

在程序执行过程中, Cache 与主存的地址映像由 (1)。

- (1) A. 硬件自动完成 B. 程序员调度
C. 操作系统管理 D. 程序员与操作系统协同完成

【答案】A

【解析】 本题考查计算机系统基础知识。

Cache 的工作是建立在程序与数据访问的局部性原理上。经过对大量程序执行情况的结果分析：在一段较短的时间间隔内程序集中在某一较小的内存地址空间执行，这就是程序执行的局部性原理。同样，对数据的访问也存在局部性现象。

为了提高系统处理速度才将主存部分存储空间中的内容复制到工作速度更快的 Cache 中，同样为了提高速度的原因，Cache 系统都是由硬件实现的。

指令寄存器的位数取决于(2)。

- (2) A. 存储器的容量 B. 指令字长 C. 数据总线的宽度 D. 地址总线的宽度

【答案】B

【解析】 本题考查计算机系统基础知识。

指令寄存器是 CPU 中的关键寄存器，其内容为正在执行的指令，显然其位数取决于指令字长。

若计算机存储数据采用的是双符号位（00 表示正号、11 表示负号），两个符号相同的数相加时，如果运算结果的两个符号位经（3）运算得 1，则可断走这两个数相加的结果产生了溢出。

- (3) A. 逻辑与 B. 逻辑或 C. 逻辑同或 D. 逻辑异或

【答案】 D

【解析】 本题考查计算机系统基础知识。

当表示数据时并规定了位数后，其能表示的数值范围就确定了，在两个数进行相加运算的结果超出了该范围后，就发生了溢出。在二进制情况下，溢出时符号位将变反，即两个正数相加，结果的符号位是负数，或者两个负数相加，结果的符号位是正数。采用两个符号位时，溢出发生后两个符号位就不一致了，这两位进行异或的结果一定为 1。

若某计算机字长为 32 位，内存容量为 2GB，按字编址，则可寻址范围为 (4)。

(4) A. 1024M

B. 1GB

C. 512M

D. 2GB

【答案】C

【解析】本题考查计算机系统基础知识。

内存容量 $2GB=2*1024*1024*1024*8$ 位，按字编址时，存储单元的个数为 $2*1024*1024*1024*8/32=512*1024*1024$ ，即可寻址范围为 512MB。

视频信息是连续的图像序列，(5)是构成视频信息的基本单元。

(5) A. 帧

B. 场

C. 幅

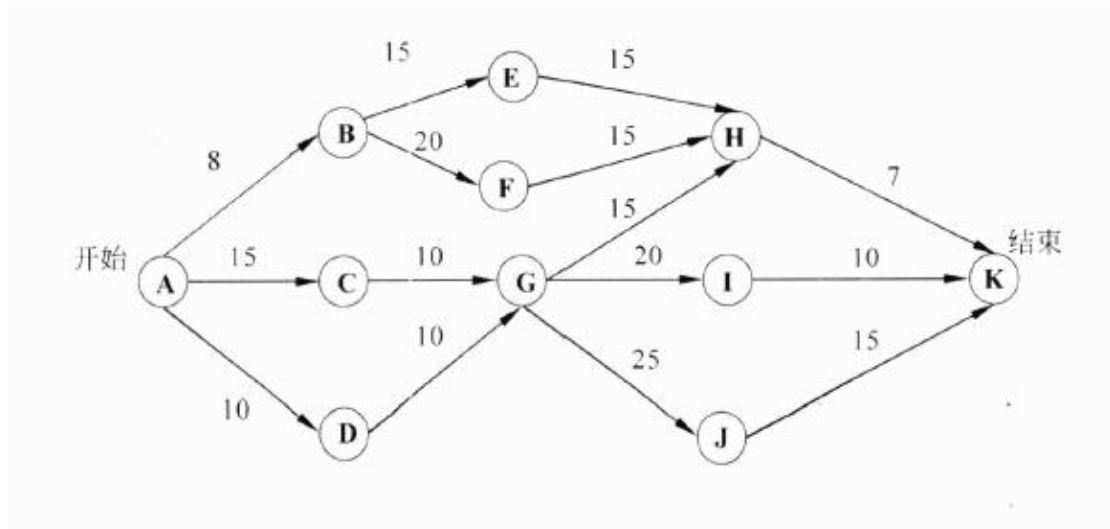
D. 像素

【答案】A

【解析】本题考查多媒体方面的基础知识。

视频信息是指活动的、连续的图像序列。一幅图像称为一帧，帧是构成视频信息的基本单元。

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，则里程碑 (6) 在关键路径上。若在实际项目进展中，活动 AD 在活动 AC 开始 3 天后才开始，而完成活动 DG 过程中，由于有临时事件发生，实际需要 15 天才能完成，则完成该项目的最短时间比原计划多了 (7) 天。



(6) A. B

B. C

C. D

D. I

(7) A. 8

B. 3

C. 5

D. 6

【答案】B B

【解析】本题考查软件项目管理的基础知识。

根据关键路径法，计算出关键路径为 A—C—G—J—K，关键路径长度为 65。因此里程碑 C 在关键路径上，而里程碑 B、D 和 I 不在关键路径上。

若完成活动 DG 需要 15 天，则相当于 A—D—G—I—K 也是一个关键路径，而且活动 AD 推迟了三天才能完成，此时，完成项目的最短时间应该是 68 天，比原来的最短时间 65 天多了 3 天。

为说明某一问题，在学术论文中需要引用某些资料。以下叙述中错误的是(8)

- (8) A. 既可引用发表的作品，也可引用未发表的作品
- B. 只能限于介绍、评论作品
- C. 只要不构成自己作品的主要部分，可适当引用资料
- D. 不必征得原作者的同意，不需要向他支付报酬

【答案】A

【解析】本题考查知识产权方面的基础知识。

选项 A “既可引用发表的作品，也可引用未发表的作品”的说法显然是错误的。因为，为说明某一问题，在学术论文中需要引用某些资料必须是已发表的作品，但只能限于介绍、评论作品，只要不构成自己作品的主要部分，可适当引用资料，而不必征得原作者的同意，不需要向他支付报酬。

程序运行过程中常使用参数在函数（过程）间传递信息，引用调用传递的是实参的(9)。

- (9) A. 地址
- B. 类型
- C. 名称
- D. 值

【答案】A

【解析】本题考查程序语言基础知识。

进行函数调用时，常需要将调用环境中的数据传递给被调用函数，作为输入参数由被调用函数处理，基本的调用方式为值调用（或传值调用）和引用调用。其中，值调用方式下是将实参的值单向地传递给被调用函数的形参，引用调用方式下通过将实参的地址传递给形参，在被调用函数中通过指针实现对实参变量数据的间接访问和修改，从而达到将修改后的值“传回来”的效果。

算术表达式 $a+(b-c)*d$ 的后缀式是(10)（-、+、*表示算术的减、加、乘运算，运算符的优先级和结合性遵循惯例）。

- (10) A. $bc-d*a+$ B. $abc-d*+$ C. $ab+c-d*$ D. $abcd-*+$

【答案】B

【解析】本题考查程序语言基础知识。

后缀式的特点是将运算符号写在运算数的后面。对于表达式，其计算次序是相减、相乘、相加，其后缀式为“ $abc-d*+$ ”。

帧中继网络的虚电路建立在 (11)，这种虚电路的特点是 (12)。

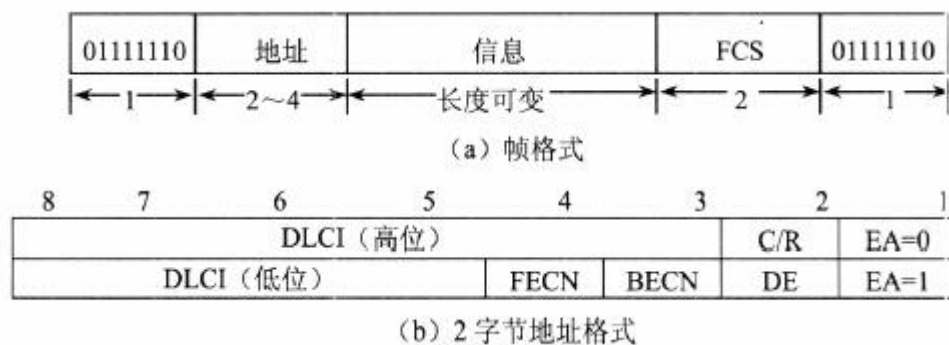
- (11) A. 数据链路层 B. 网络层 C. 传输层 D. 会话层

- (12) A. 没有流量控制功能， 也没有拥塞控制功能
B. 没有流量控制功能， 但具有拥塞控制功能
C. 具有流量控制功能， 但没有拥塞控制功能
D. 具有流量控制功能， 也具有拥塞控制功能

【答案】A B

【解析】

帧中继 (FrameRelay, FR) 是作为综合业务数字网 (ISDN) 的一种承载业务而开发的。按照 ISDN 的体系结构，帧中继在第二层建立虚电路，用帧方式承载数据业务，因而第三层被省略了。在用户平面，通过 LAP-F (Q. 922) 帧传送用户数据。LAP-F 类似于 LAP-B，但是省去了控制字段，其帧格式如下图所示。



从图 1 可以看出，帧头和帧尾都是一个字节的帧标志字段，其编码为“01111110”，与 HDLC 一样。信息字段长度可变，默认的最大长度是 1600 字节。帧效验序列也与 HDLC 相同，但是中间系统并不进行差错校验，只是接收端才用这个字段对整个帧进行校验。RF 没有流量控制功能，表现在帧结构上是没有发送顺序号和接收顺序号字段。地址字段有 3 种格式，图 1 所示为 2 字节地址格式，其中的 DLCI 为虚电路号，FECN 和 BECN 分别为向前拥塞和向后拥塞控制字段，而 DE 为 1 时表示优先丢弃，帧中继用这些机制实现拥塞控制。

循环冗余校验标准 CRC-16 的生成多项式为 $G(x)=x^{16}+x^{15}+x^2+1$, 它产生的校验码是 (13) 位。接收端发现错误后采取的措施是 (14)。

- (13) A. 2 B. 4 C. 16 D. 32
- (14) A. 自动纠错 B. 报告上层协议 C. 重新生成数据 D. 自动请求重发

【答案】C D

【解析】

CRC-16 的 $G(x)$ 为 x 的十六次方多项式, 所以产生的校验码是 16 位。CRC 校验属于后向纠错 (Backward Error Correction, BEC), 接收端发现错误后自动请求发送方重新发送数据。相反, 对于前向纠错 (Forward Error Correction, FEC), 则是由接收端利用纠错码自动进行检查和纠正错误。

设信道带宽为 3000Hz, 信噪比为 30dB, 则信道可达到的最大数据速率约为 (15) b/s。

- (15) A. 10000 B. 20000 C. 30000 D. 40000

【答案】C

【解析】

按照香农 (Shannon) 定理, 噪声信道的极限数据速率由下面的公式计算:

本题中, $F=3000\text{Hz}$, 信噪比为 30dB, 即 $S/N=1000$, 所以

$C=3000 \times \log_2(1+1000) \approx 30000\text{b/s}$ 。

下面哪个字段包含在 TCP 头部和 UDP 头部? (16)

- (16) A. 发送顺序号 B. 窗口 C. 源端口 D. 紧急指针

【答案】C

【解析】

TCP 段头如下图 1 所示, UDP 头如下图 2 所示, 可以看出, 只有源端口字段出现在两个头部中。

源 端 口					目 标 端 口				
发 送 顺 序 号									
接 收 顺 序 号									
偏置值	保留	URG	ACK	PSH	RST	SYN	FIN	窗 口	
检 查 和							紧 急 指 针		
任选项+补丁									
用 户 数 据									

图 1 TCP 段头格式

源端口	目标端口
段 长	检查和

图 2 UDP 头

下面的选项中，与服务质量管理有关的协议是 (17)，这种协议的主要特点是 (18)。

- (17) A. RSVP B. VTP C. ATM D. UDP
- (18) A. 由接收方向路由器预约资源 B. 由发送方向接收方预约资源
- C. 由发送方向路由器预约资源 D. 由接收方向发送方预约资源

【答案】A A

【解析】

本题的选项中，RSVP 是资源预约协议，根据用户要求的服务质量，由连接的接收方（或下游结点）向中间路由器（或上游结点）预约资源。VTP 是 VLAN 中继协议（VLAN Trunking Protocol），用于交换机之间共享 VLAN 配置信息，ATM 是一种信元交换网，而 UDP 是传输层协议，这些都与服务质量无关。

CHAP 协议是 PPP 链路中采用的一种身份认证协议，这种协议采用 (19) 握手方式周期性地验证通信对方的身份，当认证服务器发出一个挑战报文时，则终端就计算该报文的 (20) 并把结果返回服务器。

- (19) A. 两次 B. 三次 C. 四次 D. 周期性
- (20) A. 密码 B. 补码 C. CHAP 值 D. HASH 值

【答案】B D

【解析】

PPP 认证协议是可选的，分为两种。

口令验证协议 (Password Authentication Protocol, PAP) 提供了一种简单的两次握手认证方法, 由终端发送用户标识和口令字, 等待服务器的应答, 如果认证不成功, 则终止连接。这种方案采用明文方式发送密码, 可能会被第三方窃取。

质询握手认证协议 (Challenge Handshake Authentication Protocol, CHAP) 采用三次握手方式周期地验证对方的身份。PPP 链路建立后, 认证服务器首先发送一个挑战报文(随机数), 终端计算该报文的 Hash 值并把结果返回服务器, 然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较, 如果匹配, 则认证通过, 否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与, 而密钥是不通过网络传送的, 所以 CHAP 是更安全的认证机制。在后续的通信过程中, 每经过一个随机的间隔, 这个认证过程都可能被重复, 以缩短入侵者进行持续攻击的时间。

IP 头和 TCP 头的最小开销合计为 (21) 字节, 以太网最大帧长为 1518 字节, 则可以传送的 TCP 数据最大为 (22) 字节。

- | | | | |
|--------------|---------|---------|---------|
| (21) A. 20 | B. 30 | C. 40 | D. 50 |
| (22) A. 1434 | B. 1460 | C. 1480 | D. 1500 |

【答案】C B

【解析】

IP 头最少 20 个字节 (不计任选字段), TCP 头最少也是 20 个字节 (不计任选字段), 最小合计 40 个字节。以太网帧最大负载长度为 1500 字节, 另外帧头和帧尾还有 18 个字节。封装在以太帧中的 TCP 数据最多可以为 1460 字节。

VLAN 中继协议 (VTP) 的作用是 (23)。按照 VTP 协议, 交换机的运行模式有 (24)。如果要启动 VTP 动态修剪, 则 (25)。

- (23) A. 启动 VLAN 自动配置过程
B. 减少 VLAN 配置信息的冲突
C. 让同一管理域中的所有交换机共享 VLAN 配置信息
D. 建立动态配置 VLAN 的环境
- (24) A. 服务器模式, 客户机模式, 透明模式 B. 服务器模式, 客户机模式, 终端模式
C. 路由器模式, 交换机模式, 终端模式 D. 路由器模式, 交换机模式, 透明模式
- (25) A. 管理域中的交换机必须配置成一个服务器和多个客户机

- B. 管理域中的所有交换机都不能配置成终端模式
- C. 管理域中的所有交换机都不能配置成透明模式
- D. 管理域中的所有交换机都必须配置成服务器

【答案】C A D

【解析】

VLAN 中继协议 (VLAN Trunking Protocol, VTP) 是 Cisco 公司的专利协议。按照 VTP 协议, 交换机的运行模式分为 3 种:

- ①服务器模式 (Server): 在此模式下能创建、添加、删除和修改 VLAN 配置, 并从中继端口发出 VTP 组播帧, 把配置信息分发到整个管理域中的所有交换机
- ②客户机模式 (Client): 在此模式下不允许创建、修改或删除 VLAN, 但可以监听本管理域中其他交换机的 VTP 组播信息, 并据此修改自己的 VLAN 配置。
- ③透明模式 (Transparent): 在此模式下可以进行 VLAN 配置, 但配置信息不会传播到其他交换机。在透明模式下, 可以接收和转发 VTP 帧, 但是并不能根据 VTP 帧更新自己的 VLAN 配置。

通过 VTP 协议, 提供了在一台交换机上对整个管理域(跨不同介质类型)进行 VLAN 配置的方法, 使得同一管理域中的所有交换机共享 VLAN 配置信息。

在默认情况下, 所有交换机通过中继链路连接在一起, 如果 VLAN 中的任何设备发出一个广播包、组播包、或者一个未知的单播数据包, 交换机都会将其洪泛到所有与源 VLAN 端口相关的各个输出端口上 (包括中继端口)。在很多情况下, 这种洪泛转发是必要的, 特别是在 VLAN 跨越多个交换机的情况下。然而, 如果相邻的交换机上不存在源 VLAN 的活动端口, 则这种洪泛发送的数据包是无用的。为了解决这个问题, 可以使用静态或动态修剪的方法。所谓静态修剪, 就是手工剪掉中继链路上不活动的 VLAN。但是, 手工修剪方式容易出错, 并且对任何 VLAN 配置的变化, 都必须重新进行手工修剪。VTP 动态修剪允许交换机从中继连接上自动剪掉不活动的 VLAN, 使得中继链路上共享的 VLAN 都是活动的。

动态修剪要求 VTP 域中的所有交换机都必须配置成服务器。因为在服务器模式下, 交换机可以改变 VLAN 配置, 也可以接受 VLAN 配置的改变。

在下面的标准中, 定义快速生成树协议的是 (26), 支持端口认证的协议是 (27)。

- | | | | |
|--------------------|---------------|---------------|---------------|
| (26) A. IEEE802.1d | B. IEEE802.1w | C. IEEE802.1s | D. IEEE802.1x |
| (27) A. IEEE802.1d | B. IEEE802.1w | C. IEEE802.1s | D. IEEE802.1x |

【答案】B D

【解析】

生成树协议（STP）删除了交换机之间的网络环路，同时允许一定的冗余连接存在，以增加带宽，提高网络连接的可靠性。1990 年，IEEE 根据 DEC 公司的 STP 协议开发了 802.1d 标准。

1998 年，IEEE 颁布了快速生成树协议（RSTP）802.1w，这种协议在网络拓扑改变时可以加快生成树收敛的速度。在原来的 STP 协议中，生成树的收敛时间可能达到 30~50 秒，而 RSTP 的收敛时间通常只有 6 秒钟（默认 $hello\ time=2$ 秒）。最新的 IEEE802.1d-2004 标准包含了 RSTP 的内容，废除了原来的 STP 协议。

如果交换是以太网中有多个 VLAN 存在，可以为每个 VLAN 配置一个生成树。多生成树协议（Multiple Spanning Tree Protocol, MSTP）是 RSTP 在 VLAN 环境下的扩展，原来定义在 IEEE802.1s 中，后来被合并到新标准 IEEE802.1q-2003 中。这种“每个 VLAN 的多生成树协议”为每一组 VLAN 配置一个单独的生成树，并预留一个可用的替代通路，而将其他通路置于阻塞状态。MSTP 在一个 MST 区域中通过传播通知信息而维护多个 MST 实例。多个 MST 区域（或者其他的 STP 网桥）之间则通过公共生成树（common spanning tree, CST）互连，CST 就是 STP 协议的生成树。MSTP 协议把所有生成树信息包装在单一的 BPDU 格式中，并且保证与 STP 和 RSTP 协议向后兼容，所以 RSTP 网桥也可以解释 MSTP 的 BPDU。

IEEE802.1x 在局域网中实现基于端口的用户认证和访问控制。

在某路由器上查看路由信息，结果如下所示。其中标志“S”表明这条路由是（28）。

```

S      192.168.0.0/24 is subnetted, 1 subnets
        192.168.1.0 [1/0] via 10.1.1.1
C      10.0.0.0/24 is subnetted, 1 subnets
        10.1.1.0 is directly connected, Ethernet0
```

(28) A. 源路由 B. 静态路由 C. 发送路由 D. 快捷路由

【答案】B

【解析】本题考查路由器配置命令。

查看路由信息结果中，标记 S 表示静态路由，标记 C 表示直联，标记 R 表示采用 RIP 路由协议。

序;/lib 目录里存放着系统最基本的动态链接共享库,其作用类似于 Windows 里的 .dll 文件;
/etc 主要存放了系统配置方面的文件; /bin 目录存放了标准的 (或者说是缺省的) linux
的工具, 比如像 “ls”、“vi” 还有 “more” 等等。

Linux 中, 下列 (32) 命令可以更改一个文件的权限设置。

- (32) A. attrib B. file C. chmod D. change

【答案】C

【解析】 本题考查 Linux 操作系统中的文件及其权限。

Attrib 是 Windows 中给文件加系统属性的命令;
file 是 Linux 操作系统中检测文件类型的命令;
chmod 是 Linux 操作系统中赋予权限的命令, 使用方式为: chmod [-cfvR] [-help] [—
version] modefile.”。

以下关于 DNS 服务器的说法中, 错误的是 (33)

- (33) A. DNS 的域名空间是由树状结构组织的分层域名
B. 转发域名服务器位于域名树的顶层
C. 辅助域名服务器定期从主域名服务器获得更新数据
D. 转发域名服务器负责所有非本地域名的查询

【答案】B

【解析】 本题考查 DNS 服务器相关概念。

域名系统通过层次结构的分布式数据库建立了一致性的名字空间, 用来定位网络资源。
DNS 的逻辑结构是一个分层的域名树, Internet 网络信息中心管理着域名树的根, 称为根域。
根域下面是顶级域, 分为国家顶级域和通用顶级域。国家顶级域名包含 243 个国家和地区代
码, 例如 cn 代表中国, uk 代表英国等。

转发域名服务器负责所有非本地域名的查询。当 DNS 服务器收到查询请求后, 首先在自
己的区域文件中查找, 再在高速缓存中查找。如果查不到, 可能是因为该服务器不是请求域
的授权服务器, 并且以前查询的缓存中没有需要的记录, 这时 DNS 服务器必须向转发域名服
务器发送请求。

当主域名服务器关闭、出现故障或负载过重时, 辅助域名服务器作为备份服务器提供域
名解析服务。辅助服务器从主域名服务器获得授权, 并定期向主服务器询问是否有新数据,

如果有则调入并更新域名解析数据，以达到与主域名服务器同步的目的。

某单位架设了域名服务器来进行本地域名解析，在客户机上运行 nslookup 查询某服务器名称时能解析出 IP 地址，查询 IP 地址时却不能解析出服务器名称，解决这一问题的方法是 (34)。

- (34)A. 在 DNS 服务器区域上允许动态更新
B. 在客户机上采用 ipconfig/flushdns 刷新 DNS 缓存
C. 在 DNS 服务器上为该服务器创建 PTR 记录
D. 重启 DNS 服务

【答案】C

【解析】本试题考查 DNS 服务相关知识。

查询服务器名称时能解析出 IP 地址，而查询 IP 地址时却不能解析出服务器名称，说明可正向解析不能反向解析，因此须在 DNS 服务器上为该服务器创建反向解析 (PTR) 记录。

下列关于 DHCP 配置的叙述中，错误的是 (35)。

- (35)A. 在 Windows 环境下，客户机可用命令 ipconfig/renew 重新申请 IP 地址
B. 若可供分配的 IP 地址较多，可适当增加地址租约期限
C. DHCP 服务器不需要配置固定的 IP 地址
D. DHCP 服务器可以为不在同一网段的客户机分配 IP 地址

【答案】C

【解析】本试题考查 DHCP 服务器配置相关知识。

在 Windows 环境下，客户机可用命令 ipconfig/release 释放 IP 地址，用命令 ipconfig/renew 重新申请 IP 地址；在 DHCP 服务器的地址租约期限设置中，可依据可供分配 IP 地址的多少，适当调整地址租约期限；DHCP 服务器需要有固定的 IP 地址，便于和客户机之间通过 DHCP 协议报文分配 IP 地址；可以通过在路由器上设置中继代理，为不在同一网段的客户机分配 IP 地址。

SMTP 协议用于 (36) 电子邮件。

- (36)A. 接收 B. 发送 C. 丢弃 D. 阻挡

【答案】B

【解析】 本题考查 SMTP 协议的功能。

SMTP 协议的功能是发送电子邮件，POP3 协议的功能是接收电子邮件。

配置 POP3 服务器时，邮件服务器中默认开放 TCP 的(37)端口。

(37) A. 21 B. 25 C. 53 D. 110

【答案】 D

【解析】 本题考查 POP3 协议的相关知识。

不同的协议采用不同的 TCP 端口号，默认情况下，Web 服务器的端口号为 80;FTP 服务器的端口号为 20 和 21，Telnet 的端口号为 23，POP3 的端口号为 110。

在 Windows 的 cmd 命令窗口中输入 (38) 命令可以用来诊断域名系统基础结构的信息和查看 DNS 服务器的 IP 地址。

(38) A. DNSserver B. DNSconfig C. Nslookup D. DNSnamed

【答案】 C

【解析】 本试题考查 Windows 操作系统中网络管理命令的使用及相关知识。

通常采用 Nslookup 命令来诊断域名系统基础结构的信息和查看 DNS 服务器的 IP 地址。

计算机网络机房建设过程中，为了屏蔽外界的干扰、漏电及电火花等，要求所有计算机网络设备的机箱、机柜、机壳等都需接地，该接地系统称为安全地，安全地接地电阻要求小于(39)。

(39) A. 1 Ω B. 4 Ω C. 5 Ω D. 10 Ω

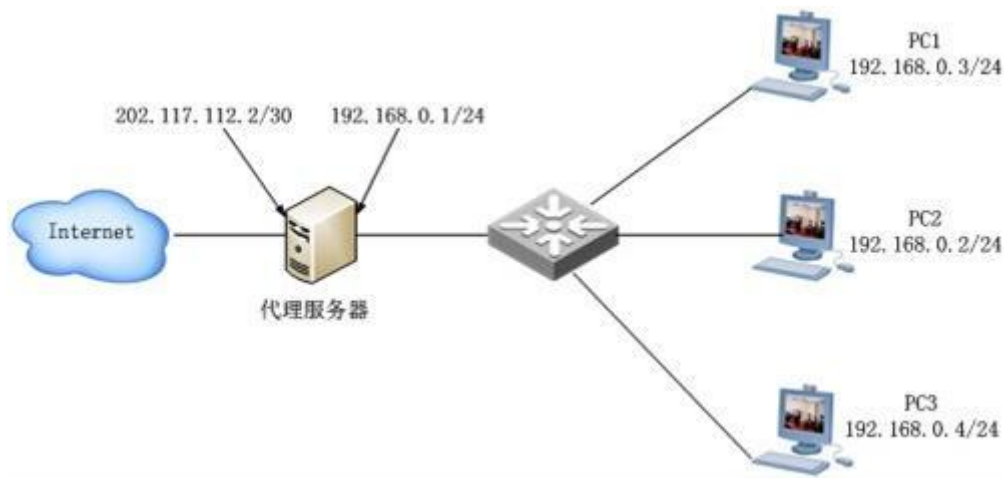
【答案】 B

【解析】 本题考查机房建设过程中需注意的问题。

通常标准接地电阻规范要求：

- ①独立的防雷保护接地电阻应小于等于 10 Ω ；
- ②独立的安全保护接地电阻应小于等于 4 Ω ；
- ③独立的交流工作接地电阻应小于等于 4 Ω ；
- ④独立的直流工作接地电阻应小于等于 4 Ω ；
- ⑤防静电接地电阻一般要求小于等于 100 Ω 。
- ⑥共用接地体（联合接地）应不大于接地电阻 1 Ω 。

某单位局域网配置如下图所示，PC2 发送到 Internet 的报文源 IP 地址为(40)。



(40) A. 192. 168. 0. 2 B. 192. 168. 0. 1 C. 202. 117. 112. 1 D. 202. 117. 112. 2

【答案】D

【解析】 本题考查局域网配置中 IP 地址设置相关问题。

PC2 发送到 Internet 上的报文经代理服务器转换后, 源 IP 地址变成代理服务器的出口 IP 地址, 即 202.117.112.2。

下面 ACL 语句中，表达“禁止外网和内网之间互相 ping”的是 (41)。

(41) A. access-list 101 permit any any
B. access-list 101 permit icmp any any
C. access-list 101 deny any any
D. access-list 101 deny icmp any any

【答案】D

【解析】本试题考查 ACL 语句规范及 ICMP 命令。

Ping 命令是 ICMP 报文的一个子集，禁止内外网用户之间采用 ICMP 协议即可禁止外网和内网之间互相 ping。

下列网络攻击行为中，属于 DoS 攻击的是 (42)。

(42) A. 特洛伊木马攻击 B. SYNflooding 攻击
C. 端口欺骗攻击 D. IP 欺骗攻击

【答案】B

【解析】 本题考查网络安全相关知识。

特洛伊木马是附着在应用程序中或者单独存在的一些恶意程序，它可以利用网络远程控制网络另一端的安装有服务端程序的主机，实现对被植入了木马程序的计算机的控制，或者窃取被植入了木马程序的计算机上的机密资料。

拒绝服务攻击通过网络的内外用户来发动攻击。内部用户可以通过长时间占用系统的内存、CPU 处理时间使其他用户不能及时得到这些资源，而引起拒绝服务攻击；外部黑客也可以通过占用网络连接使其他用户得不到网络服务。SYNFlooding 攻击以多个随机的源主机地址向目的路由器发送 SYN 包，在收到目的路由器的 SYNACK 后并不回应，于是目的路由器就为这些源主机建立大量的连接队列，由于没有收到 ACK 一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务，甚至导致路由器崩溃。服务器要等待超时才能断开已分配的资源，所以 SYNFlooding 攻击是一种 DoS 攻击。

端口欺骗攻击是采用端口扫描找到系统漏洞从而实施攻击。

IP 欺骗攻击是产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。

PKI 体制中，保证数字证书不被篡改的方法是(43)。

- (43) A. 用 CA 的私钥对数字证书签名 B. 用 CA 的公钥对数字证书签名
C. 用证书主人的私钥对数字证书签名 D. 用证书主人的公钥对数字证书签名

【答案】 A

【解析】 本题考查 PKI 体制。

PKI 体制中，为保障数字证书不被篡改而且要发送到证书主人手中，需要用 CA 的私钥对数字证书签名，防伪造，不可抵赖。

报文摘要算法 SHA-1 输出的位数是(44)。

- (44) A. 100 位 B. 128 位 C. 160 位 D. 180 位

【答案】 C

【解析】 本题考查报文摘要算法 SHA-1。

SHA-1 从一个最大 264 位的信息中产生一串 160 位的摘要。

下面算法中，不属于公开密钥加密算法的是(45)。

- (45) A. ECC B. DSA C. RSA D. DES

【答案】D

【解析】本题考查加密算法的基础知识。

常用的加密算法依据所使用的密钥数分为单钥和双钥加密体制，也称私钥和公钥加密算法。ECC、DSA 和 RSA 都属于公开密钥加密算法，DES 是典型的私钥加密体制。

在 DHCP 服务器配置过程中，可以把使用 DHCP 协议获取 IP 地址的主机划分为不同的类别进行管理，下面划分类别规则合理的是 (46)。

- (46) A. 移动用户划分到租约期较长的类别
- B. 固定用户划分到租约期较短的类别
- C. 服务器划分到租约期最短的类别
- D. 服务器可以采用保留地址

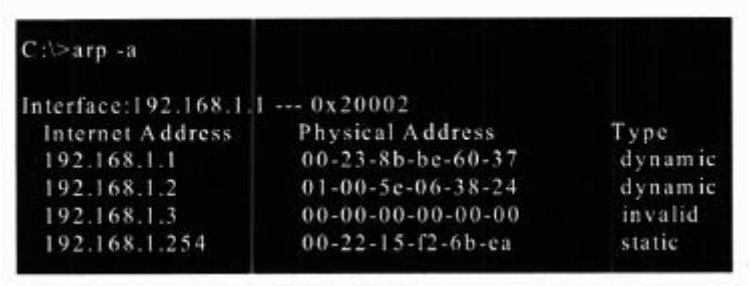
【答案】D

【解析】本题考查 DHCP 服务器配置的基础知识。

DHCP 服务器分配 IP 地址时，默认租约期限为 8 天，租约到期前客户端若需要续订，续订工作由客户端自动完成。如果网络中有较多可用的 IP 地址并且很少对配置进行更改，则增加租约期限长度可以减少客户端和 DHCP 服务器之间的租约续订查询的频率。这将会减少由客户端续订租约引起的一些网络通信量。如果网络上可用的 IP 地址数量较少并且经常更改客户端配置或客户端移动频繁，则应减少租约期限，以促进 DHCP 服务器对过时 IP 地址的清理工作。

一般来说，对于移动用户设置较短的租约期限较好，对于固定用户设置较长的租约期限较好。服务器一般不能随便更改 IP 地址，所以在配置 DHCP 服务器时，一般为服务器保留特定的 IP 地址。

在某公司局域网中的一台 Windows 主机中，先运行 (47) 命令，再运行 “arp -a” 命令，系统显示的信息如下图所示。



C:\>arp -a		
Interface: 192.168.1.1 --- 0x20002		
Internet Address	Physical Address	Type
192.168.1.1	00-23-8b-be-60-37	dynamic
192.168.1.2	01-00-5e-06-38-24	dynamic
192.168.1.3	00-00-00-00-00-00	invalid
192.168.1.254	00-22-15-f2-6b-ea	static

- (47) A. arp -s 192.168.1.1 00-23-8b-be-60-37
- B. arp -s 192.168.1.201 00-5e-06-38-24

C. arp -s 192.168.1.3 00-00-00-00-00-00

D. arp -s 192.168.1.254 00-22-15-f2-6b-ea

【答案】D

【解析】本题考查 Windows 系统的基本命令。

在 Windows 系统的命令行中，运行“arp-a”命令可以主机 ARP 缓存中的 IP 地址以及 MAC 地址的对应关系，“arp-s”命令用于绑定 ARP 缓存中的某个 IP 地址以及 MAC 地址对，对于某一个绑定的 IP 地址及 MAC 地址对，在 ARP 缓存表中“Type”项的值将由“dynamic”改为“static”。

“arp-s”命令的参数为“-sInetAddrEtherAddr[IfaceAddr]”，根据图中所给的系统提示信息，答案应为 D 选项。

SNMPc 软件支持的 4 个内置 TCP 服务是 (48)。

(48)A. FTP、SMTP、WEB 和 TELNET

B. DHCP、SMTP、WEB 和 TELNET

C. DNS、SMTP、WEB 和 TELNET

D. TFTP、SMTP、WEB 和 TELNET

【答案】A

【解析】本题考查网络管理软件 SNMPc 的基本知识。

SNMPc 是一个通用的分布式的网络管理平台，可以轮询定制的 TCP 应用服务和 4 个内置的 TCP 应用服务 (FTP、SMTP、WEB 和 TELNET)。

在 MIB-2 的系统组中，(49)对象以 7 位二进制数表示，每一位对应 OSI/RM7 层协议中的一层。

(49)A. sysDescr

B. sysUpTime

C. sysName

D. sysServices

【答案】D

【解析】本题考查管理信息库第二版的有关系统组的内容

系统组提供了系统的一般信息，系统服务对象 sysServices 是 7 位二进制数，每一位对应 OSI/RM7 层协议中的一层。如果系统提供某一层服务，则对应的位为 1，否则为 0。

SNMPv2 提供了几种访问管理信息的方法，其中属于 SNMPv2 特有的是 (50)。

(50)A. 管理站与代理之间的请求/响应通信

B. 管理站与管理站之间的请求/响应通信

- C. 代理到管理站的非确认通信
- D. 代理向管理站发送陷入报文

【答案】B

【解析】

SNMPv2 提供了 3 种访问管理信息的方法:一是管理站与代理之间的请求/响应通信,这种方法与 SNMPv1 是一样的;二是管理站与管理站之间的请求/响应通信,这种方法是 SNMPV2 特有的,可以由一个管理站把有关管理信息告诉另一个管理站;三是代理到管理站的非确认通信,即由代理向管理站发送陷入报文,报告出现的异常情况,SNMPv1 中也有对应的通信方式。

属于网络 202.115.200.0/21 的地址是 (51)。

- (51)A. 202.115.198.0
- B. 202.115.206.0
- C. 202.115.217.0
- D. 202.115.224.0

【答案】B

【解析】

网络地址 202.115.200.0/21 的二进制是: 11001010.01110011.11001000.00000000 网络地址 202.115.198.0 的二进制是: 11001010.01110011. 11000110.00000000 网络地址 202.115.206.0 的二进制是: 11001010.01110011.11001110.00000000 网络地址 202.115.217.0 的二进制是: 11001010.01110011. 11011001.00000000 网络地址 202.115.224.0 的二进制是: 11001010.01110011. 11100000.00000000 可见,能与网络地址 202.115.200.0/21 达到最长匹配的是 202.115.206.0

4 条路由:220.117.129.0/24 、 220.117.130.0/24 、 220.117.132.0/24 和 220.117.133.0/24 经过汇聚后得到的网络地址是 (52)。

- (52)A. 220.117.132.0/23
- B. 220.117.128.0/22
- C. 220.117.130.0/22
- D. 220.117.128.0/21

【答案】D

【解析】

4 条路由的二进制形式分别是:
220.117.129.0/24 11011100.01110101.10000001.00000000

220.117.130.0/24 11011100.01110101.10000010.00000000

220.117.132.0/24 11011100.01110101.10000100.00000000

220.117.133.0/24 11011100.01110101.10000101.00000000

经过汇聚后得到的网络地址是：

220.117.128.0/21 11011100.01110101.10000000.00000000

某网络的地址是 200.16.0.0, 其中包含 480 台主机, 指定给该网络的合理子网掩码是 (53), 下面的选项中, 不属于这个网络的地址是 (54)。

(53) A. 255.255.255.0

B. 255.255.252.0

C. 255.255.254.0

D. 255.255.248.0

(54) A. 200.16.0.23

B. 200.16.3.0

C. 200.16.1.255

D. 200.16.1.0

【答案】C B

【解析】

网络 200.16.0.0 中包含 480 台主机, 其主机地址必须占 9 位, 即其网络掩码为 255.255.254.0。

A. 200.16.0.23 11001000.00010000.00000000.00010111

B. 200.16.3.0 11001000.00010000.00000011.00000000

C. 200.16.1.255 11001000.00010000.00000001.11111111

D. 200.16.1.0 11001000.00010000.00000001.00000000

可以看出, A 是网络 200.16.0.0/23 中的主机地址, B 不是网络 200.16.0.0/23 中的地址。C 是 200.16.0.0/23 中的定向广播地址, D 是 200.16.0.0/23 中的主机地址。

两个主机的 IP 地址分别是 10.11.7.24 和 10.11.7.100, 要使得这两个主机包含在同一个子网中, 则指定的子网掩码长度应该为 (55) 比特。

(55) A. 25

B. 26

C. 27

D. 28

【答案】A

【解析】

主机地址 10.11.7.24 的二进制形式是: 00001010.00001011.00000111.00011000

主机地址 10.11.7.100 的二进制形式是: 00001010.00001011.00000111.01100100

要使这两个主机地址包含在同一个子网中，指定的地址掩码最长为 25 位。

IPv6 链路本地单播地址的前缀为 (56)，可聚集全球单播地址的前缀为 (57)。

(56) A. 001 B. 1111 1110 10 C. 1111 111011 D. 1111 1111

(57) A. 001 B. 1111 1110 10 C. 1111 111011 D. 1111 1111

【答案】B A

【解析】

地址前缀 001 代表可聚集全球单播地址，地址前缀 1111111010 代表链路本地单播地址，地址前缀 1111111011 代表站点本地单播地址。IPv6 组播地址格式前缀为 11111111。

在 IPv4 向 IPv6 的过渡期间，如果要使得两个 IPv6 结点可以通过现有的 IPv4 网络进行通信，则应该使用 (58)；如果要使得纯 IPv6 结点可以与纯 IPv4 结点进行通信，则需要使用 (59)。

(58) A. 堆栈技术 B. 双协议栈技术 C. 隧道技术 D. 翻译技术

(59) A. 堆栈技术 B. 双协议栈技术 C. 隧道技术 D. 翻译技术

【答案】C D

【解析】

如果要使得两个 IPv6 结点可以通过现有的 IPv4 网络进行通信，则应该使用隧道技术，如果要使得纯 IPv6 结点可以与纯 IPv4 结点进行通信，则需要使用翻译技术。

以太网链路聚合技术是将 (60)。

(60) A. 多个逻辑链路聚合成一个物理链路 B. 多个逻辑链路聚合成一个逻辑链路

C. 多个物理链路聚合成一个物理链路 D. 多个物理链路聚合成一个逻辑链路

【答案】D

【解析】

IEEE802.3ad 定义了链路聚合控制协议 (Link Aggregation Control Protocol, LACP)，它的功能是将多个物理链路聚合成一个逻辑链路。链路汇聚技术可以将多个链路绑定在一起，形成一条高速链路，以达到更高的带宽，并实现链路备份和负载均衡。

POP3 协议采用 (61) 模式进行通信，当客户机需要服务时，客户端软件与 POP3 服务器

建立 (62) 连接。

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

(62) A. TCP B. UDP C. PHP D. IP

【答案】B A

【解析】

POP3 协议采用 C/S 模式进行通信，POP3 需要 TCP 连接的支持，当客户机需要服务时，客户端软件与 POP3 服务器建立 TCP 连接。

TCP 协议使用 (63) 次握手过程建立连接，这种方法可以防止 (64)。TCP 使用的流量控制协议是 (65)。

(63) A. 一 B. 二 C. 三 D. 四

(64) A. 出现半连接 B. 出现错误连接 C. 假冒的连接 D. 无法连接

(65) 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. 选择重发 ARQ 协议

【答案】C B B

【解析】

TCP 协议使用三次握手过程建立连接，这种方法可以防止出现错误连接。大部分错误连接是由于迟到的或网络中存储的连接请求引起的。由于三次握手过程强调连接的双方都要提出自己的连接请求标识，也要应答对方的连接请求标识，所以不会受到过期的连接请求的干扰。

TCP 使用的流量控制协议是可变大小的滑动窗口协议，这种协议把肯定应答信号与扩大窗口的信号分开，更适合建立在不可靠网络上的远程连接使用。

IEEE 802.11 标准采用的工作频段是 (66)，下列标准中采用双频工作模式的是 (67)。

(66) A. 900MHz 和 800MHz B. 900MHz 和 800MHz

C. 5GHz 和 800MHz D. 2.4GHz 和 5GHz

(67) A. IEEE802.11a B. IEEE802.11b C. IEEE802.11g D. IEEE802.11n

【答案】D D

【解析】

1997 年颁布的 IEEE 802.11 标准运行在 2.4GHz 的 ISM (Industrial Scientific and

Medical) 频段,1999 年推出的 IEEE 802. 11a 标准运行在 5GHz 的 U-NIIC Unlicensed National Information Infrastructure) 频段, 802. 11b 和 802. 11g 也是运行在 2. 4GHz 频段, 2009 年发布的 802. 11n 标准则采用 2. 4GHz 和 5GHz 双频工作模式。

PC 机不能接入因特网, 这时采用抓包工具捕获的以太网接口发出的信息如下:

Source	Destination	Protocol	Info
QuantaCo_33:9b:be	Broadcast	ARP	Who has 213.127.115.254? Tell 213.127.115.31
213.127.115.31	213.127.115.255	NBNS	Name query NB TRACKER9.BOL.BG<00>
213.127.115.31	213.127.115.255	NBNS	Name query NB BT.ROMMAN.NET<00>
213.127.115.31	224.1.1.1	UDP	Source port: ircu Destination port: ircu
QuantaCo_33:9b:be	Broadcast	ARP	Who has 213.127.115.254? Tell 213.127.115.31
QuantaCo_33:9b:be	Broadcast	ARP	Who has 213.127.115.254? Tell 213.127.115.31

可以看出该 PC 机的 IP 地址为(68), 默认网关的 IP 地址为(69)。PC 不能接入 Internet 的原因可能是 (70)。

- (68)A. 213. 127. 115. 31

B. 213. 127. 115. 255

C. 213. 127. 115. 254

D. 224. 1. 1. 1
- (69)A. 213. 127. 115. 31

B. 213. 127. 115. 255

C. 213. 127. 115. 254

D. 224. 1. 1. 1
- (70)A. DNS 解析错误

B. TCP/IP 协议安装错误

C. 不能连接到网关

D. DHCP 服务器工作不正常

【答案】A C C

【解析】

由截图中的 ARP 广播包可以看出 PC 机的地址是 213. 127. 115. 31, 默认网关的地址是 213. 127. 115. 254。截图信息显示 TCP/IP 协议安装正确, 而且 DNS 服务器工作正常, 所以 PC 机不能接入 Internet 的原因, 只能选择 “不能连接到网关”。

The de facto standard Application Program Interface (API) for TCP/IP applications is the " sockets" interface. Although this API was developed for (71) in the early 1980s it has also been implemented on a wide variety of non-Unix systems. TCP/IP (72) written using the sockets API have in the past enjoyed a high degree of portability and we would like the same (73) with IPv6 applications. But changes are required to the sockets API to support IPv6 and this memo describes these changes.

These include a new socket address stmcture to carry IPv6 (74) , new address conversion functions, and some new socket options. These extensions are designed to provide access to the basic IPv6 features required by TCP and UDP applications, including multicasting, while introducing a minimum of change into the system and providing complete (75) for existing IPv4 applications.

- | | | | |
|---------------------|------------------|---------------|----------------|
| (71)A. Windows | B. Linux | C. Unix | D. DOS |
| (72)A. applications | B. networks | C. protocols | D. systems |
| (73)A. portability | B. availability | C. capability | D. reliability |
| (74)A. connections | B. protocols | C. networks | D. addresses |
| (75)A. availability | B. compatibility | C. capability | D. reliability |

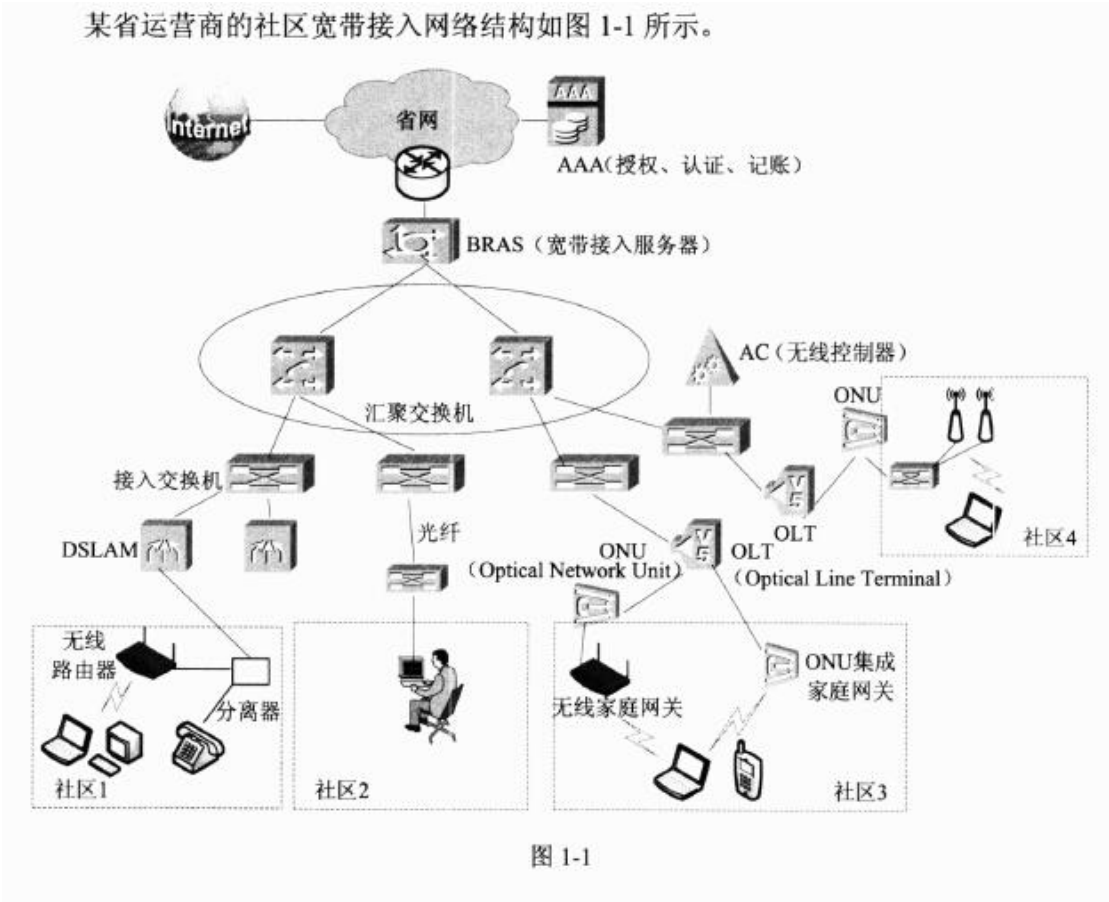
【答案】 C A A D B

【解析】

对于 TCP/IP 应用, 事实上的应用程序接口 (API) 标准是“套接字”口。虽然这个 API 是在 1980 年代早期为 Unix 开发的, 但是也广泛的在各种非 Unix 系统中得到了实现。以前采用套接字 API 编写的 TCFIP 应用具有高度的兼容性, 因而我们也希望对 IPv6 应用也具有同样的兼容性。为了支持 IPv6, 需要对套接字 API 作出某些改变, 这个便笺就是描述这些变化的。这些改变包括一种新的用于支持 IPv6 地址的套接字地址结构、新的地址转换功能以及新的套接字选项。这些扩展可以满足 TCP 和 UDP 应用访问 IPv6 基本功能 (包括组播) 时的需要, 但是只对系统进行了最小的改变, 而且与现有的 IPv4 应用是完全兼容的。

试题一

某省运营商的社区宽带接入网络结构如图 1-1 所示。



【问题 1】

高速数据主干网的一个建设重点是解决“最后一公里”的问题，即宽带接入问题。图 1-1 所示的四个社区采用的小区宽带接入方法分别是：社区 1 (1)，社区 2 (2)，社区 3 (3)，社区 4 (4)。除了这几种宽带接入方法以外，采用有线电视网进行宽带接入的方法是 (5)，利用电力网进行宽带接入的方法是 (6)，遵循 IEEE802.16 标准进行宽带接入的方法是 (7)。

空 (1)～(7) 备选答案：

- A. FTTx+PON
- B. HFC
- C. FTTx+LAN
- D. WLAN
- E. WiMax
- F. xDSL
- G. PLC (Power-Line Communication)

H. GPRS

- (1) F 或 xDSL
- (2) C 或 FTTx+LAN
- (3) A 或 FTTx+PON
- (4) D 或 WLAN
- (5) B 或 HFC
- (6) G 或 PLC (Power-Line Communication)
- (7) E 或 WiMax

本问题主要考查宽带接入网络的形式。

高速数据主干网的一个建设重点是解决“最后一公里”的问题，即宽带接入问题。

目前常见的几种宽带接入技术主要有 xDSL、FTTx+LAN、FTTx+PON、WLAN、HFC 以及 PLC 等。根据图 1-1 中的提示信息，社区 1 通过 DSLAM 以及分离器实现上网和电话同时使用，因此采用的是传统的 xDSL 技术接入网络；社区 2 通过光纤接入交换机，交换机直接连接用户，因此使用的是 FTTx+LAN 的方式接入网络；社区 3 通过 OLT 和 ONU 家庭集成网关实现上网和电话同时使用，显然采用的是 FTTx+PON 的形式；社区 4 利用无线 AP 接入网络，那么就是采用 WLAN 的方式无线接入网络。除此以外电力上网，即 PLC (Power Line Communication)，也就是利用电线实现电力线通信。它通过利用传输电流的电力线作为通信载体，使得 PLC 具有极大的便捷性。此外，除了利用电力上网外，还可将房屋内的电话、电视、音响、冰箱等家电利用 PLC 连接起来，进行集中控制，实现“智能家庭”的梦想。HFC (Hybrid Fiber Coaxial) 是光纤和同轴电缆相结合的混合网络，除可以进行有线电视信号的传输外还可以进行多媒体数据的高速传输。Wimax，即全球微波互联接入，是一项新兴的宽带无线接入技术，遵循 IEEE802.16 标准，特别适合户外使用。

【问题 2】

在宽带接入中，FTTx 是速度最快的一种有线接入方式，而 PON (Passive Optical Network) 技术是未来 FTTx 的主要解决方案。PON 目前有两种主要的技术分支，分别是 GPON 和 EPON，EPON 是 (8) 技术和 (9) 技术的结合，它可以实现上下行 (10) 的速率。

- (8) 以太网

(9) PON(注：(8) (9)可互换)

(10) 1.25Gbps

本问题主要考查光纤接入宽带网络系统的 PON 技术。

FTTx 技术主要应用于光纤接入宽带网络系统中，具体的应用范围包括该区域内从局端到用户端的光线路终端 (Optical Line Terminal, OLT) 和光网络终端 (Optical Network Terminal, ONT) 或光网络单元 (Optical Network Unit, ONU)，以及连接以上两种设备的光分配网络 (Optical Distribution Network ODN)。FTTx 的实现技术包括：点到点 (P2P) 和点到多点 (P2MP) 两种。点到多点 (P2MP) 技术主要应用于 PON 网络接入，常用的 FTTx 实现 PON 技术，包括 BPON (APON)、EPON、GPON。

EPON (Ethernet Passive Optical Network) 以太无源光网络，由 IEEE802.3 提出定义其基本操作模式和标准，是新型光纤接入网技术之一，同时也是未来光接入网的支撑技术。EPON 综合了 PON 技术和以太网技术的优点，EPON 网络采用了 WDM 波分复用技术，以光纤作为载体，利用单根光纤实现双向速率为 1.25Gbit/s 的传输，基于 IEEE802.3ah 的 EPON 标准，规定了上下行波长 (1310nm、1490nm 和 1550nm)、传输速率 1.25Gbit/s、传输距离 10/20km、最大分光比 1:64 和主要业务。

【问题 3】

宽带接入通常采用 PPPoE 进行认证。PPP 协议一般包括三个协商阶段，(11) 协议用于建立和测试数据链路；(12) 协议用于协商网络层参数；(13) 协议用于通信双方确认对方的身份。

(11) LCP (链路控制协议)

(12) NCP (网络层控制协议)

(13) 认证 (CHAP/PAP)

本问题主要考查宽带接入的 PPPoE 认证原理。

PPP 是传统的认证方式之一，PPPoE 是利用以太网发送 PPP 包的传输方法和支持在同一以太网上建立多个 PPP 连接的接入技术。PPPoE 结合了以太网和 PPP 连接的综合属性。

PPP 协议是一种点到点的链路层协议，它提供了点到点的一种封装、传递数据的一种方法。PPP 协议一般包括三个协商阶段：LCP (链路控制协议) 阶段，认证阶段 (比如 CHAP/PAP)，

NCP(网络层控制协议, 比如 IPCP)阶段。拨号后, 用户计算机和局方的接入服务器在 LCP 阶段协商底层链路参数, 然后在认证阶段通过用户计算机将用户名和密码发送给接入服务器认证, 接入服务器可以进行本地认证, 可以通过 RADIUS 协议将用户名和密码发送给 AAA 服务器进行认证。认证通过后, 在 NCP(IPCP)协商阶段, 接入服务器给用户计算机分配网络层参数如 IP 地址等。经过 PPP 的三个协商阶段后, 用户就可以发送和接受网络报文。用户收发的所有网络层报文都封装在 PPP 报文中。PPP 协议的一个重要的功能提供身份验证功能。

以太网是一种广播网络, 其缺点是通讯双方无法相互验证对方身份, 通讯是不安全的。PPP 协议提供了通讯双方身份验证的功能, 但是 PPP 协议是一种点对点的协议, 协议中没有提供地址信息。如果 PPP 应用在以太网上, 必须使用 PPPoE 再进行一次封装, PPPoE 协议提供了在以太网广播链路上进行点对点通讯的能力。

【问题 4】

在运营商网络中, 一般会有多个用户和不同的业务流需要融合。运营商常用外层 VLAN 区分不同的 (14), 在 ONU 或家庭网关处采用内层 VLAN 来区分不同的 (15); 这种处理方式要求运营商网络和用户局域网中的交换机都支持 (16) 协议, 同时通过 802.1ad(运营商网桥协议) 来实现灵活的 QinQ 技术。

(14) 业务

(15) 用户

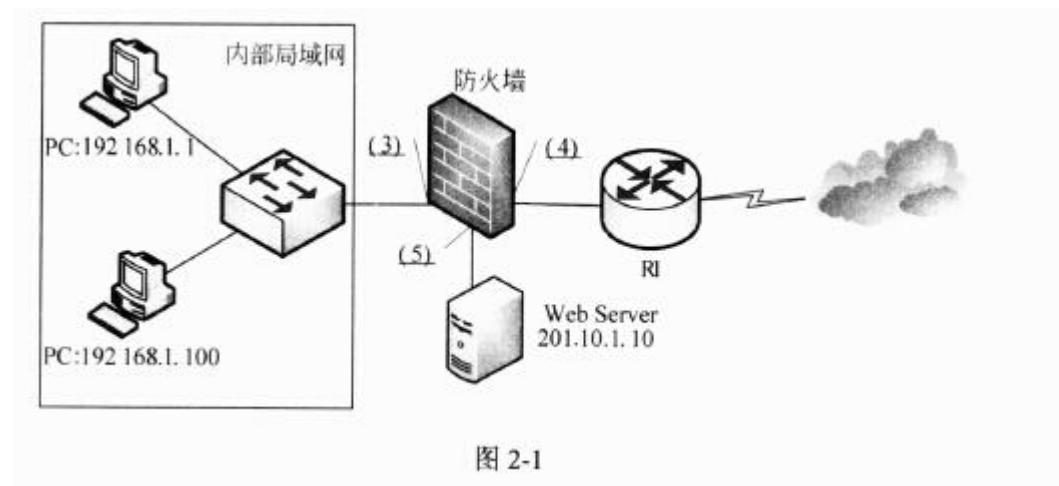
(16) 802.1Q

本问题主要考查 QinQ 技术。

QinQ 技术 (也称 StackedVLAN 或 DoubleVLAN)。标准出自 IEEE802.1ad, 其实现为在 802.1Q 协议标签前再次封装 802.1Q 协议标签, 其中一层标识用户系统网络(customer network), 一层标识网络运营网络 (service provider network), 将其扩展实现用户线路标识, 使报文带着两层 VLANTag 穿越运营商的骨干网络 (公网)。当前部分交换机可以支持 QinQ 功能。QinQ 允许运营商为每个用户分配最大到 4K 的第二个 VLANID。运营商 VLAN 标记在 IPDSLAM 网络侧插入, 在用户侧删除。BAS 通过识别用户的第二个 VLAN 确定用户线路标识。QinQ 也较好地解决了 VLAN(最大 4k)数量不足问题。在实际使用中运营商常用外层 VLAN 区分不同的业务, 在 ONU 或家庭网关处采用内层 VLAN 来区分不同的用户。

试题二

为了保障网络安全，某公司安装了一款防火墙，对内部网络、Web 服务器以及外部网络进行逻辑隔离，其网络结构如图 2-1 所示。



【问题 1】

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 1-99 的 ACL 根据 IP 报文的源地址域进行过滤，称为(1)；编号为 100-199 的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为 (2)。

(1) 标准访问控制列表 (标准 ACL)

(2) 扩展访问控制列表 (扩展 ACL)

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 1-99 的 ACL 根据 IP 报文的源地址域进行过滤，称为标准访问控制列表 (标准 ACL);编号为 100-199 的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为扩展访问控制列表 (扩展 ACL)。

【问题 2】

根据图 2-1，防火墙的三个端口连接的网络分别称为 (3)、 (4)和 (5)。

(3) 内网 (Trusted)

(4) 外网 (Untrusted)

(5) DMZ (非军事区)

防火墙的端口连接的网络依据被保护对象的安全级别分为三个：内网（Trusted）有要保护的数据和主机，安全级别最高；DMZ（非军事区）放置可对外提供的服务器群，安全级别次之；外网（Untrusted）是内网用户可访问资源，安全设置较少，安全级别最低。

【问题 3】

防火墙配置要求如下：

- ◆ 公司内部局域网用户可以访问 WebServer 和 Internet；
- ◆ Internet 用户可以访问 WebServer；
- ◆ Internet 上特定主机 202.110.1.100 可以通过 Telnet 访问 WebServer；
- ◆ Internet 用户不能访问公司内部局域网。

请按照防火墙的最小特权原则补充完成表 2-1。

表 2-1					
源 地 址	源 端 口	目 的 地 址	目 的 端 口	协 议	规 则
Any	Any	(6)	(7)	WWW	允许
192.168.1.0/24	Any	(8)	(9)	Any	允许
202.110.1.100	Any	(10)	(11)	TELNET	允许
Any	Any	Any	Any	Any	(12)

(6) 201.10.1.10

(7) 80

(8) Any

(9) Any

(10) 201.10.1.10

(11) 23

(12) 拒绝

表中第一条规则允许 WWW 服务，对应要求中的第 2 条，即 Internet 用户可以访问 WebServer，故目的地址及目的端口分别是服务器的 IP 地址和 80 端口号；

第二条规则源地址为 192.168.1.0/24，对应要求中的第 1 条，即公司内部局域网用户可以访问 WebServer 和 Internet，故目的地址和端口号为任意值均可，故 (8)、(9) 处应填 any 和

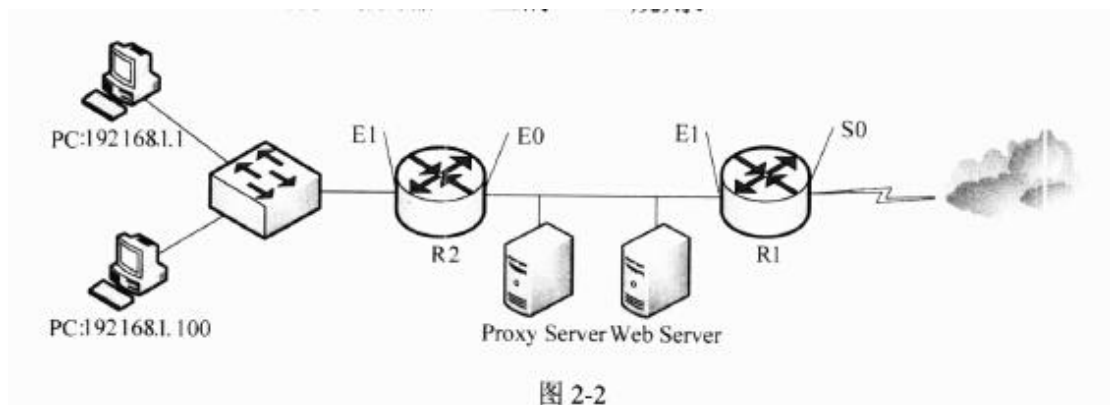
any;

第三条规则源地址为 202.110.1.100、服务为 TELNET, 对应要求中的第 3 条, 即 Internet 上特定主机 202.110.1.100 可以通过 Telnet 访问 WebServer, 故目的地址和端口号为服务器的 IP 地址和 TELNET 的端口号 23;

第四条规则对应要求中的第 4 条, 即 Internet 用户不能访问公司内部局域网, 故规则动作为拒绝。

【问题 4】

由于防火墙出现故障, 现将网络拓扑进行调整, 增加一台包过滤路由器 R2, 与 ProxyServer 和路由器 R1 共同组成一个屏蔽子网防火墙, 结构如图 2-2 所示。为了实现与表 2-1 相同的过滤功能, 补充路由器 R1 上的 ACL 规则。



```
R1>...
R1(config-s0)> access-list 101 permit (13)
//允许 Internet 用户访问 WebServer
R1(config-s0)> access-list 101 permit (14)
//允许主机 202.110.1.100 Telnet 到 Web Server
R1(config-s0)> access-list 101 (15)
//禁止所有 IP 包
R1 (config-s0)> ip access-group 101 in
//应用 101 规则到 s0 入口

R1>...
R1(config-ethernet1)> access-list 102 permit ip any any
R1 (config-ethernet1)> ip access-group 102 out
R1>...
```

(13) tcp any host 201.10.1.10 eq www

(14) tcp host 202.110.1.100 host 201.10.1.10 eq telnet

(15) deny ip any any

空(13)处为允许 Internet 用户访问 Webserver, 故语句为: tcp any host 201.10.1.10 eq www

空(14)处为允许主机 202.110.1.100 Telnet 到 Web Server, 故语句为: tcp host 202.110.1.100 host 201.10.1.10 eq telnet

空(15)处为禁止所有 IP 包, 故语句为: deny ip any any

试题三

某单位网络拓扑结构如图 3-1 所示，内部各计算机终端通过代理服务器访问 Internet，网络要求如下：

1. 运营商提供的 IP 地址为 202.117.112.0/30，网络出口对端 IP 地址为 202.117.112.1；
2. 代理服务器采用 Linux 系统；
3. Web、DNS 和 DHCP 服务器采用 Windows Server2003 系统，Web 服务器 IP 地址为 192.168.0.3，DNS 服务器 IP 地址为 192.168.0.2，DHCP 服务器 IP 地址为 192.168.0.4；
4. 内部客户机采用 WindowsXP 系统，通过 DHCP 服务器动态分配 IP 地址，子网为 192.168.0.0/25，内网网关 IP 地址为 192.168.0.1；
5. 代理服务器、DNS、Web 和 DHCP 服务器均通过手动设置 IP 地址。

【问题 1】

Linux 系统中，IP 地址的配置文件一般存放在（1）目录下。

A. /etc B. /var C. /dev D. /home

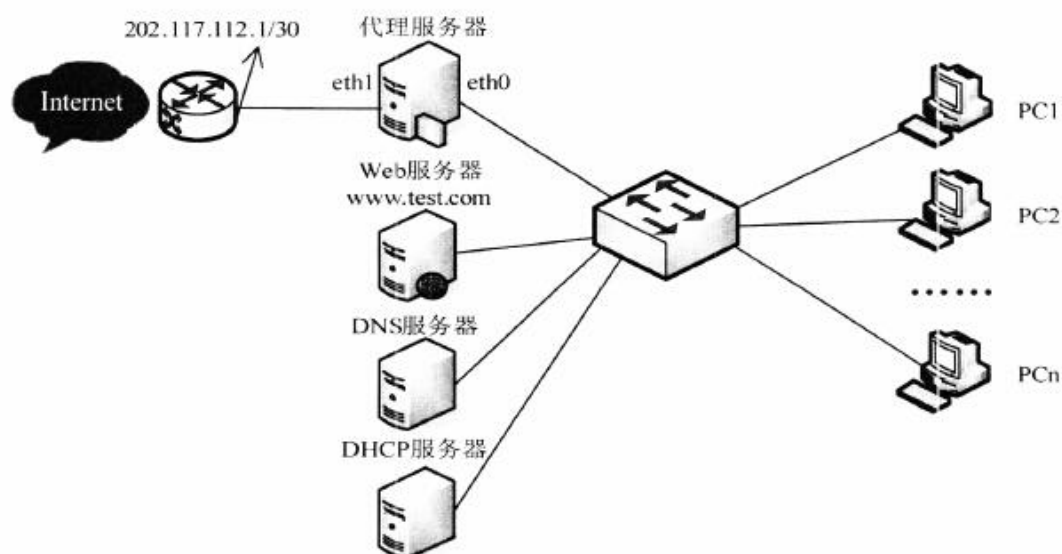


图 3-1

(1) A 或/etc

本问题主要考查考生对 Linux 操作系统中目录的了解程度。Linux 系统中，IP 地址的配置文件一般存放在/etc 目录下。

【问题 2】

请完成图 3-1 中代理服务器 eth0 的配置。

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:24:F8:9B
NETMASK= (2)
IPADDR= (3)
GATEWAY=192.168.0.1
TYPE=Ethernet
NAME="System eth0"
IPV6INIT=no
```

(2) 255.255.255.128

(3) 192.168.0.1

本问题主要考查对文本方式下网络配置的掌握程度。HWADDR 是 MAC 地址信息，NETMASK 是网络掩码信息，IPADDR 是 IP 地址，GATEWAY 为网关 IP 地址。

【问题 3】

请完成图 3-1 中代理服务器 eth1 的配置。

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:21:A1:78
NETMASK= (4)
IPADDR= (5)
```

```
GATEWAY= (6)
TYPE=Ethernet
NAME="System eth0"
IPV6INIT=no
DEVICE=eth0
```

(4) 255.255.255.252

(5) 202.117.112.2

(6) 202.117.112.1

本问题主要考查对文本方式下网络配置的掌握程度。HWADDR 是 MAC 地址信息，NETMASK 是网络掩码信息，IPADDR 是 IP 地址，GATEWAY 为网关 IP 地址

【问题 4】

DNS 使用 (7) 来处理网络中多个主机和 IP 地址的转换，当 DNS 服务器配置完成后，在客户机的 cmd 命令窗口中，可用于测试 DNS 服务状态的命令有 (8) (多选)。

(7) 备选答案：

A. 集中式数据库 B. 分布式数据库

(8) 备选答案：

A. nslookup B. arp C. ping D. tracert E. ipconfig

(7) B 或分布式数据库

(8) A、C、D 或 nslookup、ping、tracert

本问题主要考查 DNS 原理和测试命令。

nslookup 命令是一个用于查询 Internet 域名信息或诊断 DNS 服务器问题的工具。arp 命令可用于查询本机 ARP 缓存、添加或删除静态对应关系。ping 命令是因特网包探索器，用于测试网络连接量的程序，当 ping 域名时可以根据能否返回 IP 地址来判断 DNS 状态。

tracert 命令是路由跟踪实用程序，可以通过追踪域名查看能否返回相应 IP 地址来判断 DNS 状态。

ipconfig 命令是调试计算机网络的常用命令。

【问题 5】

安装 DNS 服务时，在图 3-2 所示 Windows 组件中，选择 (9)，然后点击“详细信息”进行 DNS 组件安装。

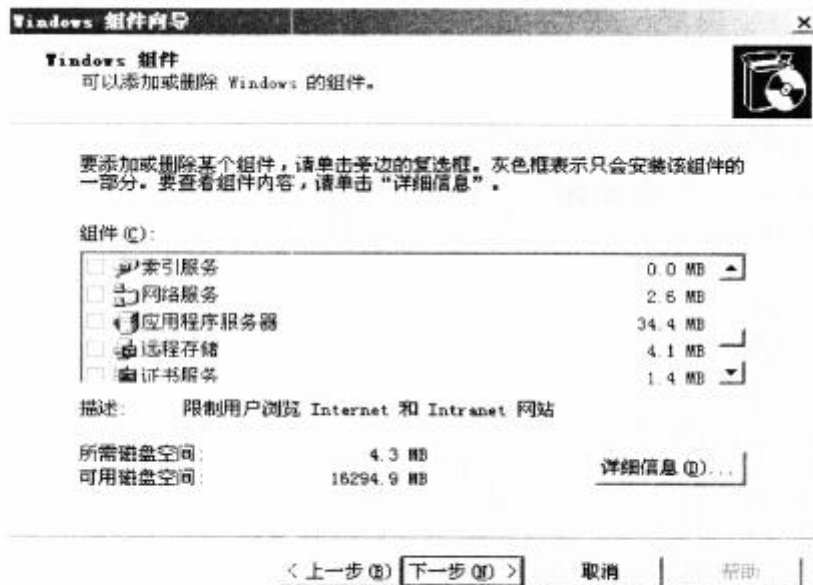


图 3-2

(9) 网络服务

DNS 组件属于网络服务组件。

【问题 6】

在 DNS 服务器中为 Web 服务器添加主机记录时，在图 3-3 中区域名称应填写 (10) 来建立正向查找区域。在图 3-4 所示的“新建主机”对话框中名称栏应填写 (11)，IP 地址栏应填写 (12)。



图 3-3

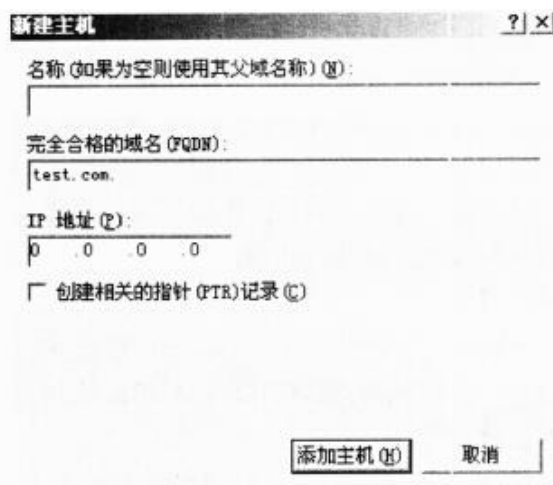


图 3-4

(10) test.com

(11) www

(12) 192.168.0.3

本问题主要考查考生对 WindowsServer2003 操作系统中具体添加正向解析记录操作的掌握程度。

在添加主机记录时，为区域名为 test.com、名称栏为 www 来建立正向查找 K 域，对应的 IP 地址为 192.168.0.3。

【问题 7】

在建立反向区域时，图 3-5 中的“网络 ID”中输入（13）。在图 3-6 所示的创建指针记录对话框中，主机的 IP 地址为（14），主机名为（15）。

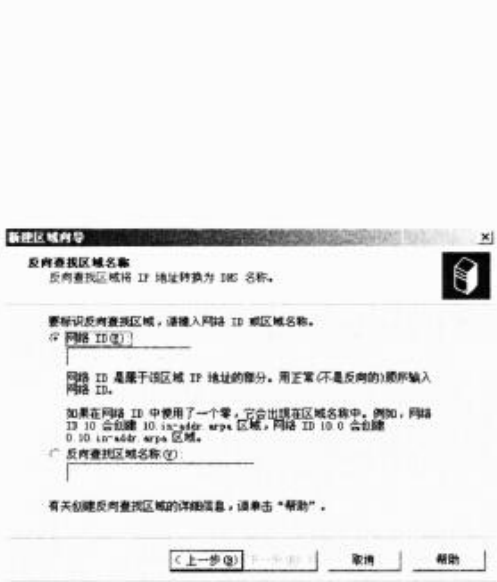


图 3-5



图 3-6

(13) 192.168.0.0

(14) 3

(15) www.test.com

本问题主要考查考生对 WindowsServer2003 操作系统中具体添加反向解析记录操作的掌握程度。

在建立反向区域时，网络 ID 应为 192.168.0.0。在创建指针记录对话框中，主机的 IP 地址为 192.168.0.3，主机名为 www.test.com。

试题四

某公司计划使用路由器作为 DHCP Server, 其网络拓扑结构如图 4-1 所示。根据业务需求, 公司服务器 IP 地址使用 192.168.2.1/24, 部门 1 使用 192.168.4.1/24 网段、部门 2 使用 192.168.3.1/24 网段 (其中 192.168.3.1~192.168.3.10 地址保留不分配), 部门 1 和部门 2 通过路由器的 DHCP 服务自动获取 IP 地址。

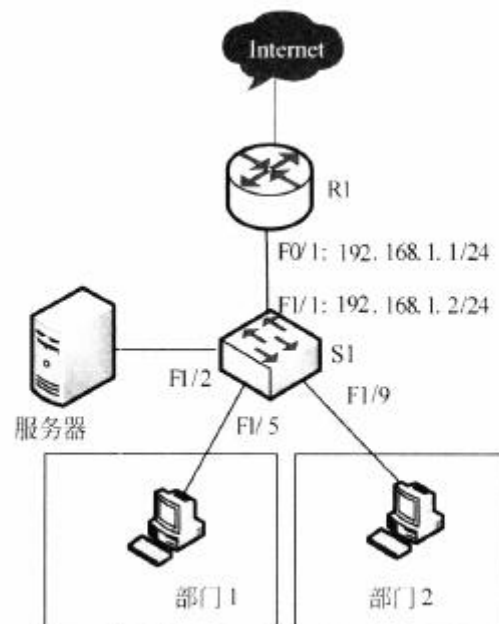


图 4-1

【问题 1】

根据网络拓扑和需求说明, 完成 (或解释) 路由器 R1 的配置:

```

R1#config t
R1 (config)# interface FastEthernet0/1
R1 (config-if)#ip address (1) (2)
R1 (config-if)#no shutdown
R1(config-if)#exit
R1 (config)#ip dhcp pool vlan 3
R1 (dhcp-config)# network 192.168.3.0 255.255.255.0
R1 (dhcp-config)# default-router 192.168.3.254 255.255.255.0
: (3)
R1 (dhcp-config)# dns-server 192.168.2.1 : (4)
R1 (dhcp-config)# lease 0 8 0 : (5)
R1 (dhcp-config)#exit
R1 (config)# ip dhcp pool vlan 4
R1(dhcp-config)# network (6) (7)
R1 (dhcp-config)# default-router 192.168.4.254 255.255.255.0
R1 (dhcp-config)# dns-server 192.168.2.1
R1 (dhcp-config)# lease 0 8 0
R1 (dhcp-config)#exit
R1 (config)# ip dhcp excluded-address (8) (9)
R1 (config)# ip dhcp excluded-address 192.168.3.254 ; 排除掉不能分配的
IP 地址
R1 (config)# ip dhcp excluded-address 192.168.4.254

R1 (config)# (10) 192.168.3.0 255.255.255.0 FastEthernet0/1 ; 在以太网
接口和 VLAN3 间建立一条静态路由

```

(1) 192.168.1.1

(2) 255.255.255.0

(3) 设置 vlan3 默认网关及掩码

(4) 设置 dns 服务器地址

(5) 设置 dhcp 租约时间为 8 小时

(6) 192.168.4.0

(7) 255.255.255.0

(8) 192.168.3.1

(9) 192.168.3.10

(10) iproute

本问题考查路由器的接口配置及 DHCP 服务设置。

根据图 4-1 可以确定路由器的接口地址及 vlan4 的地址范围，同时题目说明明确指出了 192.168.3.1~192.168.3.10 地址保留不分配。所以路由器的配置及说明应如下所示：

```

R1#config t
R1 (config)# interface FastEthernet0/1
R1 (config-if)#ip address 192.168.1.1 255.255.255.0

R1 (config-if)#no shutdown
R1(config-if)#exit
R1 (config)#ip dhcp pool vlan 3
R1 (dhcp-config)# network 192.168.3.0 255.255.255.0
R1 (dhcp-config)# default-router 192.168.3.254 255.255.255.0 ; 设
vlan3 默认网关及掩码
R1 (dhcp-config)# dns-server 192.168.2.1 ; 设 dns 服务器地址
R1 (dhcp-config)# lease 0 8 0 ; 设 dhcp 租约为 8 小时
R1 (dhcp-config)#exit
R1 (config)# ip dhcp pool vlan 4
R1(dhcp-config)# network 192.168.4.0 255.255.255.0
R1 (dhcp-config)# default-router 192.168.4.254 255.255.255.0
R1 (dhcp-config)# dns-server 192.168.2.1
R1 (dhcp-config)# lease 0 8 0
R1 (dhcp-config)#exit
R1 (config)# ip dhcp excluded-address 192.168.3.1 192.168.3.10

R1 (config)# ip dhcp excluded-address 192.168.3.254 ; 排除掉不能分配的
IP 地址
R1 (config)# ip dhcp excluded-address 192.168.4.254

R1 (config)# ip route 192.168.3.0 255.255.255.0 FastEthernet0/1 ; 在以
以太网接口和 VLAN3 间建立一条静态路由
.....

```

【问题 2】

根据网络拓扑和需求说明，完成（或解释）交换机 S1 的部分配置。

```

S1#config t
S1(config)#interface vlan2
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan3
S1(config-if)# ip helper-address (11) ;指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan4
.....
S1(config)#interface f1/1
S1(config-if)#switchport mode (12)
S1(config-if)# switchport trunk allowed vlan all

```

```
S1(config-if)#exit
S1(config)#interface f1/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access (13)
S1(config-if)#exit
S1(config)#interface f1/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access (14)
S1(config)#interface f1/9
S1(config-if)#switchport mode access
S1(config-if)#switchport access (15)
.....
```

(11) 192.168.1.1

(12) trunk

(13) vlan2

(14) vlan4

(15) vlan3

本问题考查交换机基本配置。依据问题 1 可以确定 DHCP 服务器的地址，枝据拓扑图可以判定交换机各个接口连接的部门，再根据题目描述确定其 Vlan，所以该交换机的配置如下：


```
S1#config t
S1(config)#interface vlan2
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan3
S1(config-if)# ip helper-address 192.168.1.1 ;指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan4
.....
S1(config)#interface f1/1
S1(config-if)#switchport mode trunk
S1(config-if)# switchport trunk allowed vlan all
S1(config-if)#exit
S1(config)#interface f1/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan2
S1(config-if)#exit
S1(config)#interface f1/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan4
S1(config)#interface f1/9
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan3
```