

●为了有效地保护电子商务交易的安全，出现了一系列相应的安全标准协议，其中要求参与电子商务交易的两方（客户端与服务端）都有数字证书的是(1)。如果采用这种协议，客户端（公钥 $K_c$ ，私钥 $P_c$ ）要将信息 $M$ 发送给服务器（公钥 $K_s$ ，私钥 $P_s$ ），则需要进行(2)操作。

(1) A. SSL                      B. SHTTP                      C. SET                      D. DES

(2) A.  $P_s(K_c(M))$       B.  $P_s(P_c(M))$                       C.  $K_s(K_c(M))$                       D.  $K_s(P_c(M))$

查看答案

C, D

查看分析

**分析：**在电子商务交易安全方面，有三个不同的安全标准：(1) SSL，这是传输层的安全协议，它只是在服务端使用数字证书；(2) SET，是应用层的安全协议，它要求交易两方都有数字证书；(3) SHTTP，是应用层的安全协议，在 HTTP 协议的基础上实现，无需数字证书，采用对称钥加密。

交易双方都有数字证书时，则将基于非对称钥进行加密。发送时，应先将信息用自己的私钥加密（这样才能够确保别人可以用你的公钥加密），然后再用服务器的公钥加密（这样可以确保只能服务器能够用自己的私钥进行加密），因此整个操作是  $K_s(P_c(M))$ 。

● 电子邮件是最普及的Internet应用之一，E-mail服务器的职责之一就是完成邮件的外发，它工作在(3)端口上。如果要为abc.com这个域构建E-mail服务器，则需在相应的DNS服务器的(4)文件中添加一条(5)记录。在Linux中，DNS服务器的主配置文件是(6)。

- |                         |                    |                    |                    |
|-------------------------|--------------------|--------------------|--------------------|
| (3) A. 110              | B. 80              | C. 53              | D. 25              |
| (4) A. DNS 启动文件         | B. 正向解析文件          | C. 反向解析文件          | D. 缓存文件            |
| (5) A. MX               | B. NS              | C. PTR             | D. SRV             |
| (6) A. /etc/resolv.conf | B. /etc/hosts.conf | C. /etc/named.boot | D. /etc/named.conf |

#### 查看答案

D, B, A, D

#### 查看分析

分析：E-mail 是 Internet 上使用最多的一种网络服务，与 E-mail 相关的有三个协议，如下所示。

- (1) SMTP：简单邮件传送协议，用于邮件的发送，工作在 25 号端口上；
- (2) POP3：邮局协议 V3.0，用于接收邮件，工作在 110 号端口上；
- (3) IMAP：邮件访问协议，是用于替代 POP3 协议的新协议，工作在 143 号端口上。

由于 E-mail 服务器的特殊性，在 DNS 解析时需要进行特别的处理，也就是在“正向解析文件”加入一条邮件服务器记录：MX 记录。DNS 服务除了标识主机的 A 记录、邮件服务器的 MX 记录之外，还有标识 DNS 服务器的 NS 记录、反向解析的 PTR 记录、用于活动目录的 SRV 记录等。

在 Linux 中常用于构架 DNS 服务器的软件是 BIND，其守候进程是 named。而其主配置文件也符合其常用的命名规范：/etc/named.conf。

●在以下的无线局域网标准中，不是工作在ISM频段上的是(6)，使用CCK技术的是(7)

(6), (7) A. IEEE 802.11

B. IEEE 802.11a

C. IEEE 802.11b

D. IEEE 802.11g

查看答案

B, C

查看分析

分析：IEEE 802.11 委员会发布的无线局域网标准，现在已有四个：

(1) 802.11。工作在 2.4GHz 的 ISM 频段，使用扩频通信技术，速率是 1Mb/s 和 2Mb/s。

(2) 802.11b。工作在 2.4GHz 的 ISM 频段，使用 CCK 技术，速率是 11Mb/s。

(3) 802.11a。工作在 5GHz U-NII 频段，使用 OFDM 调制技术，速率是 54Mb/s。

(4) 802.11g。工作在 2.4GHz 的 ISM 频段，使用 OFDM 调制技术，速率是 54Mb/s。

● 设有一个使用CSMA/CD介质访问技术的网络，其速度为 100Mb/s，信号的传播速度是 200 米/ $\mu$ 秒，网络的最大段长是 100 米，则其最小帧长是(8)。如果该网络上的站点在信道忙时将一直监听网络，直到信道空闲时就立即发送，则说明使用的是(9)监听算法。当发送信息时，出现冲突，则(10)。

- (8) A. 400bit      B. 200bit      C. 100bit      D. 64bit  
(9) A. 非坚持型      B. 1-坚持型      C. P-坚持型      D. P-非坚持型  
(10) A. 马上停止发送，然后向整个网络广播 Jamming 信号  
B. 将当前的数据包发送完后，向整个网络广播 Jamming 信号  
C. 向冲突来源站点发送 Jamming 信号，使其停止发送后自己继续发送  
D. 继续发送数据包，并向网络广播 Jamming 信号

查看答案

C, B, A

查看分析

**分析：**CSMA/CD 采用了边发边听的冲突检测方法。也就是由发送者一边发，一边自己接收回来，一旦发现结果出现不同，马上停止发送，并发出 Jamming（冲突）信号。正是由于采用了边发边听的检测方法，因此检测冲突所需要花的最长时间是网络传播延迟的两倍（最大段长/信号传播速度，对于基带系统而言，有些宽带系统需要网络传播延迟的四倍时间才够），这称为冲突窗口。因此，为了保证在信息发送完成之前能够检测到冲突，发送的时间应该大于等于冲突窗口，这也就规定了最小的帧长=2（网络数据速率×最大段长/信号传播速度）。

因此在本题中，最小的帧长=2×（100Mb/s×100 米/200 米/ $\mu$  秒）=100bit。

为了缓解冲突发生的频率，CSMA/CD 设计了几种不同的监听算法：

（1）非坚持型监听算法：当遇信道空闲时，则立即发送；当信道忙时，则等待 N 个单位时间，再监听；它能够减少冲突，但也降低了信道利用率。

（2）1-坚持型监听算法：当遇信道空闲时，则立即发送；当信道忙时，继续监听；它虽然提高了信道利用率，但增大了冲突的可能。

（3）P-坚持型监听算法：当遇信道空闲时，以概率 P 发送；当信道忙时，继续监听；它能够有效平衡，但是算法复杂。

●ICMP的报文是封装在(11)里进行传送的，在网络中起到差错和拥塞控制的作用。在该协议中定义了 13 种报文，其中ping命令是基于(12)报文工作的，而当发现“目的主机未知”时，会产生(13)报文。

- (11) A. HDLC 协议包    B. BPDU    C. TCP 数据包    D. IP 数据报  
(12) A. 回送请求与应答    B. 信息请求    C. 时间戳请求    D. 重定向  
(13) A. 数据报参数错    B. 数据报超时    C. 目的地不可达    D. 源站抑制

查看答案

D, A, C

查看分析

分析：ICMP（Internet 控制报文协议）是 IP 的一部分，属于网络层协议，其报文是封装在 IP 协议数据单元中进行传送的，在网络中起到差错和拥塞控制的作用。

ICMP 协议中定义了 13 种报文，包括回送应答、目的地不可达、源站抑制、重定向（改变路由）、回送请求、数据报超时、数据报参数错、时间戳请求、时间戳应答、信息请求（已过时）、信息应答（已过时）、地址掩码请求、地址掩码回答。

而 ping 命令是基于回送请求与应答报文工作的，当发现“目的主机未知”时，会产生目的地不可达报文。

●实现FTTB的关键技术是(14)，(14)可以分为(15)两种。

(14) A. SDH                      B. PON                                      C. SONET                      D. HFC

(15) A. APON 和 EPON                                      B. SDH 和 PDH  
C. SPON 和 EPON                                      D. Hi-HFC 和 Wi-HFC

查看答案

B, A

查看分析

分析：无源光网（PON）是实现 FTTB 的关键性技术。其在光分支点不需要节点设备，只需安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。目前无源光网 PON 技术主要有 APON（基于 ATM 的无源光网络）和 EPON（基于以太网的无源光网络）两种。

●在HFC网络中，需要一个名为Cable MODEM的设备，它不单纯是一个调制解调器，而是多种设备的组合，但不包括(16)；它采用的复用技术是(17)。

(16) A. 加/解密设备    B. 以太网集成器    C. 电视解压卡    D. 网络接口卡

(17) A. 时分复用    B. 频分复用    C. 码分复用    D. 波分复用

查看答案

C, B

查看分析

分析：有线电视网的双向改造之后，就催生了 Cable MODEM 接入的技术。与该技术直接相关的就是 HFC（混合光纤—同轴电缆）技术。

在同轴电缆的技术方案中，用户端需要使用一个称为 Cable MODEM（电缆调制解调器）的设备，它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身，它无需拨号，可提供随时在线的永远连接。其上行速度已达 10Mb/s 以上，下行速率更高。其采用的复用技术是 FDM（频分复用技术），使用的编码格式是 64QAM 调制。

●在以下选项中，（18）不能作为专利申请。

（18）A. 疾病的诊断和治疗方法

B. 手机的外观设计

C. 软件开发技术

D. 钢铁冶炼方法

查看答案

A

查看答案

~ 专利法第25条

~ 第25条第1款第2项

**分析：**而对于科学发现、智力活动的规则和方法、疾病的诊断和治疗方法、动植物品种以及用原子核变换方法获得的物质，不能够被授予专利权。



●某软件产品注册版权后 51 年，原作者的(19)仍受到保护。

(19) A. 获得报酬权 B. 使用许可权 C. 署名权 D. 转让权

查看答案

C

查看答案

分析： 本题主要考查了计算机软件保护条例的相关知识。

●CRC码是一种常见的差错控制方法，假设CRC的生成多项式是 $G(x)=x^3+x+1$ ，而信息码为11001，则其产生的校验码是(20)，码字(21)是CRC错误的。

(20) A. 100

B. 111

C. 011

D. 001

(21) A. 10101101

B. 10011101

C. 10111011

D. 11111110

查看答案

B, B

查看分析

分析：问题一考查的是CRC校验码的计算方法，如图1所示。

1. 生成多项式最高位为3，因此补3个0，也确认校验码为3位。
2. 生成多项式等价于：  
 $1 \cdot X^3 + 0 \cdot X^2 + 1 \cdot X + 1 = 1$   
 因此等到除数，1011
3. 通过模2除得到余数为111，因此校验码为111。

$$\begin{array}{r}
 1011 \overline{) 11001000} \\
 \underline{1011} \phantom{000} \\
 1111 \\
 \underline{1011} \\
 1000 \\
 \underline{1011} \\
 1100 \\
 \underline{1011} \\
 111
 \end{array}$$

图1 CRC 校验码计算

问题2考查的则是该运算的反计算，即用生成的码字去除生成多项式，余数不为0则错误，如图2所示。

$  \begin{array}{r}  1011 \overline{) 10101101} \\  \underline{1011} \\  1110 \\  \underline{1011} \\  1011 \\  \underline{1011} \\  0  \end{array}  $ <p>A</p>	$  \begin{array}{r}  1011 \overline{) 10011101} \\  \underline{1011} \\  1011 \\  \underline{1011} \\  0001  \end{array}  $ <p>B</p>	$  \begin{array}{r}  1011 \overline{) 10111011} \\  \underline{1011} \\  1011 \\  \underline{1011} \\  0  \end{array}  $ <p>C</p>	$  \begin{array}{r}  1011 \overline{) 11111110} \\  \underline{1011} \\  1001 \\  \underline{1011} \\  1011 \\  \underline{1011} \\  0  \end{array}  $ <p>D</p>
---	--	---	---

图2 CRC 码字检错

●假设待传送数据的总长度为 2560 位，每个分组的长度为 256 位，其中头部开销长度为 16 位，源节点到目的节点之间的链路数为 4，每个链路上的延迟时间为 0.1 秒，数据传输率为 2560bps，线路交换建立连接的时间均为 0.2 秒，在分组交换方式下每个中间节点产生 25.6 位的延迟时间，则传送所有的数据，线路交换需时间为 (22) 秒，数据报分组交换所需时间则为 (23) 秒。

(22) A. 1.4

B. 10.6

C. 1.6

D. 1.2

(23) A. 1.54

B. 5.5

C. 5.83

D. 5.3

查看答案

C, C

查看答案

**分析：**线路交换，也称为电路交换，其传输时间的计算公式是：链路建立时间+链路延迟时间+数据传输时间。根据题意，链路建立时间为 0.2 秒；链路延迟时间=链路数×每链路延迟时间=4×0.1=0.4 秒；数据传输时间=数据总长度/数据传输率=2560B/2560bps=1 秒。因此总的传输时间=0.2+0.4+1=1.6 秒。

而采用数据报分组交换形式，其传输时间的计算公式显然是：(链路延时时间+中间结点延迟时间+分组传送时间)×分组数。根据题意，显然链路延迟时间=链路数×每链路延迟时间=4×0.1=0.4 秒；而中间结点延迟时间应=中间结点数×每中间结点延迟时间，中间结点数没有直接给出，但根据源点到目标共有 4 条链路，就可以得知中间结点应该是 4-1=3 个，每个中间结点延迟 25.6 位，因此其延迟时间就是 25.6 位/2560bps=0.01，因此中间结点延迟时间就=3×0.01=0.03 秒；而分组传送时间显然就=分组大小/数据传输率=256/2560bps=0.1 秒。这三者之和就是每个分组传输的时间，即 0.4+0.03+0.1=0.53 秒。最后，我们还要求出分组数，由于每个分组是 256 位，但其中有 16 位是头开销，因此实际可以装载的信息只有 256-16=240 位，而我们的数据报文的长度是 2560 位，因此其需要打包为 11 个分组，当然最后一个分组实际上没有达到最大值。因此采用数据报分组交换所需的时间=0.53×11=5.83 秒。

●在ATM网络中,信息交换的基本单位是(24),在其四层体系结构中,流量控制是由(25)负责的。在通信时,是使用虚通路标识符(VPI)和虚信道标识符(VCI)的组合来标识连接的,在做VP交换或交叉连接时(26)。ATM高层定义了4类5种业务类型,其中适合于突发式通信的是(27)。(28)是ATM所采用的拥塞措施之一。

- (25) A. 分组      B. 数据报      C. 位      D. 信元  
(26) A. ATM 高层      B. ATM 适配层      C. ATM 层      D. 物理层  
(27) A. VPI 变化, VCI 不变      B. VPI 不变, VCI 变化  
      C. VPI 不变, VCI 也不变      D. VPI 和 VCI 都变化  
(28) A. CBR      B. VBR      C. ABR      D. UBR  
(29) A. 采用 FECN、BECN 两个特殊字段实现显式前、后向拥塞控制  
      B. 采用 FECN 字段实现显式前向拥塞控制  
      C. 采用 BECN 字段实现显式后向拥塞控制  
      D. 采用 GFC 字段实现显式前向拥塞控制

查看答案

D, C, A, C, D

查看分析

**分析:** 在 ATM 网络中,信息的传输和交换基本单位是信元,它是定长的,53 个字节。ATM 整个体系结构由四层组成:(1) ATM 高层:对用户数据的控制;(2) ATM 适配层,包括为高层数据提供统一接口的汇聚子层,以及分割和合并用户数据的拆装子层;(3) ATM 层,负责虚通道和虚信道的管理、信元头的组装和拆分、信元的多路复用和流量控制;(4) 物理层,包括负责信元校验和速率控制、数据帧的组装和分拆的传输会聚子层,以及负责比特定时、物理网络接入的物理介质子层。

ATM 层相当于网络层的功能,它通过虚电路技术提供面向连接的服务。在 ATM 中,虚电路有两级:虚通路(VP)和虚信道(VC),在其逻辑通道中,是使用 VPI+VCI 的组合来标识连接的,在做 VP 交换或交叉连接时,只需要交换 VP,无需改变 VCI 的值。

ATM 定义了 4 类 5 种业务:适用于交互式语音和视频流的 CBR;适用于交互式压缩视频信号的 RT-VBR;适用于多媒体邮件的 NRT-VBR;适用于突发式通信的 ABR;以及适用于 IP 分组传送的 UBR。

[查看答案](#)

D, C, A, C, D

[查看答案](#)

**分析：**在 ATM 网络中，信息的传输和交换基本单位是信元，它是定长的，53 个字节。ATM 整个体系结构由四层组成：（1）ATM 高层：对用户数据的控制；（2）ATM 适配层，包括为高层数据提供统一接口的汇聚子层，以及分割和合并用户数据的拆装子层；（3）ATM 层，负责虚通道和虚信道的管理、信元头的组装和拆分、信元的多路复用和流量控制；（4）物理层，包括负责信元校验和速率控制、数据帧的组装和分拆的传输会聚子层，以及负责比特定时、物理网络接入的物理介质子层。

ATM 层相当于网络层的功能，它通过虚电路技术提供面向连接的服务。在 ATM 中，虚电路有两级：虚通路（VP）和虚信道（VC），在其逻辑通道中，是使用 VPI+VCI 的组合来标识连接的，在做 VP 交换或交叉连接时，只需要交换 VP，无需改变 VCI 的值。

ATM 定义了 4 类 5 种业务：适用于交互式语音和视频流的 CBR；适用于交互式压缩视频信号的 RT-VBR；适用于多媒体邮件的 NRT-VBR；适用于突发式通信的 ABR；以及适用于 IP 分组传送的 UBR。

ATM 为了能够尽量减少拥塞的强度、扩散程度及持续时间而采取了一系列拥塞控制措施，主要包括：（1）选择性信元丢弃，它与优先级控制类似，通过信元头的 CLP 字段来实现；（2）显式前向拥塞指示，它的工作方式与帧中继网络相同，一般是通过 GFC（流量控制）字段来实现的。

●基于Linux平台的应用系统开发中，不能够采用的中间件技术是(29)，在使用Web Services时，服务提供方需使用(30)来对外描述服务。

- (29) A. EJB                      B. DCOM                      C. CORBA                      D. Web Services  
(30) A. WDSL                      B. SOAP                      C. IDL                      D. UDDI

查看答案

B, A

查看分析

分析：最常见的中间件技术包括 COBRA, COM/DCOM, J2EE/EJB 和 Web Services，其中 COM/DCOM 是微软的技术，只限于在 Windows 系列平台使用，因此在 Linux 平台中无法使用。

Web Services 就是可以通过 Web 描述、发布、定位和调用的模块化应用，它是一个可以工作在 Internet 上的远程服务组件。首先，服务提供方使用 WDSL (Web 服务描述语言，类似于 IDL) 说明服务；然后使用 UDDI 发布服务；服务使用方也是使用 UDDI 查找服务；它们之间的访问与通信则是使用基于 HTTP 协议的 SOAP (简单对象访问协议) 协议。

● 在Linux中，    (31)    目录下的文件都不是真实存储在硬盘、软盘上的数据，在整个Linux系统中，目录树个数为    (32)    。

- (31) A. /dev 和 /proc      B. /dev 和 /mnt      C.      /dev      和      /var  
D. /proc 和 /mnt
- (32) A. 仅有 1 个      B. 和硬盘数相同      C. 和硬盘分区相同      D. 没有规律

查看答案

A, A

查看分析

(32) A. 仅有 1 个      B. 和硬盘数相同      C. 和硬盘分区相同      D. 没有规律

分析：这是一道实际应用题，主要考查了 Linux 下目录树的一些特性。在 Linux 中，/dev 目录存放的都是设备，每一个文件实际上就是指向一个设备；而 /proc 目录则是当前内存信息的一个映射。而 /mnt 则是一个默认的挂接目录，它是用来挂接外部存储设备上的文件系统的，如软盘、光盘。/var 则是一个用来存放易于增长的信息的目录。

在 Linux 操作系统中磁盘的管理是与 Windows 不同，它仅有一个目录树，所有的磁盘都将 mount（挂载）在目录树上使用。



● 在下列的加密算法中，不属于非对称加密算法（公钥加密算法）的是\_\_\_\_（32）\_\_\_\_，对于对称加密算法而言，存在的最大不足是\_\_\_\_（33）\_\_\_\_。

- （32） A. SDBI                      B. DH                      C. Elgamal                      D. ECC
- （33） A. 密钥的产生不便                      B. 密钥的使用不便
- C. 密钥的分发不安全                      D. 密文容易被破解

查看答案

A, C

查看分析

**分析：**本题的前一道是基础知识题，后一道则是工作原理题，主要考查了对称加密算法的主要代表和主要缺点。SDBI 是由山东大学网络信息安全研究所研制的具有自主知识产权的对称加密算法，该算法已经通过了国家密码委员会的批准。DH 算法是 Whitfield Diffie 和 Martin Hellman 提出的，是最早的公钥算法。Elgamal 算法既能够用于数据加密也能够用为数字签名，它是一种公钥算法，其安全性依赖于计算有限域上离散对数的困难性。ECC 是椭圆曲线加密算法的简称，其安全性也是基于离散对数计算的困难性，SET 协议的制订者已经将其作为缺省的公钥密码技术。

对于对称加密算法而言，其加密密钥和解密密钥是相同的（或者是可推导的），因此需要在加密者和解密者之间传递（分发）密钥，而这个过程正是最不安全的时候。



● 网络监视器软件 (33) 是只能够应用于以太网环境的，它能够支持大量的网络协议，但不支持 (34)。

(33) A. Ethereal      B. NetXRay      C. Sniffer      D. Tivoli

(34) A. NetBEUI      B. TCP/UDP      C. IP      D. IPX

查看答案

B, D

查看答案

**分析：**这是一道基础知识题，主要考查了网络监视器软件的一些基本知识。在网络维护时，我们经常需要监视网络数据流并对其进行分析，这也称为网络监视，而常见的网络监视器包括 Ethereal、NetXRay 和 Sniffer。其中 Ethereal 提供了对 TCP、UDP、SMB、telnet、ftp 等常用协议支持，覆盖了大部分应用需求。而 NetXRay 则主要是用做以太网络上的网管软件，能够对 IP、NetBEUI、TCP/UDP 等协议进行详细分析，但无法支持 IPX 协议。Sniffer 则是通过使网络接口处于混杂模式，以截获网络内容。它是最完善、应用最广泛的一种网络监视器。

● 以下关于病毒的描述中，正确的是 (39)；现有的反病毒方法大都还是遵循“检测、标识、清除”模式，它与最新的反病毒技术“主动内核”相比较，最大的不足是 (40)。

- (39) A. 宏病毒是一类新型的网络病毒，它会破坏各种 EXE、DLL 文件  
B. 网络病毒就是指通过 E-Mail 传播的病毒  
C. 蠕虫病毒的主要特点是利用网络中软件系统的缺陷进行自我复制和主动传播  
D. 启发式的扫描程序技术，对于新的病毒是没有办法的，必须更新特性库
- (40) A. 防治病毒的基础是建立在病毒入侵之后  
B. 它的查、杀病毒的速率要慢很多  
C. 对操作系统的依赖比较大一些  
D. 以上都不是

查看答案

C, A

查看分析

**分析：**这是一道工作原理题，主要考查了病毒的工作原理和“主动内核”技术的特点。对于前一个问题而言，解答时应该使用排除法。宏病毒是指利用 Office 或者类似的字处理系统中的宏编写的病毒，宏是一系列组合在一起的命令和指令，因此它只会感染微软的 Office 或者类似的字处理系统文档。而网络病毒不仅仅可以通过 E-Mail 传播，还可以通过软件系统的漏洞（如蠕虫病毒）、网页上的恶性脚本等方式传播。在启发式的扫描程序中，它是采用启发式规则和完整性检查，因此可以发现部分未知的病毒。

传统的反病毒技术，采用的是被动式防御理念。这种理念最大的缺点在于将防治病毒的基础建立在病毒侵入操作系统或网络系统之后，作为上层应用软件的反病毒产品才能够被动地防治病毒。而主动内核技术是将已经开发好的各种网络防病毒技术从源程序级嵌入到操作系统或网络系统的内核中，实现网络防毒产品与操作系统的无缝连接。

● 在Bind服务器中，用于配置DNS的数据文件是(41)，它将指定DNS的正向解析文件、反向解析文件和(42)。

(41) A. `named.boot`      B. `named.conf`      C. `db.域名`      D.  
`bind.conf`

(42) A. 指针文件      B. 配置文件      C. 缓存文件      D. 日志文件

查看答案

A, C

查看分析

分析：这是一道实际应用题，考查了Bind服务器的主要配置文件。在Bind中包括五个主要的配置文件，其中有两个比较核心：一是`/etc/named.boot`，用于设置DNS的数据文件，`named`启动时会自动读取；二是`/etc/named.conf`，是DNS服务器的主要配置文件。

而其它三个都是由`named.boot`指令的，包括：

- 正向解析文件：通过对每个域名有一个正向解析文件，用来指定其主机项，文件格式通常为`db.域名`；
- 反向解析文件：通常是一个IP地址段一个反向解析文件，用来指定IP→域名的解析；
- 缓存文件：通常为`db.cache`，用来缓存解析结果

● 在下面的关于Windows平台下安装DHCP服务器的描述中，正确的是(43)，如果要使用路由器另一端网络中的DHCP服务器，则应该(44)

- (43) A. 在 Windows 9x/Me/XP、Windows 2000/2002/2003 中均可安装 DHCP  
B. 在 Windows 平台中，已经默认安装了 DHCP 服务器组件  
C. 必须在 Windows 2000 以上版本，并添加“DHCP 服务”组件  
D. Windows 平台无法作为 DHCP 服务器
- (44) A. 在没有 DHCP 服务器的网络上做一个镜像服务器  
B. 在没有 DHCP 服务器的网络上做一个 DHCP 中继服务器  
C. 在有 DHCP 服务器的网络上做一个 DHCP 中继服务器  
D. 没有办法实现

查看答案

C, B

查看答案

**分析：**这是一道实际应用题，主要考查了 Windows 平台下的 DHCP 服务器安装以及跨路由器的 DHCP 应用。在 Windows 下安装 DHCP 服务器很简单，只需要安装了“网络服务”中的“动态主机配置协议 (DHCP)”组件即可。不过要注意的是只有 Windows 2000 Server 以上版本才有 DHCP 服务的功能，而且还需要具有静态 IP 地址。

DHCP 客户端向 DHCP 服务器发送的 IP 地址租用请求通常是不能够跨越路由器的（除非路由器支持 RFC1542 标准），如果想利用一台 DHCP 服务器给多个物理网段的计算机分配 IP 地址，就要求在没有 DHCP 服务器的网段创建一个 DHCP 服务器中继代理，它可以将本网段内客户端的 IP 地址租用请求发给 DHCP 服务器，起到一个“中继”作用。

● 我们在浏览器中输入的URL通常是“http://www.xxx.com/”，并没有指定具体的页面，而Web服务器将根据配置项\_\_\_\_(45)\_\_\_\_来决定回应什么页面；而为了改善交互的友好性，你可以定制一些出错提示页面，以在出现诸如“404 错误 文件未找到”等错误时，能够提供个性化的页面，这些页面存放的地方则通过配置项\_\_\_\_(46)\_\_\_\_进行设置。

(45) A. ServerRoot      B. DocumentRoot      C. DirectoryIndex      D. UserDir

(46) A. ErrorDocument      B. ErrorLog      C. UserDir      D.

DirectoryIndex

查看答案

C, A

查看分析

分析：这是一道实际应用题，考查了 Web 服务器 Apache 的常用配置项。当我们使用浏览器时，经常使用的 URL 是没有指定具体的页面名称的，特别是针对首页而言更是如此。而在 Web 服务器中，是允许对“首页的名称”进行设置，其格式为“DirectoryIndex 文件名 1 ……”，即一个搜索顺序。而我们可以通过“ErrorDocument 目录”来配置错误提示页面的位置。

● 在DNS中，将一个主机名对应于多个IP地址的技术称为（47）。在DNS服务器配置完成后，我们通常使用（48）命令来测试其工作是否正常。

(47) A. 负载均衡技术 B. 别名技术 C. 服务器群集技术 D. 镜像技术

(48) A. dnstest B. ping C. traceroute D.

nslookup

查看答案

B, D

查看分析

**分析：**这是一道基础知识题，考查了 DNS 的一种特殊用途与测试工具。在设置 DNS 记录时，可以使一个主机名对应多个 IP 地址，这可以实现最简单的负载均衡技术。对于 DNS 解析的请求，DNS 服务器会自动循环地应答不同的 IP 地址，从而将访问请求均衡地分布到不同的主机上。也可以将一个 IP 地址对应多个主机名，实现别名。而当 DNS 安装完成后，通常使用的是 nslookup 来测试其工作是否正常。

●在Linux下几乎都采用了Paul Vixie/ISC DHCPd来实现DHCP服务器端功能，其默认的配置文件的配置项“default-lease-time”的用途是

(49) A. dhcpd.conf B. dhcpd.boot C. dhcpd.leases D. dhcpd.cf

(50) A. 设置默认的租约时间 B. 设置默认的服务器响应时间  
C. 设置租约超时时间 D. 设置默认的自动断开时间

查看答案

A, A

查看分析

分析：这是一道实际应用题，考查了 DHCPd 的配置文件和基本配置项。DHCP 服务器的默认配置文件是 /etc/dhcpd.conf，租约数据库文件是 dhcpd.leases，默认目录为 /var/state/dhcp。从英文中就不难发现配置项“default-lease-time”的意思是设置默认的租约时间。

●TCP 使用三次握手协议来建立连接, 设甲乙双方发送报文的初始序号分别为 X 和 Y, 甲方发送 (51) 的报文给乙方, 乙方接收报文后发送 (52) 的报文给甲方, 然后甲方发送一个确认报文给乙方便建立了连接。(注: ACK的下标为捎带的序号)

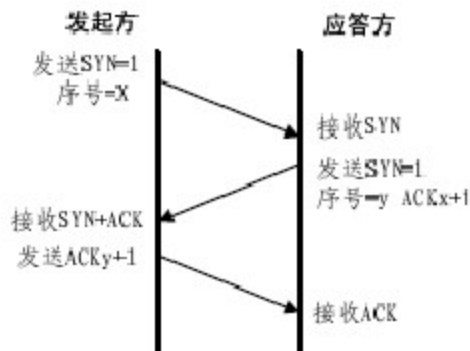
- (51) A. SYN=1, 序号=X                      B. SYN=1, 序号=X+1, ACK X=1  
C. SYN=1, 序号=Y                      D. SYN=1, 序号=Y, ACK Y+1=1
- (52) A. SYN=1, 序号=X+1                      B. SYN=1, 序号=X+1, ACK X=1  
C. SYN=1, 序号=Y, ACK X+1=1                      D. SYN=1, 序号=Y, ACK Y+1=1

查看答案

A, C

查看分析

分析: TCP 协议中的三次握手机制是实现 TCP 可靠连接的最核心机制。因此需要认真的理解和记忆。其过程如图 a 所示:



图a TCP协议的三次握手

整个过程是: 首先由发起方发送一个同步序号包 (将 SYN 置为 1, 并提供序号); 当应答方接收到同步序号包 (SYN) 时, 就对其进行肯定确认 (ACK 序号+1), 并发送自己的同步序号包 (将 SYN 置为 1, 并提供序号); 当发送方收到后, 则对其进行肯定确定 (ACK 序号+1), 以通知目的主机双方已完成连接建立。



●在下面关于VLAN的描述中，不正确的是（53）。

- (53) A. VLAN 把交换机划分成多个逻辑上独立的交换机  
B. 主干链路(Trunk)可以提供多个 VLAN 之间通信的公共通道  
C. 由于包含了多个交换机，所以 VLAN 扩大了冲突域  
D. 一个 VLAN 可以跨越多个交换机

查看答案

C

查看答案

VLAN 是交换机提供的一个很方便的功能，它可以将交换机上的端口分配到不同的逻辑网段，使它们处于不同的广播域。因此从某种意义上说，VLAN 的确是将交换机划分成了多个逻辑上独立的交换机。而在现有的交换机中，是允许一个 VLAN 跨越多个交换机的，这就是通过 VLAN Trunk 来实现的，即它提供了一个多个 VLAN 间通信的公共通道。而本题的 C 显然是错误的，不同 VLAN 的机器都不处于同一个广播域，更不属于同一个冲突域。

●在RIP协议中，默认的路由更新周期是(54)秒。而在这种距离矢量路由协议中，可以使用多种方法防止路由循环，以下选项中，不属于这些方法的是(55)。

- (54) A. 30 B. 60 C. 90 D. 100  
(55) A. 垂直翻转(flip vertical) B. 水平分裂(split horizon)  
C. 反向路由中毒(posion reverse) D. 设置最大度量值(metric infinity)

查看答案

A, A

查看答案

**分析：**这道题目考查的是路由更新周期与路由循环避免的相关知识。路由更新周期是常考知识点，RIP 是 30 秒，IGRP 是 90 秒，而 OSPF 则是通过每 10 秒发送一个 HELLO 包。而在路由循环的防范方面，距离矢量路由协议通常采用以下措施：

■ 设置最大度量值 (metric infinity)

也称为计数到无穷大。减小计数到无穷大影响的方法是定义无穷大。大多数距离矢量协议定义无穷大为 16 跳。这也是路由器如何通告网络不可达的一种方法。一个网络发生故障，不管它是毒性逆转路由，还是超过最大跳数 15 的路由，路由器将把所有跳数为 16 的路由看作是不可达的。

■ 水平分裂 (split horizon)

逆向路由 (reverse route)是指路由的指向与数据包流动方向相反的路由。水平分割是一种两台路由器之间阻止逆向路由的技术，这样做除了不会浪费资源，还有一个很重要的原因是不会把从路由器学习到的可靠信息再返回给这台路由器。动态路由选择协议最重要的功能是监测和抵消拓扑变化——如果到网络的最优路径不可用，协议就必须寻找下一个最优路径。执行水平分割可以阻止环路的发生，有两类水平分割的方法：简单水平分割法和毒性逆转分割法。

简单水平分割的规则是，当更新数据包被发送出某接口时，更新信息中不能包含从该接口接收的更新信息中获取到的网络。采用抑制信息的工作方式。

■ 反向路由中毒 (posion reverse, 也称为反向路由毒化)

而反向路由中毒法，就是指前面的毒性逆转分割法，其规则是当更新信息被发出某接口时，信息中将指定从该接口接收到更新信息中获取的网络是不可达的。

而实际上，并不存在垂直翻转这一概念。

●TCP 是一个面向连接的协议，它提供连接的功能是（56）的，采用（57）技术来实现可靠数据流的传送。为了提高效率，又引入了滑动窗口协议，协议规定重传（58）的分组，这种分组的数量最多可以（59），TCP协议采用滑动窗口协议解决了（60）。

- (55) A. 全双工            B. 半双工            C. 单工            D. 单方向
- (57) A. 超时重传            B. 肯定确认（捎带一个分组的序号）  
C. 超时重传和肯定确认（捎带一个分组的序号）    D. 丢失重传和重复确认
- (58) A. 未被确认及至窗口首端的所有分组            B. 未被确认  
C. 未被确认及至退回N值的所有分组            D. 仅丢失的
- (59) A. 是任意的            B. 1 个  
C. 大于滑动窗口的大小            D. 等于滑动窗口的大小
- (60) A. 端到端的流量控制            B. 整个网络的拥塞控制  
C. 端到端的流量控制和网络的拥塞控制    D. 整个网络的差错控制

### 查看答案

A, C, B, D, A

### 查看分析

**分析：**本题综合考查了 TCP 协议的基本机制。TCP 协议是一个面向连接的可靠传输协议，具有面向数据流、虚电路连接、有缓冲的传输、无结构的数据流、全双工连接五大特点。而实现可靠传输的基础是采用具有重传功能的肯定确认、超时重传技术，而通过使用滑动窗口协议则解决了传输效率和流量控制问题。

要注意的是，TCP 所采用的滑动窗口机制与“基本的滑动窗口机制”的最大不同是，TCP 滑动窗口允许随时改变窗口大小的，在每个确认中，除了指出已经收到的分组外，还包括一个窗口通告，用来说明接收方还能接收多少数据。通告值增加，发送方扩大发送滑动窗口；通告值减少，发送方缩小发送窗口。

●多协议标记交换(MPLS)是IETF提出的第三层交换标准,下面有关MPLS的描述中,正确的是 (61)。

- (61) A. MPLS 支持各种网络层协议, 带有 MPLS 标记的分组必须封装在 PPP 帧中传送  
B. MPLS 标记在各个子网中是特定分组的唯一标识  
C. 路由器可以根据转发目标把多个 IP 流聚合在一起, 组成一个转发等价类(FEC)  
D. 传送带有 MPLS 标记的分组之前先要建立对应的网络连接

查看答案

查看分析

**分析:** MPLS 是一种将二层交换与三层交换结合的新技术, 现在已经广泛地应用起来。在 MPLS 网络中, 在入口 LSR 处分组按照不同转发要求划分成不同转发等价类(FEC), 并将每个特定 FEC 映射到下一跳, 即进入网络的每一特定分组都被指定到某个特定的 FEC 中。每一特定 FEC 都被编码为一个短而定长的值, 称为标记, 标记加在分组前成为标记分组, 再转发到下一跳。在后续的每一跳上, 不再需要分析分组头, 而是用标记作为指针, 指向下一跳的输出端口和一个新的标记, 标记分组用新标记替代旧标记后经指定的输出端口转发。在出口 LSR 上, 去除标记使用 IP 路由机制将分组向目的地转发。

由于 MPLS 的标记栈封装可以定义在多种不同的媒质上, 栈顶的标记仍然可以沿用现有的格式, 如在 ATM 媒质上, 就可以沿用 VPI、VCI 作为栈顶的标记; 低一些级别的标记可以使用“夹层”或者叫“垫层”标记, 以消除不同媒质之间的差异。因此 A 显然是错误的。MPLS 标记在不同 LSR 上是不同的, 因此 B 也是错误的。而 C 中, 对 IP 流的描述显然是不正确的。

则传递标签需要建立专用连接, 而传递带有标签的分组时不需要建立对应的网络连接。相邻的 LSR 之间必须建立一条非 MPLS 连接链路作为信令通道, 用于传送 LDP 信令报文。因此 D 是正确的。

●在下面关于VLAN的描述中，不正确的是（62）。

- (62) A. VLAN 把交换机划分成多个逻辑上独立的交换机  
B. 主干链路(Trunk)可以提供多个 VLAN 之间通信的公共通道  
C. 由于包含了多个交换机，所以 VLAN 扩大了冲突域  
D. 一个 VLAN 可以跨越多个交换机

查看答案

C  
查看分析

分析：VLAN 是交换机提供的一个很方便的功能，它可以将交换机上的端口分配到不同的逻辑网段，使它们处于不同的广播域。因此从某种意义上说，VLAN 的确是将交换机划分成了多个逻辑上独立的交换机。而在现有的交换机中，是允许一个 VLAN 跨越多个交换机的，这就是通过 VLAN Trunk 来实现的，即它提供了一个多个 VLAN 间通信的公共通道。而本题的 C 显然是错误的，不同 VLAN 的机器都不处于同一个广播域，更不属于同一个冲突域。

●设信号的波特率为 600Baund，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，则信道的数据率为(63)。

(63) A. 600b/s                      B. 2400b/s                      C. 4800b/s                      D. 9600b/s

查看答案

B

查看分析

**分析：**这道题就是一个典型的尼奎斯特定律应用的实例，根据该公式要确定两个值，一是波特率，二是码元种类。显然在本题中，波特率和码元都已经明确地指出，因此显然可以套用公式计算： $R=600\text{Baund} \times \log_2 16=2400\text{b/s}$ 。

●在一个带宽为 3KHZ、没有噪声的信道，传输二进制信号时能够达到的极限数据传输率为(64)。一个带宽为 3KHZ、信噪比为 30dB 的信道，能够达到的极限数据传输率为(65)。上述结果表明，(66)。

- (64) A. 3Kbps                      B. 6Kbps                      C. 56Kbps                      D. 10Mbps
- (65) A. 12Kbps                      B. 30Kbps                      C. 56Kbps                      D. 10Mbps
- (66) A. 有噪声信道比无噪声信道具有更大的带宽  
B. 有噪声信道比无噪声信道可达到更高的极限数据传输率  
C. 有噪声信道与无噪声信道没有可比性  
D. 上述值都为极限值，条件不同，不能进行直接比较

查看答案

B, B, D

查看分析

分析：这道题结合了尼奎斯特和香农两个理论。对于第一空而言，显然应根据尼奎斯特定律，得到其极限数据传输率是 2W，即  $2 \times 3K = 6Kbps$ 。而第二空显然适用于香农理论，其可达到的极限数据传输率，套用公式计算为： $3000 \times \log_2 1001 \approx 3000 \times 9.97 \approx 30Kbps$ 。



● 在对一个项目进行计划时，首先要做的一件事就是对工作进行分级分解，即(67)，如果这种分级分解是根据时间来进行，那么称为(68)。

- (67) A. WBS                      B. PERT                      C. WorkList                      D. WBL
- (68) A. 横向分解                      B. 纵向分解                      C. 阶段分解                      D. 粒度分解

查看答案

A, B

查看分析

**分析：**本题是一种概念比较题，考查了项目管理中的工作分解结构（WBS）的基本知识。在做项目计划时，识别项目活动是十分关键的。这这通常使用工作分解结构（WBS）来实现。它包括两种分解的方式，一是纵向分解，即按时间轴分解，按工作阶段进行分解；二是横向分解，即按功能轴分解，按工作产品进行分解。



● 根据信息资源管理的观点，负责完成数据的采集、数据变换和数据存储等工作的是 (69)。信息化体系的六个要素是：信息资源、(70)、信息技术应用、信息产业、信息化人才和信息化政策法规及标准规范。

(69) A. 信息源                      B. 信息处理者                      C. 信息使用者                      D. 信息管理者

(70) A. 信息系统                      B. 信息网络                      C. 信息平台                      D. 信息技术

查看答案

B, B

查看答案

**分析：**这是一道基本概念题，考查了信息化基础概念。从信息资源管理的观点出现，信息系统的逻辑结构一般由四个部分组成：

- 信息源：信息发生的来源；
- 信息处理器：完成数据的采集、数据变换和数据存储等；
- 信息使用者：是企业不同部门和不同层次的管理人员；
- 信息管理者：是指负责管理信息系统开发和运行的人员。

而信息化则是以信息资源开发利用为核心，以网络技术、通信技术等高科技技术为依托的一种新技术扩散的过程。信息化体系的六个要素是：信息资源、信息网络、信息技术应用、信息产业、信息化人才和信息化政策法规及标准规范。

● XML is a text-based markup language that is fast becoming the standard (71) data interchange on the Web. As with HTML, you (72) data using tags (identifiers enclosed in angle brackets, like this: <...>). Collectively, the tags are known as "markup".

But (73) HTML, XML tags identify the data, rather than specifying how to display it. Where an HTML tag says something like "display this data in bold font" (<b>...</b>), an XML tag (74) like a field name in your program. It puts a label on a piece of data that identifies it (for example: <message>...</message>).

In the same way that you (75) the field names for a data structure, you are free to use any XML tags that make sense for a given application.

- |                    |             |             |                 |
|--------------------|-------------|-------------|-----------------|
| (71) A. of         | B. for      | C. to       | D. as           |
| (72) A. use        | B. look for | C. identify | D. marker       |
| (73) A. likely     | B. like     | C. unlike   | D. unlikely     |
| (74) A. act        | B. look     | C. perform  | D. consummation |
| (75) A. definition | B. fill     | C. made up  | D. define       |

查看答案

B, C, C, A, D

查看分析

**分析:**XML 是一种基于文本的标记语言,它正迅速成为 Web 上的数据交换标准(standard for data interchange)。像 HTML 一样,你可以用标签来鉴别(identify)数据,各种各样的标签统称为“标记”。

与 HTML 不同(unlike)的是,XML 标签用来标识数据,而不是说明如何显示它。例如,在 HTML 语言中用标记<b>...</b>表示“使用粗体显示数据”,而 XML 则使用字段名来完成(act)这一功能。它在数据中设置一个标签来标记它(如:<message>...</message>)。同样,你也可以为数据结构定义(define)字段名,对一个给定的应用,可以用任意的 XML 标记来完成。