都在汇聚层实施。汇聚层应向核心层隐藏接入层的详细信息，汇聚层向核心层路由器进行路由宣告时，仅宣告多个子网地址汇聚而形成的一个网络。另外，汇聚层也会对接入层屏蔽网络其他部分的信息，汇聚层路由器可以不向接入路由器宣告其他网络部分的路由，而仅仅向接入设备宣告自己为默认路由。

接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户之间的互访需要，并且为这些访问提供足够的带宽。接入层还应该适浩负责一些用户管理功能，包括地址认证、用户认证和计费管理等内容。接入层还负责一些信息的用户信息收集工作，例如用户的 IP 地址、MAC 地址和访问日志等信息。

The Dynamic Host Configuration Protocol provides configuration parameters to Internet (71). DHCP consists of two components: a (72) for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver (73) parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a (74) IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time. In "manual allocation", a client's IP address is assigned by the network (75), and DHCP is used simply to convey the assigned address to the client.

- | | | | |
|-------------------|--------------|------------------|------------------|
| (71)A. switch | B. terminal | C. hosts | D. users |
| (72)A. router | B. protocol | C. host | D. mechanism |
| (73)A. control | B. broadcast | C. configuration | D. transmission |
| (74)A. permanent | B. dynamic | C. correction | D. session |
| (75)A. controller | B. user | C. host | D. administrator |

【答案】C B C A D

【解析】

动态主机配置协议向因特网主机提供配置参数。DHCP 由两个部分组成：一个用于从 DHCP 服务器向主机提交主机专用配置参数的协议，以及一种给主机分配网络地址的机制。DHCP

建立在客户机-服务器模式上，专用的 DHCP 服务器负责分配网络地址，并且向动态配置的主机提交配置参数。DHCP 支持 3 种 IP 地址分配机制。在“自动分配”方式中，DHCP 为客户指定一个固定的 IP 地址。在“动态分配”模式中，DHCP 给客户分配一个仅在一定时间段内有效的 IP 地址。在“手工分配”模式中，客户的 IP 地址是由网络管理员指定的，DHCP 只是把分配的地址转送给客户。

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。

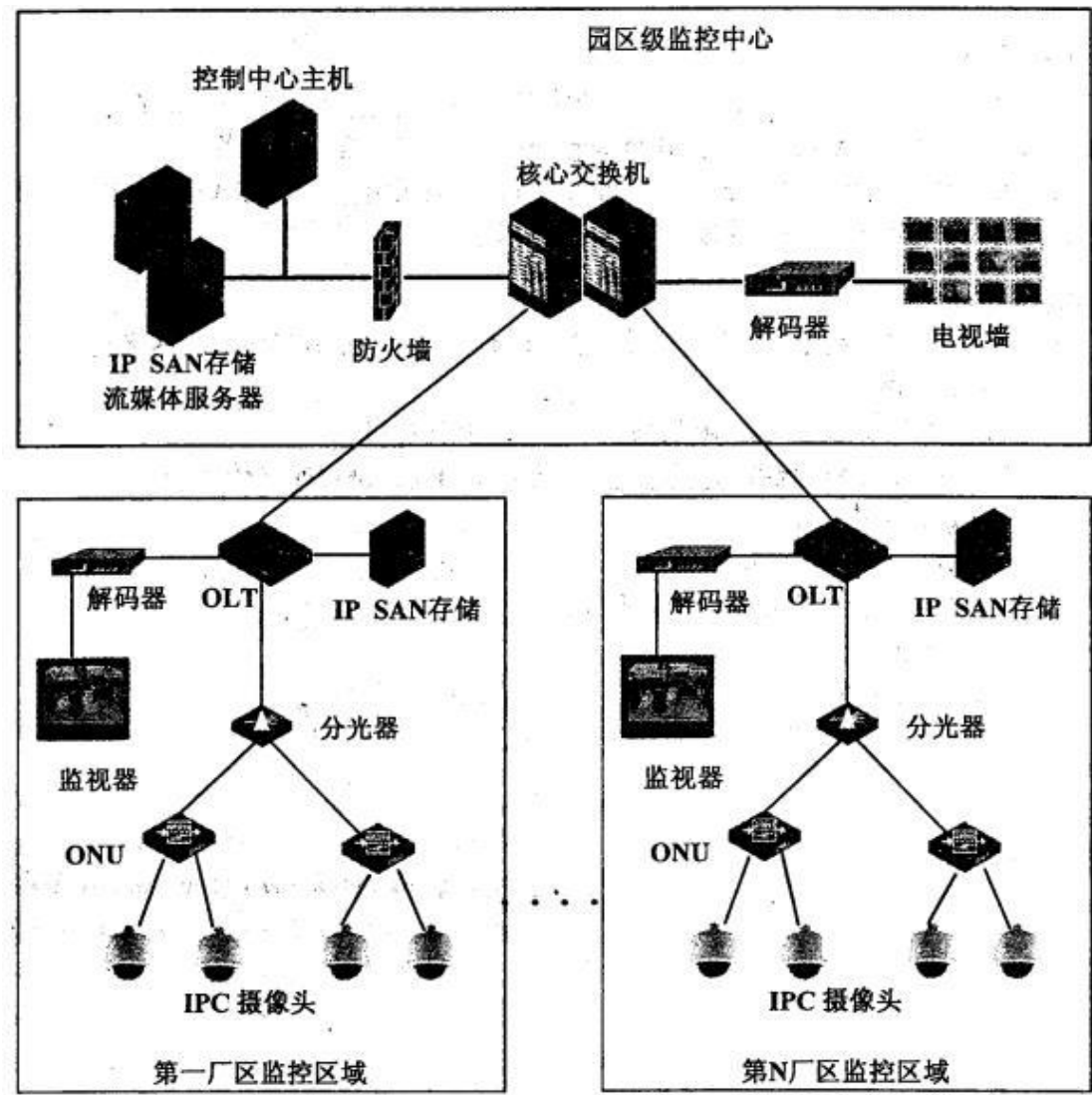


图 1-1

【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 IP SAN，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)。

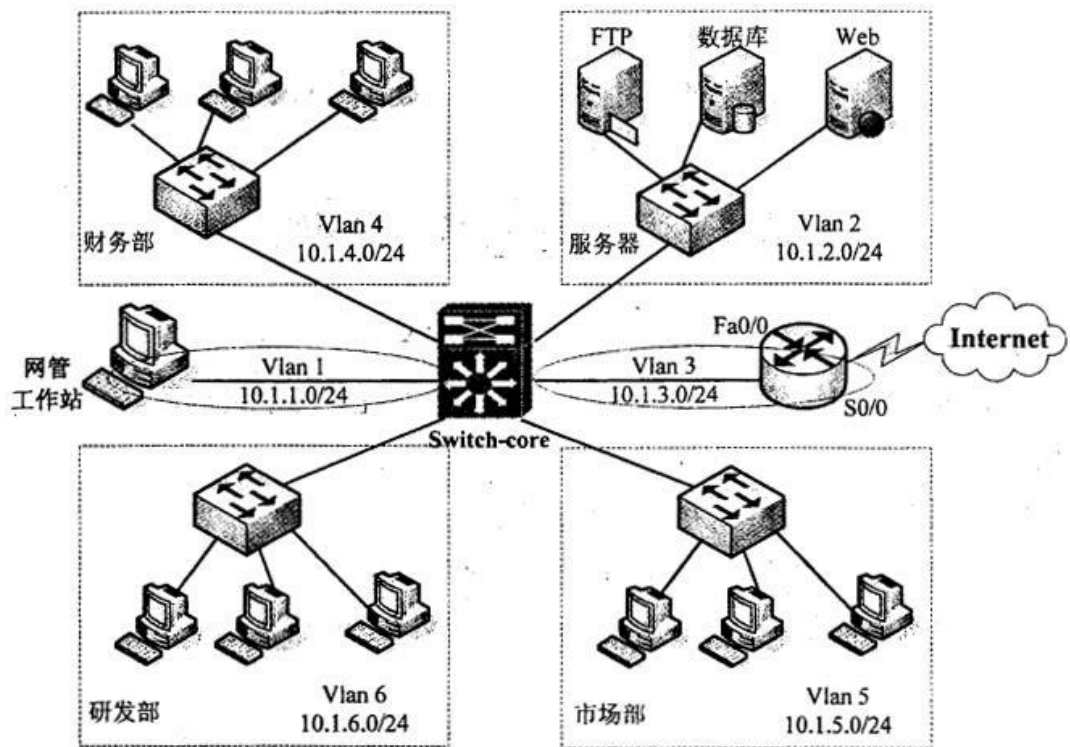


图 2-1 某企业网络拓扑图

【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 telnet 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

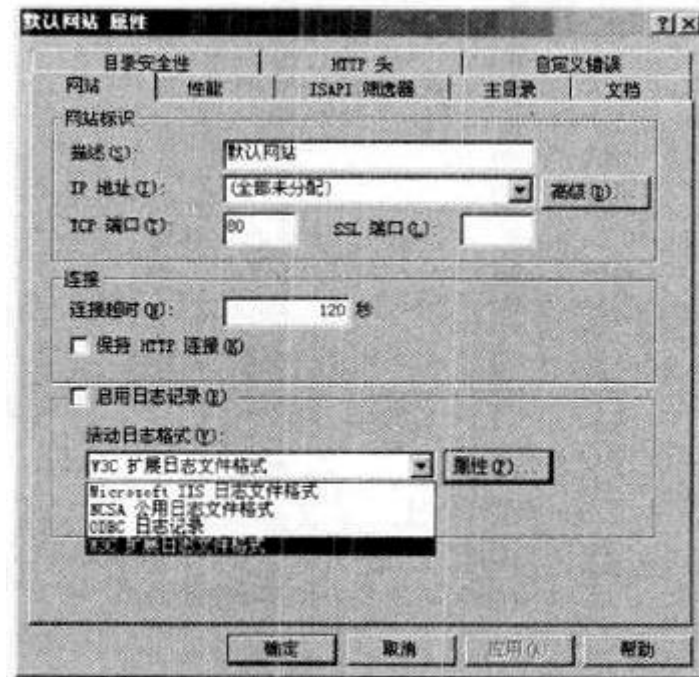


图 3-2

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。

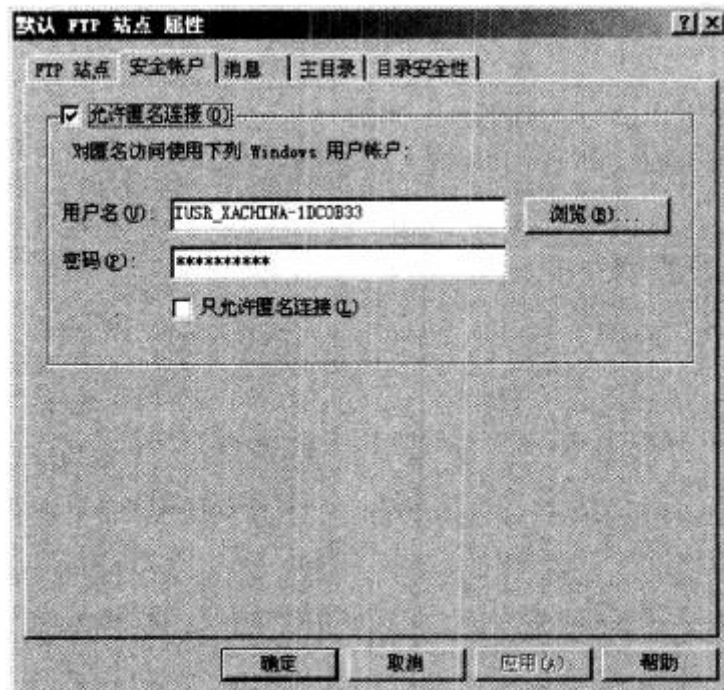


图 3-3

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。

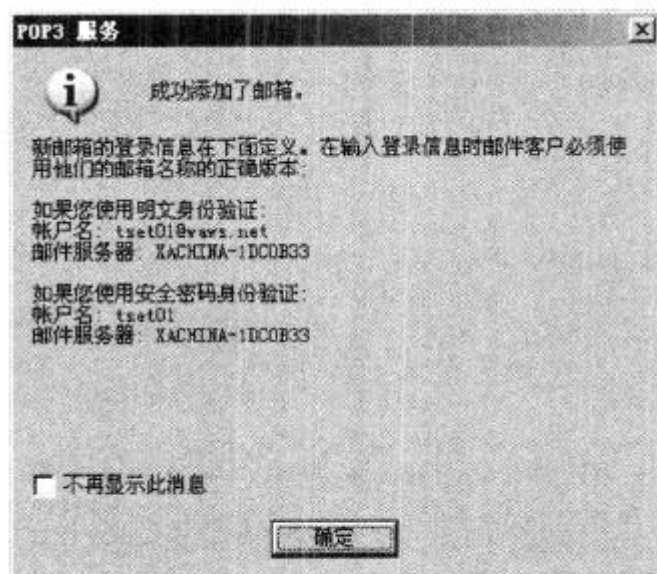


图 3-4

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送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 。

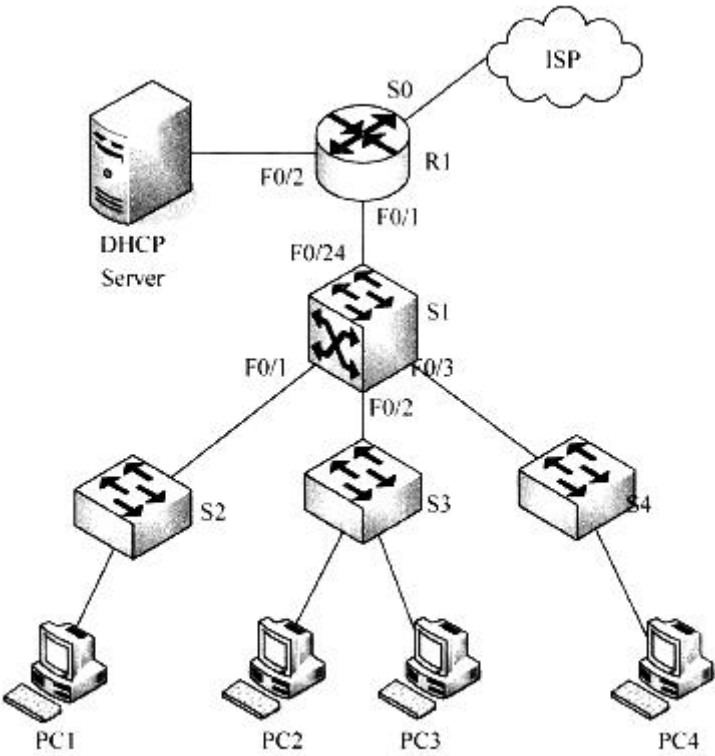


图 4-1

【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)
DHCP Server	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 Virtual 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。