●假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包。这时你使用哪一种类型的进攻手段？（1）

（1）A. 缓冲区溢出　　B. 地址欺骗　　C. 拒绝服务　　D. 暴力攻击

查看答案

B

查看分析

**分析：**

本题考查网络攻击的知识。网络攻击的第一步就是隐藏自己的位置；第二步是寻找目标主机并分析目标主机；第三步是获取账号和密码，登录主机；第四步是获得控制权；第五步是窃取网络资源和特权。

●病毒是一项经常性的工作，下列不属于关键因素的是（2）。

（2）A. 加强计算机系统的管理　　B. 不使用计算机移动优盘

C. 注意病毒入侵的预防措施　　D. 切断病毒传播的途径

查看答案

B

查看分析

**分析：**

本题考查病毒防治常识。抗病毒工作的关键在于加强计算机系统的管理，注意病毒入侵的预防措施，尽量控制移动磁盘交换的对象和范围，加强对程序做带病毒情况下的检查和测定，以防止计算机病毒的进一步扩散等。

●对于计算机或网络安全的攻击中，通信量分析属于__（3）__。

（3）A. 被动攻击　　B. 主动攻击　　C. 中断　　D. 假冒

查看答案

A

查看分析

**分析：**

本题考查网络攻击的类型知识。被动攻击的特点是偷听或监视传送，其目的是获得正在传送的信息，被动攻击有泄露信息内容和通信量分析等；主动攻击涉及修改数据流或创建错误的数据流，包括假冒、重放、修改消息和拒绝服务等；中断是指系统资源遭到破坏或变得不能使用，这是对可用性的攻击，例如对一些硬件进行破坏、切断通信线路或禁用文件管理系统；假冒是一个实体假装成另一个实体。假冒攻击通常包括一种其他形式的主动攻击，例如，在发送身份验证序列时，可以捕获身份验证序列并重新执行，这样通过扮演具有特权的实体，几乎没有特权的实体获得了额外的特权。

●下列行为不属于网络攻击的是__(4)__。

(4) A. 连续不停地 Ping 某台主机　　B. 发送带病毒和木马的电子邮件

C. 向多个邮箱群发一封电子邮件　　D. 暴力破解服务器密码

查看答案

C

查看分析

**分析：**

本题考查网络攻击的形式知识。常见的网络攻击形式有如：窃取口令、缺陷和后门、鉴别失败、协议失败、信息泄露、拒绝服务等。

●如果一个登录处理子系统允许处理一个特定的用户识别码，以绕过通常的口令检查。这种威胁属于__（5）__。

（5）A. 假冒　　B. 授权侵犯　　C. 旁路控制　　D. 陷门

查看答案

D

查看分析

**分析：**

本题考查网络攻击特征知识。陷门：是在某个系统或某个文件中设置的“机关”，使得当提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许处理特定的用户识别码，以绕过通常的口令检查。假冒：这是多数黑客采用的攻击方法。某个未授权实体使守卫者相信它是一个合法的实体，从而获取该合法用户的特权。旁路控制：攻击者通过各种手段发现本应保密却又暴露出来的一些系统“特征”，利用这些“特征”，攻击者绕过防线守卫者渗入系统内部。授权侵犯：也称为“内部威胁”，授权用户将其权限用于其他未授权的目的。

●下列关于网络安全P2DR模型说法不正确的是__（6）__。

（6）A. P2DR 模型称为动态信息安全理论的主要模型

B. P2DR 模型是 TCSEC 模型的发展，也是目前被普遍采用的安全模型

C. P2DR 模型有自己的理论体系，采用的数学模型是基于时间的安全理论

D. 根据 P2DR 模型的理论，安全策略不是整个网络安全的依据

查看答案

D

查看分析

**分析：**

本题考查网络安全模型知识。P2DR 模型是可适应网络安全理论或称为动态信息安全理论的主要模型。P2DR 模型是 TCSEC 模型的发展，也是目前被普遍采用的安全模型。P2DR 模型有自己的理论体系，有数学模型作为其论述基础——基于时间的安全理论（Time Based Security）。根据 P2DR 模型的理论，安全策略是整个网络安全的依据。

●在无线局域网中，客户端设备用来访问接入点（AP）的唯一标识是__（7）__。

（7）A. BSSID　　B. ESSID　　C. SSID　　D. IP 地址

查看答案

C

查看分析

**分析：**

IP 地址用于网络层寻址，与本题解答没有关系。前三个备选答案中，BSSID 和 ESSID 都是以 SSID 为基础的。

根据无线局域网的的规模和组成，可以使用多种方式标识无线 LAN。

SSID（Service Set Identifier，服务集标识符）：也称为网络名称，用来区分不同的无线网络，网络上的所有无线设备都必须使用同一个 SSID。SSID 最多可以有 32 个字符，无线网卡设置了不同的 SSID 就可以进入不同网络，SSID 通常由无线 AP 广播出来，通过无线网卡扫描可以查看当前区域内的 SSID。若出于安全考虑，可以不广播 SSID，此时用户就要手工设置 SSID 才能进入相应的网络。

BSSID（Basic Service Set Identifier，基本服务集标识符）：每个无线设备的唯一标识符。BSSID 是设备的以太网 MAC 地址。

ESSID（Extended Service Set Identifier，扩展服务集标识符）：ESSID 是 SSID 的特例，用于标识包含接入点的无线网络。

●某家庭需要通过无线局域网将分布在不同房间的三台计算机接入Internet，并且ISP只给其分配一个IP地址。在这种情况下，应该选用的设备是__(8)__。

（8）A. AP　　B. 无线路由器　　C. 无线网桥　　D. 交换机

查看答案

B

查看分析

**分析：**

交换机是有线局域网常用的设备，AP、无线路由器和无线网桥都属于无线局域网设备。

AP（Access Point，无线接入点）相当于一个连接有线网和无线网的桥梁，是无线局域网客户端计算机进入有线网络的接入点，主要用于宽带家庭、大楼内部以及园区内部，典型距离覆盖几十米至上百米。

无线路由器是同时兼具无线 AP 和路由器功能的一种无线局域网设备，它借助于路由器功能，可实现无线局域网中的 Internet 连接共享等功能。

无线网桥的主要功能是无线桥接和无线中继，通常用于室外，主要用于实现两个或多个网络之间桥接。无线网桥除了具备有线网桥的基本特点之外，比有线网络设备更方便部署。

●采用IEEE 802.11 标准的对等解决方案，将 4 台计算机连成一个无线局域网，如果要求该无线局域网与有线局域网连接，并保持对等解决方案不变，其解决方法是（9）。

（9）A. 增加 AP　　B. 无解决方法

C. 其中一台计算机再安装一块无线网卡

D. 其中一台计算机再安装一块以太网卡

查看答案

D

查看分析

**分析：**

在 IEEE 802.11 标准的对等解决方案（即 Ad-hoc 模式）中，网络中所有结点的地位平等，无须设置任何的中心控制结点，计算机只要装上无线网卡而不必使用接入点设备，就可以达到相互连接、资源共享的目的。在该方案中，增加 AP 和在其中一台计算机中再安装一块无线网卡都无法解决无线局域网与有线局域网连接，解决方法是在其中一台计算机中再安装一块以太网卡。

●局域网交换机增加带宽的方法是在交换机的多个端口之间建立（10）。

（10）A. 全连接　　B. 会话连接　　C. 并发连接　　D. 数据连接

查看答案

C

查看分析

**分析：**

交换局域网的核心部件是它的局域网交换机。典型的交换局域网是交换式以太网（Switch Ethernet），其核心部件是以太网交换机（Ethernet Switch）。Ethernet Swich可以有多个端口，每个端口可与一个结点连接，也可与一个共享式 HUB 连接。交换局域网每个端口提供 10Mbps 或 100Mbps 的带宽，可以通过 Ethernet Switch 支持交换机端口之间的多个结点开放连接，实现多个结点之间数据的并发传输，因此增加了局域网带宽，改善了局域网的性能。

在典型的交换局域网中，结点可以通过点-点线路与局域网交换机连接，局域网交换机可以在多对通信结点之间建立并发的逻辑连接。

●　（11）　就是在系统发生意外（如黑客攻击、病毒感染、操作失误、软件错误等）的情况下的应急处理方案，是为网络安全设置的最后一到防线。

（11）A. 防火墙　　B. 加密　　C. 入侵检测　　D. 网络备份

查看答案

D

查看分析

网络备份就是在系统发生意外（如黑客攻击、病毒感染、操作失误、软件错误等）的情况下的应急处理方案，是为网络安全设置的最后一到防线。

网络备份的最终目的是保障网络系统安全运行，在网络发生意外时能够迅速、完全地将网络系统恢复到正常状态。网络系统双机热备份能保障网络系统发生问题时在几乎零时间内恢复网络服务，而网络系统数据冷备份则是将系统数据从备份设备完整地还原到网络系统，数据的恢复是非实时的，需要一定时间。

对重要的系统，还应考虑异地容灾技术，以期抵御自然灾害（如地震、火灾等）、战争以及恐怖袭击等灾难。这些灾难将导致本地数据中心毁灭性的破坏。此时，必须依赖完善的异地系统容灾措施才能保证本地数据中心的信息安全。

●美国国防部安全标准定义了 4 个安全级别，其中最高安全级别提供了最全面的安全支持，它是 （12） 。

(12)A. A 级　　B. B 级　　C. C 级　　D. D 级

查看答案

A

查看分析

**分析：**

本题考查可信计算机评估准则知识。可信计算机系统评估准则将计算机系统的安全可信度从低到高分为 D、C、B、A 四类共七个级别：D 级、C1 级、C2 级、B1 级、B2 级、B3 级、A1 级。

●IEEE 802.11 定义了无线局域网的两种工作模式，其中（13）模式是一种点对点连接，不需要无线接入点和有线网络的支持，用无线网卡连接的设备之间就可以直接通信。

(13)A. Roaming　　B. Ad-hoc

C. Infrastructure　　D. DiffuseIR

查看答案

B

查看分析

**分析：**

IEEE 802.11 定义了无线局域网的两种工作模式：对等网络（Ad-hoc）模式和结构化网络（Infrastructure）模式。

在 Ad-hoc 模式（也称为点对点模式）下，无线客户端直接相互通信，不使用无线 AP。使用 Ad-hoc 模式通信的两个或多个无线客户端就形成了一个独立基础服务集（Independent Basic Service Set，IBSS）。Ad-hoc 模式用于在没有提供无线 AP 时连接无线客户端。

在 Infrastructure 模式下，至少存在一个无线 AP 和一个无线客户端。无线客户端使用无线 AP 访问有线网络的资源。有线网络可以是一个机构的 Intranet 或 Internet，具体情况取决于无线 AP 的布置。

支持一个或多个无线客户端的单个无线 AP 称为一个基础服务集（Basic Service Set，BSS）。一组连接到相同有线网络的两个或多个 AP 称为一个扩展服务集（Extended Service Set，ESS）。一个 ESS 是单个逻辑网段（也称为一个子网），并通过它的服务集标识符（Service Set Identifier，SSID）来识别。如果某个 ESS 中的无线 AP 的可用物理区域相互重叠，那么无线客户端就可以漫游，或从一个位置（具有一个无线 AP）移动到另一个位置（具有一个不同的 AP），同时保持网络层的连接。

●用RSA算法，网络中N个用户之间进行加密通信，需要的密钥个数是__(14)__。

(14)A.N*(N-1)　　B.N　　C.2N　　D.N*N

查看答案

C

查看分析

**分析：**

本题考查信息密码学技术知识。密码学中所出现的密码体制可分为两大类：对称加密体制和非对称加密体制。DES 是最典型的对称加密算法。对称加密算法的优点是加密、解密处理速度快，保密度高等。缺点是多人通信时密钥组合的数量会出现爆炸性膨胀，使密钥分发更加复杂化，N 个人进行两两通信，总共需要的密钥数为 N(N-1)/2 个。非对称加密体制最典型的代表是 RSA。非对称加密体制的优点是网络中的每一个用户只需要保存自己的私有密钥，则 N 个用户仅需产生 N 对密钥。密钥少，便于管理。缺点是与对称加密体制相比，非对称加密体制的加密、解密处理速度较慢，同等安全强度下非对称加密体制的密钥位数要求多一些。

●下面哪种加密算法不属于对称加密__(15)__。

(15)A. DES　　B. IDEA　　C. TDEA　　D. RSA

查看答案

D

查看分析

**分析：**

本题考查加密算法知识。目前，已有一些比 DES 算法更安全的对称加密算法，如 IDEA、TDEA、RC2 算法、RC4 算法与 Skipjack 算法等。

●下列关于RSA说法中，错误的是__(16)__。

(16)A. RSA 是至今为止理论上最为成熟的公钥密码体制

B. RSA 是一种公钥体制

C. RSA 体制基于 Euler 定理

D. RSA 的加密、解密速度比 DES 快

查看答案

D

查看分析

**分析：**

本题考查密码学的基本知识。RSA 公钥密码是 1977 年由 Ron Rivest、Adi Shamirh 和 LenAdleman 提出的一个公开密钥密码体制。RSA 就是以其发明者的首字母命名的 RSA 体制，被认为是迄今为止理论上最为成熟完善的一种公钥密码体制。该体制的构造基于 Euler 定理，它利用了如下的基本事实：寻找大素数是相对容易的，而分解两个大素数的积在计算上是不可行的。RSA 的加密、解密速度比 DES 慢。

●用户A通过计算机网络向用户B发消息，表示自己同意签订某个合同，随后用户A反悔，不承认自己发过该条消息。为了防止这种情况，应采用__(17)__。

(17)A. 数字签名技术　　B. 消息认证技术

C. 数据加密技术　　D. 身份认证技术

查看答案

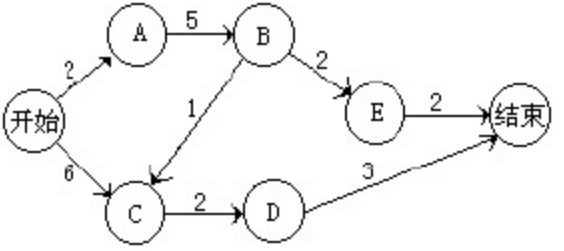
A

查看分析

**分析：**

本题考查网络安全技术应用知识。数字签名是一种使用加密认证电子信息的方法，是以电子形式存储的一种消息，可以在通信网络中传输。消息认证就是验证所收到的消息确实是来自真正的发送方且未被修改的消息，也可以验证消息的顺序和及时性。密码技术的应用是当今信息安全的主流技术，同时也是证书管理系统的核心安全技术。加密用来保护敏感信息的传输，保证信息的安全性。身份认证是指计算机及网络系统确认操作者身份的过程。在信息系统中，一般来说，有三个要素可以用于认证过程，即：用户的知识，如口令等；用户的物品，如 IC 卡等；用户的特征，如指纹等。

● 下面的网络图中，关键路径是__(18)__。




(18) A. 开始-A-B-E-结束　　B. 开始-C-D-结束

C. 开始-A-B-C-D-结束　　D. 确定关键路径的信息不充分

查看答案

C

查看分析

**分析：**

关键路径是最长的路径，你可以通过把每条可能的路径从开始到结束途中的数字相加来确定。

●项目范围根据__(19)__进行评定，而产品范围则根据__(19)__进行评定。

(19) A. 计划；要求　　B. 要求；成功的评定标准

C. 合同；核实　　D. 范围基准计划；范围定义

查看答案

A

查看分析

**分析：**

项目范围是否完成以项目管理计划为衡量标准，而产品范围是否完成以产品需求为衡量标准。

● 项目范围确认是指项目干系人对项目范围的正式确认，项目范围确认是__(20)__。

(20) A. 发生在可行性分析阶段　　B. 仅在启动阶段

C. 仅在制定项目计划阶段　　D. 贯穿于整个项目生命周期

查看答案

D

查看分析

**分析：**

项目范围确认贯穿于整个项目生命周期，从开始项目管理组织确认 WBS 的具体内容，到项目各个阶段的交付物检验，直至最后项目收尾文档验收，甚至最后项目评价的总结。

● IPSec VPN是基于__(21)__的。

(21) A. 网络　　B. 设备　　C. 应用　　D. 数据源

查看答案

B

查看分析

**分析：**

IPSec VPN 是基于设备的，而不是基于网络的，提供商无需对路由器进行额外的配置。

● CA（认证机构）的主要职责不包括__(22)__。

(22) A. 数字证书管理　　B. 证书和证书库

C. 清空密钥　　D. 交叉认证

查看答案

C

查看分析

**分析：**

CA（认证机构）的主要职责包括：数字证书管理、证书和证书库、密钥备份及恢复、密钥和证书的更新、证书历史档案、客户端软件、交叉认证。

● 甲企业投资研发出某一新软件产品，并投入销售。甲企业技术核心人员被乙企业高薪挖走，在甲企业之后三个月后，乙企业依据该技术核心人员的技术也开发出同样的新产品，正确的论述是__(23)__。

(23) A. 乙企业不侵权，该技术核心人员侵权

B. 乙企业侵权，该技术核心人员不侵权

C. 乙企业和该技术核心人员均侵权

D. 乙企业和该技术核心人员均不侵权

查看答案

C

查看分析

**分析：**

乙企业和该技术核心人员均侵权，非法获取了商业秘密，并由此获利。

● 我国标准与国际标准的对应关系有：等同采用(idt)、修改采用(mod)、等效采用(eqv)、非等效采用(neq)，其中__(24)__指技术内容相同，没有或仅有编辑性修改，编写方法完全对应。

(24) A. 等同采用(idt)　　B. 修改采用(mod)

C. 等效采用(eqv)　　D. 非等效采用(neq)

查看答案

A

查看分析

**分析：**

等同采用指技术内容相同，没有或仅有编辑性修改，编写方法完全对应。

●在空战训练中甲机先向乙机开火，击落乙机的概率为0.2；若乙机未被击落，就进行还击，击落甲机的概率是0.3；若甲机未被击落，则再进攻乙机，击落乙机的概率为0.4。那么甲机被击落的概率为（25），乙机被击落的概率为（26）。

（25）A. 0.06　　B. 0.14　　C. 0.24　　D. 0.56

（26）A. 0.324　　B. 0.424　　C. 0.524　　D. 0.624

查看答案

C, B

查看分析

**分析：**

设A表示“甲机被击落”这一事件，则A发生只可能在第2回合中发生，而第2回合又只能在第1回合甲失败了才可能进行，用Ai表示第i回合设计成功(i=1，2，3)，B表示“乙机被击落“的事件，则A=$\overline{A1}A2$，B=$A1+\overline{A1A2}A3$，利用乘法定理得：

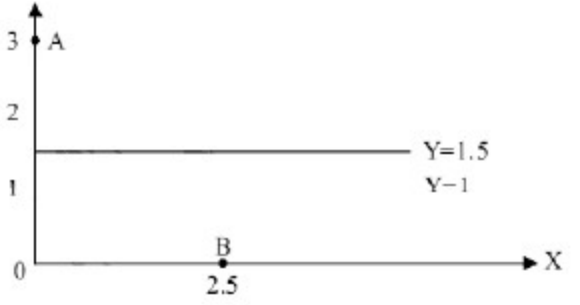
（1）P(A)=P($\overline{A1}A2$)=P($\overline{A1}$)P(A2|$\overline{A1}$)=0.8*0.3=0.24

（　　2　　）

P(B)=P($A1+\overline{A1A2}A3$)=P($A1$)+P($\overline{A1A2}A3$)=P($A1$)+P($\overline{A1}$)P($\overline{A2}$|$\overline{A1}$)+P(A3|$\overline{A1}\,\overline{A2}$)=

0.2+0.8*0.7*0.4=0.424

● 如图，希赛公司的厂区 A（有空气污染）与生活区 B 拟建于一条大河的两侧，其坐标表示大致为（单位：公里）：厂区位于点A(0，3)，生活区位于点B(2.5，0)，河的两岸分别为直线Y=1 与Y=1.5。为方便希赛公司职工在厂区与生活区之间来往，还需要在该条河上建一座垂直于两岸的桥。为使希赛公司职工通过该桥往来厂区与生活区之间的距离最短，桥应建在坐标X=__(27)__处。




（27）A. 1　　B. 1.25　　C. 1.5　　D. 2

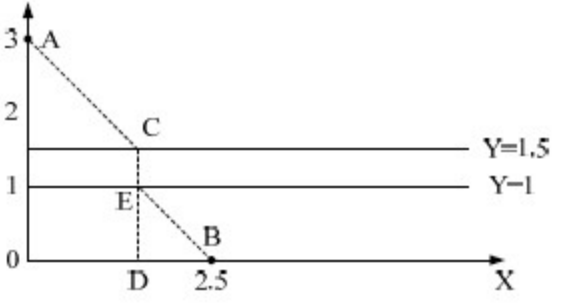
查看答案

C

查看分析

**试题分析**

因为试题规定了“该条河上建一座垂直于两岸的桥”，我们假设桥的横坐标为 D，如下图所示。



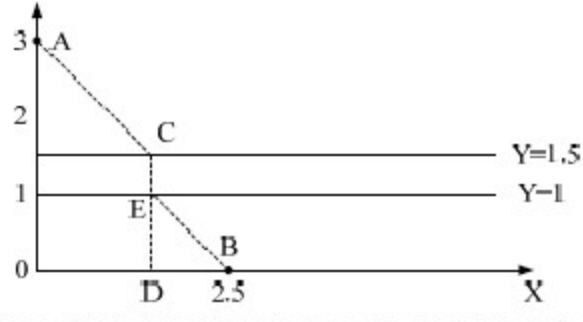
查看答案

C

查看分析

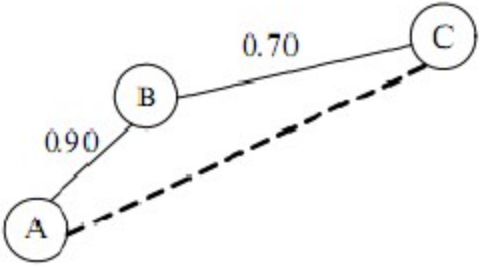
**试题分析**

因为试题规定了“该条河上建一座垂直于两岸的桥”，我们假设桥的横坐标为 D，如下图所示。




由上图可知，希赛公司的职工通过该桥往来厂区与生活区之间的距离为 S=BE+EC+CA，其中 EC=1.5-1=0.5。根据直角三角形的性质，BE=$\sqrt{1+(2.5-D)^2}$，CA=$\sqrt{1.5^2+D^2}$，因此，S=$\sqrt{1+(2.5-D)^2}+\sqrt{1.5^2+D^2}+0.5$。那么，我们的问题就转化为如何确定 D，使 S 的取值最小。把试题的 4 个选项逐一代入，可以得出当 D=1.5 时，S 的取值最小。

● 从A村通过B 村再到C 村已有一条通信线路。A村与B村间通信线路的可靠度为 0.90，B村与C村间通信线路的可靠度为 0.70。现在计划在A村与C村之间再直接建一条新的通信线路（见下图）。试问，这条新建通信线路的可靠度至少应该为__(28)__时，才使A村与C村之间的通信可靠度能达到 0.90 以上。




（28）A. 0.27　　B. 0.37　　C. 0.63　　D. 0.73

查看答案

D

查看分析

**试题分析**

在新的通信线路未建立之前，A 村与 C 村之间的通信可靠度为 0.90*0.70=0.63。新建一条通信线路后，就相当于新建的线路与原来的线路组成一个并联系统。并联系统的可靠性计算方法为：设系统各个子系统的可靠性分别用 $R_1, R_2, ..., R_n$ 表示，则系统的可靠性

$R = 1-(1-R_1)\times(1-R_2)\times...\times(1-R_n)$。

假设新建通信线路的可靠度为 x，则其建设好后，A 村与 C 村之间的通信可靠度为 1-(1-0.63)*(1-x)，题目要求这个结果要达到 0.90 以上，因此，1-(1-0.63)*(1-x)>0.90，解这个不等式，可以得到 x>0.73。

● 根据OSI网络管理标准的内容，下列功能中不属于计费管理的是__（29）__，它应该归属于__（30）__。

（29）A. 用户分组管理与访问控制　　B. 数据分析与费用计算
　　C. 数据查询　　D. 政策比较与决策支持

（30）A. 配置管理　　B. 故障管理　　C. 性能管理　　D. 安全管理

查看答案

A, D

查看分析

**分析：**这是一道基本概念题，主要考查了 OSI 网络管理标准中定义的五大功能的归属判断。计费管理：包括计费数据采集、数据管理与数据维护、计费政策制定、政策比较与决策支持、数据分析与费用计算、数据查询。因此，显然不包括用户分组管理与访问控制。

而管理员身份认证（公钥认证，局域网内的信任用户，可用简单口令认证）、管理信息存储和传输的加密与完整性（SSL、加密、消息摘要）、网络管理用户分组管理与访问控制、系统日志分析、网络资源的访问控制（访问控制链表）、告警事件分析（发现可疑的攻击迹象）、主机系统的安全漏洞检测均属于安全管理的内容。

● 在以下事件中，会触发Trap报文的是__（31）__，在SNMP中，用于请求改变管理代理上的某些对象的报文是Set-Request，那么在SNMP管理进程中，如果要想了解这个报文发出后该对象是否改变，则应该使用__（32）__。

（31）A. 该对象中不存在管理进程要检索的变量

B. 收到管理进程发出的 Get-Request 报文

C. 报文认证失败

D. 收到管理进程发出的 Get-NextRequest 报文

（32）A. 从代理回应的 Get-Response 报文中获得

B. 从代理主动发出的的 Trap 报文中获得

C. 主动向代理发送 Get-NextRequest 报文进行查询

D. 主动向代理发送 Get-Request 报文进行查询

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 SNMP 协议中五种 PDU 的工作模式。在 SNMP 协议规范中，Trap 是一种报警机制，也就是在管理进程未和代理进行通信时，代理有“紧急情况”需要汇报时的一个“热线电话”。因此，只要是在与管理进程交互时，都不可能触发 Trap 报文。因此不管是该对象中不存在管理进程要检索的变量，还是收到管理进程发出的 Get-Request 报文、Get-NextRequest 报文，都不可能出现 Trap，事实上应对 Get-Request 和 Get-NextRequest 的报文应该是 Get-Response。

后一个问题则灵活地考查了考生对 SNMP 五种协议数据单元的理解情况。Set-Request 是由管理进程发出，用来请求改变管理代理上的某些对象的。而 Get-Response，则是当管理代理收到管理进程发送的 Get-Request、Get-NextRequest 或 Set-Request 报文时，将会回应一个这种报文。

● 在RMON2协议中，对RMON 1 MIB的基础上（33），它对于矩阵组进行了相应的扩展，（34）。

（33）A．删减了部分，增加了部分　　B．重新定义了10个组

C．新增加了9个组　　D．拆分了部分组，总体数量增加了

（34）A．拆分为网络层矩阵组和应用层矩阵组两个组

B．增加了网络层矩阵组　　C．增加了应用层矩阵组

D．增加了网络层矩阵组和应用层矩阵组两个组

**分析**：这是一个工作原理题，主要考查了RMON 2对RMON 1的相关扩展。RMON 2扩充了原来的RMON MIB，增加了9个新的功能组。这9个新的功能组是：协议目录组、协议分布组、地址映像组、网络层主机组、网络层矩阵组、应用层主机组、应用层矩阵组、用户历史组、监视器配置组。

查看答案

C,D

查看分析

**分析**：这是一个工作原理题，主要考查了RMON 2对RMON 1的相关扩展。RMON 2扩充了原来的RMON MIB，增加了9个新的功能组。这9个新的功能组是：协议目录组、协议分布组、地址映像组、网络层主机组、网络层矩阵组、应用层主机组、应用层矩阵组、用户历史组、监视器配置组。

● 小张在某在线商场中订购了一台打折的数码相机，并选择了货到付款，结果商家却给他送来了一台新上市、价格高昂的数据相机，而且还提供了小张当时的订货凭证，对于这种现象，我们一般将其归为__（35）__问题。后来，他还发现有许多冲印店给他打电话，推销数码冲印服务，究其原因，原来是有黑客将在线商场的信息偷出来，卖给冲印店们，这种现象通常可归为__（36）__问题。

（35）A．有效性　　B．数据完整性　　C．不可抵赖性　　D．不可审查性

（36）A．有效性　　B．机密性　　C．数据完整性　　D．不可抵赖性

查看答案

B, B

查看分析

**分析：**这是一道基础知识题，主要考查了电子商务安全的几个不同的方面。电子交易的安全需求主要包括有效性、机密性、数据完整性、不可抵赖性和审查能力。

数据完整性是指要求能够保证数据的一致性，防止数据被非授权者建立、修改和破坏。而显然在本题案例中，就是因为交易数据被非法篡改而产生的问题。机密性则是要预防非法的信息存取和信息在传输过程中被非法窃取。而后一个案例显然是因为黑客的行为使得个人隐私信息被泄露。

● 能够使得交易双方都不能够抵赖的安全协议是（37），而仅限于Web应用的安全协议是（38）。

（37）A. SSL　　B. SET　　C. SHTTP　　D. DES

（38）A. SSL　　B. SET　　C. SHTTP　　D. DES

查看答案

B,C

查看分析

**分析：**本题的前一道是工作原理题，后一道是基础知识题，主要考查了各种安全协议的特点。SSL 是工作在传输层的协议，只要求服务端有数字证书，因此只能够保证服务端不可抵赖。而 SHTTP 是在 HTTP 协议上的扩展，目的是保证商业贸易的传输安全，工作于应用层，但由于 SHTTP 只能够工作于 HTTP 协议层，因此只限于 Web 应用。

而 SET 协议是 Visa 与 MasterCard 共同制定的一套安全又方便的交易模式，最早用于支持各种信用卡的交易，它不仅要求服务端有数字证书，还要求客户端需要数字证书，因此能够保证交易双方都不能够抵赖。

● Kerberos认证过程可以分为三个阶段，在第一阶段中，交互的主体是Kerberos客户端和（39），用户将自己的用户名以（40）的方式发送给（39）。

（39）A．认证服务器　　B．授权服务器　　C．应用服务器　　D．智能卡

（40）A．直接用明文　　B．使用用户的私钥进行加密

C．使用用户的公钥进行加密　　D．用会话密钥加密

查看答案

A, A

查看分析

**分析：**这是一道工作原理题，考查了 Kerberos 认证过程。Kerberos 认证分为三个阶段，分别是 Kerberos 客户端与认证服务器、授权服务器、应用服务器进行交互。在第一个阶段中，用户首先输入自己的用户名，以明文的方式发给认证服务器；然后认证服务器返回一个会话密钥、一个票据，这个会话密钥是一次性的，也可以是从智能卡生成的。

● 在Linux操作系统中，最常用的Web服务器是Apache，关于服务器的监听端口号、运行方式等配置参数位于（41）文件内，如果要配置虚拟主机则应该使用（42）命令。

（41）A. httpd.conf　B. access.conf　C. apache.conf　D. main.conf

（42）A. UseDir　B. DocumentRoot　C. ServerRoot　D. VirtualHost

查看答案

A, D

查看分析

**分析：**这是一道实际应用题，考查的是 Web 服务器 Apache 的配置文件和主要命令。Apache 相关的配置文件包括四个，而监听端口号、运行方式都是与服务器自身相关的配置项，因此是位于主配置文件中，即 httpd.conf。

配置项 UseDir 用于指定个人主页的位置，DocumentRoot 用于指定 Web 页面的目录位置，ServerRoot 用于指定 Apache 服务器的安装目录，VirtualHost 才是用于配置虚拟主机的。

● 当我们要通过FTP传输JPEG文件，那么应该采用__（43）__传输模式；如果要一次性下载多个文件则应该使用__（44）__命令。

（43）A. 文本文件　　B. 二进制　　C. 图形图像　　D. 流

（44）A. download　　B. get　　C. append　　D. mget

查看答案

B, D

查看分析

**分析**：这是一道基础知识题，考查了FTP应用的传输模式与常用命令。FTP传输模式只包括Bin（二进制）和ASCII（文本文件）两种，除了文本文件之外，都应该使用二进制模式传输。显然JPEG文件不是文本文件，因此应该采用二进制传输模式。

FTP命令行客户端常用命令：get—下载文件、mget—一次下载多个文件、!dir—显示当前目录中的文件信息、put—上传文件、mput—一次性上传多个文件、lcd—设置客户端当前目录、bye—退出FTP连接。

● 假设在Linux操作系统中，在/etc/hosts文件中的第一行是“Order hosts,NIS,DNS”，那么最优先使用的地址解析方法是（45），而在Linux中通常使用（46）来架设DNS服务器。

（45） A. 文本文件解析 B. 网络信息服务 C. 域名解析服务 D. 不确定

（46） A. named B. Bind C. NIS D. AD

查看答案

D,B

查看分析

**分析**：这是一道实际应用题，主要考查了Linux下域名解析方面的一些实际知识。在本题的第一个问题中，存在一个有意设置的迷惑点。也许很多人会很直接地选择C，但是题目中是说这行配置文件是写在/etc/hosts中，而非/etc/hosts.conf中，因此并没有起到设置解析顺序的作用，因此显然其结果是“不确定”。

在Linux中，我们通常是使用BIND来架构DNS服务器，其守候进程的名字是named。而NIS是网络信息服务，AD是Windows中的活动目录。

● 在Windows 2000中，内置的Web服务器是（47），其目录安全性配置的默认设置是（48）。

（47）A. Apache　　B. IIS　　C. PWS　　D. FrontPage

（48）A. 匿名访问　　B. 基本验证　　C. 域服务器验证　　D. 集成Windows验证

查看答案

B, A

查看分析

**分析：**这是一道基础知识题，考查的是Windows平台下的Web服务器IIS。在Windows系列操作系统中（包括NT、2000、XP、2003等）都集成了了一个Internet信息服务器—IIS，它能够用来构建Web服务器、FTP服务器、SMTP服务器。IIS可以提供匿名访问（默认使用的模式）、基本验证（使用IIS站点设置的用户名/口令）、Windows域服务器验证（在内部使用）、集成Windows验证（使用IIS所在机器的操作系统用户设置）。也可以对访问者的IP地址和域名进行限制，并能够支持SSL、HTTPS的安全通信。

● 在下列E-Mail服务器软件中，不能够在Linux下使用的是__（49）__传输模式；关于其描述正确的是__（50）__。

（49） A. Sendmail　　B. Postfix　　C. IMail　　D. Qmail

（50） A. 它的功能十分简单，对垃圾邮件的处理没有提供任何措施

B. 它的配置十分复杂，需要通过编辑冗长、费解的配置文件来实现

C. 它提供了邮件过滤规则，并且是 Windows 下的第一个邮件服务器软件

D. 它是在 SNMP 协议的基础上，提供 E-Mail 服务的系统软件

查看答案

C,C

查看分析

**分析**：这是一道基础知识题，主要考查了常见的 E-Mail 服务器软件。在 Linux 和 Unix 环境中，常用的 E-Mail 服务器包括 Sendmail、Postfix 和 Qmail 三种。Sendmail 做为最早的 E-Mail 服务器，拥有着广大的用户群体，许多 Linux 套件也都内建了 Sendmail 软件包。但由于 Sendmail 过于庞大，加上可扩展性和性能上的因素，使得 Postfix 和 Qmail 的用户群体都在日益扩大之中。而 IMail Server 是 Windows 操作系统上的第一个邮件服务器软件，已有 10 余年的历史，现在还内建了防垃圾邮件功能、基于网页的日历功能、邮件规则过滤功能，配置简单、功能强大。由于 IMail 采用的是图形化的操作界面，很少直接修改配置文件。

● 在如图a所示的网络结构中，总共有__（51）__个广播域，__（52）__个冲突域。

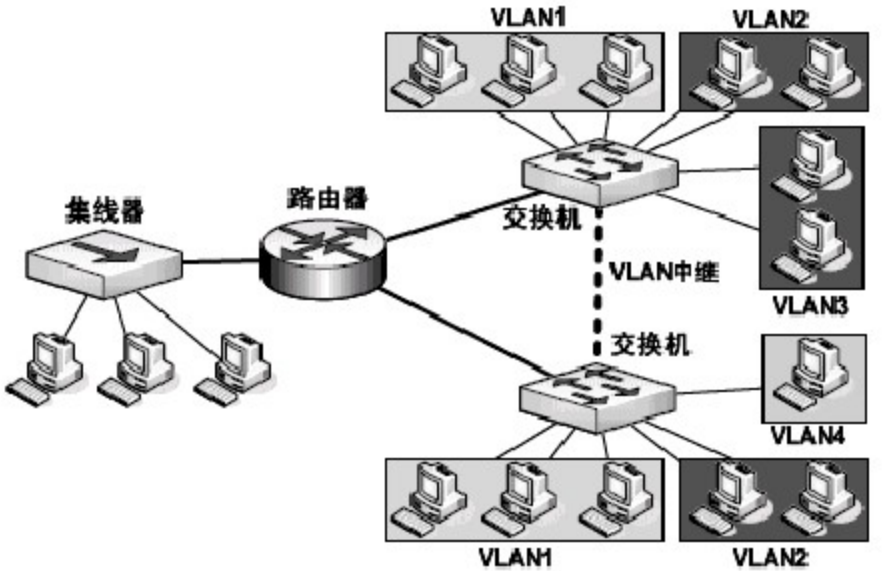



图 a 网络结构示意图

（51） A. 1　　B. 2　　C. 3　　D. 5

（52） A. 5　　B. 14　　C. 16　　D. 20

查看答案

D,B

查看分析

查看答案

D,B

查看分析

**分析**：这是一道原理应用题，主要考查了冲突域与广播域的判断。在本章的例题中已经讲解了这类题的解答方法。在此我们再重申一下概念。

- 冲突域：数据分组产生和发生冲突的这样一个区域被称为冲突域。所有的共享介质环境（用工作在物理层的设备互连）都是冲突域。
- 广播域：能够接收到相同网段中的广播包的区域。所有的用工作在数据链路层的设备互连的非共享介质环境均是属同一广播域。

而从判断的角度来看，交换机就能够分割冲突域，路由器等第三层设备才能够分割广播域，但要注意的是 VLAN 也是可以分割广播域的。

因此，本题中判断广播域个数的过程是：看到路由器，两边肯定处于不同广播域；左边是个集线器，无法分割，只有 1 个；可边是 2 个交换机分隔，但是相互连接的，分成了 4 个 VLAN，因此有 4 个广播域；从而得到总数就是 1+4=5 个。

而判断冲突域个数的过程是：集线器连接的 3 台 PC 是共享介质环境，只有 1 个冲突域；而右边交换机的每个端口都是 1 个冲突域，因此 13 台 PC 就有 13 个冲突域；从而得到总数就是 1+13=14 个。

● 在以下以太网标准中，其网络拓扑结构是总线型的标准是__（53）__，该网络中单根传输介质的最大长度是__（54）__。

（53） A. 10Base2　　B. 10Base-F　　C. 10GBase-CX4　　D. 100Base-T4

（54） A. 100 米　　B. 185 米　　C. 200 米　　D. 500 米

查看答案

A, B

查看分析

**分析：**这是一道基础知识题，考查了以太网标准的拓扑结构和最大段长度。以太网的所有标准中，除了最早的使用同轴电缆的两个使用总线拓扑的标准之外，后面的所有标准（即使用双绞线和光纤）都是星型拓扑。

因此，满足条件的就是 10Base2，而单根传输介质的最大长度就是最大段长度，标准的名称中已经给出了提示，但要记住的是，是 185 而不是 200。

● 在WLAN体系结构中，在MAC子层定义了三种访问控制机制，而点协调功能PCF是建立在__（55）__的基础之上的，而__（55）__则是利用__（56）__来定义的。

（55） A. DCF　　B. PLCP　　C. PMD　　D. PHY

（56） A. RTS/CTS　　B. CSMA/CD　C. PLCP　　D. DCF

查看答案

A, B

查看分析

**分析：**这是一道原理应用题，考查了 WLAN 的体系结构。在 WLAN 体系结构中，由 MAC 子层负责访问控制和分组拆装；它定义了三种访问控制机制：CSMA/CA（载波监听多路访问/冲突避免协议）支持竞争访问，RTS/CTS 和点协调功能支持无竞争访问。利用 CSMA/CA 定义了分布式协调功能 DCF（用于信道的竞争期），并在此基础上又定了的点协调功能 PCF（用于信道的非竞争期），对于时间敏感的帧都应该由点协调功能控制发送。

● FDDI使用的也是一种__（57）__协议，由于FDDI通常应用于城域网，网络段比较长，为了更有效地利用资源，其使用的主要策略是__（58）__。

（57） A. CSMA/CD　　B. 令牌总线　　C. 令牌环　　D. 双总线

（58） A. 改变编码格式　　B. 扩大帧的大小

C. 改为多帧发送　　D. 减小帧的大小

查看答案

C,C

查看分析

**分析：**这是一道原理应用题，主要考查了FDDI的基础知识。FDDI（光纤环网）是一种用于连接不同建筑物和不同场地的多种局域网的城域网协议。它使用光纤作为传输介质，数据速率可达到100Mb/s，环路长度可扩展到200公里，连接的站点数据达到1000个。它与IEEE 802.5类似，也是使用令牌环协议。不过，802.5是单帧发送，环上同时仅有一个帧在流动；而FDDI的环比较长，因此允许将帧附到前面帧的后面进行流动，因此也称为多帧发送。

● 假设有一个采用 CSMA/CD 协议的网络，其电缆长度为 1 公里，不使用重发器，运行速率为 1Gbps，电缆中信号速率是 20 万公里/秒，则最小帧长是（59）。假设该网络的平均帧长是 5000 字节，平均每秒实际传送 20000 个这样的帧，那么该网络的利用率是（60）。

（59） A．1250　　B．2500　　C．1564　　D．1000

（60） A．0.7　　B．0.756　　C．0.8　　D．0.825

查看答案

A, C

查看分析

**分析：**这是一道计算题，考查的是 CSMA/CD 网络中最小帧长和网络利用率的计算方法。CSMA/CD 网络中的最小帧长计算公式是：2×（网络数据速率×最大段长/信号传播速度）。根据题意，网络数据速率是 1Gbps，最大段长是 1 公里，信号传播速率是 20 万公里/秒。代入公式得到：

最小帧长=2×（1Gbps×1/200000）=10000bit=1250 字节

其含义是什么呢？我们首先可以根据信号传播速度来计算 1km 电缆单程传输所需的时间，应为 $1/200000=5*10^{-6}$s，即 5μs，因此来回程传播时间就是 2τ=10μs。而根据 CSMA/CD 的工作原理，最小帧的传输时间不能够小于这个时间，因此将这个时间去乘以网络数据速率 1Gbps，即 $10*10^{-6}\times10^{9}=10000$，这时单位是 bit，再转成字节就是 1250。

而要求网络利用率，根据公式是：吞吐率/网络数据速率。而吞吐率就是单位时间内实际传送的位数。在本题中，可以简单地通过平均帧长乘以每秒帧数来获得，而无需使用复杂的公式："T=帧长/（网络段长/传播速度+帧长/网络数据速率）"。

因此，网络利用率=$5000\times8\times20000/1Gbps=8\times10^{8}/10^{9}=0.8$。

●图a为曼彻斯特编码（表示的数据可能为（61），这种编码适用的网络是（62）。为了在广域网上高速传输数字信号，一般可用的编码方式是（63），其编码效率为（64）。设某编码体制的编码方法为：输入数据、（m=1，2，…），发送时，首先计算 $b_m=(a_m+b_{m-1})$ MOD 2，发送的编码为 $C_m = b_m-b_{m-1}$。收到的编码为Cm，其译码方法可表示为（65）。

图 a 某一曼彻斯特编码

| | | | | |
|---|---|---|---|---|
| （61）A. | 10100 | B. 01110 | C. 10101 | D. 00011 |
| （62）A. | 广域网 | B. 城域网 | C. 局域网 | D. 任意网 |
| （63）A. | NRZ | B. AMI | C. 曼彻斯特 | D. 8B/10B |
| （64）A. | 20% | B. 50% | C. 70% | D. 80% |
| （65）A. | $C+C_{m-1}$ | B. $C_m-C_{m-1}$ | C. $C_m$ MOD 2 | D. $(C_m- C_{m-1})$ MoD 2 |

查看答案

A,C,D,D,C

查看分析

**分析**：这题主要是考查了曼彻斯特码以及其他常见码的适用性、编码效率、译码方法等知识。对于给定曼码的波形图，要求给出对应的二进制的题，在解答之前首先要知识曼码是一种自同步的编码，每一个数字都有一次跳变，这样我们就可以将每个编码用虚线隔开，如图 b 所示：

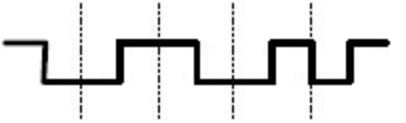


图 b 分解后的曼彻斯特编码

查看答案

A, C, D, D, C

查看分析

**分析**：这题主要是考查了曼彻斯特码以及其他常见码的适用性、编码效率、译码方法等知识。对于给定曼码的波形图，要求给出对应的二进制的题，在解答之前首先要知识曼码是一种自同步的编码，每一个数字都有一次跳变，这样我们就可以将每个编码用虚线隔开，如图 b 所示：

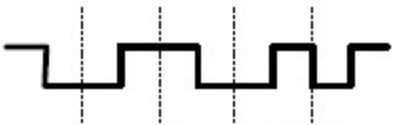


图 b 分解后的曼彻斯特编码

其次，我们需要知识“从高到低”表示 1，“从低到高”表示 0 的曼码规则。因此很容易就可以知道图 b 中编码所对应的数据就应该是 10100。

而对于编码的适用性，应该从以下三个方面来进行记忆：

- 基础编码，不适用于网络：单极性码、极性码、三极性码、不归零码、归零码、双相码。
- 低速局域网：曼彻斯特编码（以太网）、差分曼彻斯特编码（令牌环网），编码效率为 50%。
- 高速局域网、广域网：4B/5B、8B/10B（效率均为 80%）、8B/6T。

而对于本题给出的编码方案，其译码方案可表示为 $C_n$ MOD 2。因为根据编码方案，如果没有出错，接收到的编码与发送的编码相同，即我们需要证明 $C_n$ MOD 2=$a_n$。而整个推导过程为：

$C_n \bmod 2 = (b_n - b_{n-1}) \bmod 2$

$= (((a_n + b_{n-1}) \bmod 2) - b_{n-1}) \bmod 2$

$= ((a_n + b_{n-1}) \bmod 2) - (b_{n-1} \bmod 2)$

$= (a_n + b_{n-1} - b_n) \bmod 2 = a_n \bmod 2 = a_n$

●双极性AMI编码通过一个噪声信道，接收的波形如图a所示，那么出错的是第（66）位。

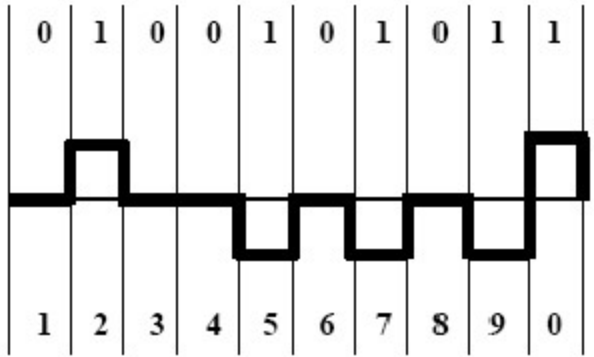



图 a 接收波形示意图

（66）A.3　　B.5　　C.7　　D.9

查看答案

C

查看分析

**分析：**这题考查的就是双极性 AMI 编码的编码规则。首先从双极性，就可以得知它使用了正负两极以及零电平。而 AMI 则是一种典型的双极性码，它是指“信号交替反转”，即零电平表示 0，而 1 则使电平在正、负极间交替翻转。

了解了这样的规则后，我们就可以对图 a 所示的波形进行验证。首先看 0，可以发现所有的“0”对应的对是 0 电平（在中间的线上）。然后我们再看 1，它的序列是“正极（第 2 位）、负极（第 5 位）、负极（第 7 位）、负极（第 9 位）、正极（第 10 位）”。显然第 7 位，是不符合 AMI 的规则的，因此说明其是受噪声影响的。

● 网格计算系统一般由网格硬件、网格操作系统、__（67）__、网格应用4层基本结构构成。网格系统可以分为资源层、__（68）__和应用层三个基本层次。

（67）A. 网格软件　　B. 网格中间件　　C. 网格界面　　D. 网格管理

（68）A. 界面层　　B. 中间件层　　C. 管理层　　D. 硬件层

查看答案

C, B

查看分析

**分析：**这是一道基本概念题，考查的是网格的基本概念。网格计算系统一般由网格硬件、网格操作系统、网格界面、网格应用4层基本结构构成。网格系统可以分为资源层、中间件层和应用层三个基本层次。

● 在图（a）所示的系统中，R1、R2、R3 为 3 个加工部件，其可靠度分别为 0.93、0.95、0.98，则系统的可靠性约为__（69）__，而这时如图（b）所示添加一个R3，则与图（a）相比其可靠性__（70）__。

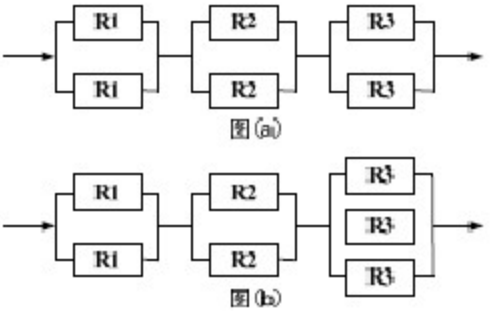



图 3-12 可靠性模型

（69）A. 0.7497　　B. 0.8658　　C. 0.9533　　D. 0.9922

（70）A. 有所降低　　B. 所有提高　　C. 没有变化　　D. 有变化，但无规律

查看答案

D,B

查看分析

**分析**：这是一道计算题，考查的是串—并联系统的可靠性计算。对于图（a）而言，就是三个“并联组”串联起来的系统，因此我们应分别计算各个并联组的可靠性：

- R1 并联组的可靠性=1-（1-0.93）×（1-0.93）=0.9951
- R2 并联组的可靠性=1-（1-0.95）×（1-0.95）=0.9975
- R3 并联组的可靠性=1-（1-0.98）×（1-0.98）=0.9996

而整个系统是这三个并联组串联而成的，因此只需要将这三个并联组的可靠性相乘就可以得到整个系统的可靠性：0.9951×0.9975×0.9996=0.9922。

而对于图（b）而言，和图 3-10（a）相比，在 R3 并联组处多了一个并联元件，因此该并联组的可靠性就应该是 1-（1-0.98）×（1-0.98）×（1-0.98）=0.999992，显然更加可靠，整个系统的可靠性就应该是：0.9951×0.9975×0.999992≈0.9926，显然可靠性是提高了。

●Personal firewall is a technology that helps（71）intruders from accessing data on your PC via the Internet or another network, by keeping（72）data from entering or exiting your system.

Hackers do not just target national security organizations for（73）: They want your tax returns, network passwords, or bank account numbers. And you do not want the FBI kicking in your door because someone hijacked your PC to（74）in the latest denial-of-service attack on the Internet. Now that "always-on" broadband connections such as cable modems and digital subscriber line are becoming more popular, home users are at risk. Fortunately, you can protect your data. Firewalls can block（75）attacks and protect your PC from outside threats.

| | | | | |
|---|---|---|---|---|
| （71）A. allow | B. prevent | C. invite | D. get |
| （72）A. authorized | B. refused | C. denied | D. unauthorized |
| （73）A. attacks | B. aggression | C. help | D. repair |
| （74）A. enlist | B. go to | C. participate | D. attach |
| （75）A. malicious | B. friendly | C. neighborly | D. goodwill |

查看答案

B, D, A, C, A

查看分析

**分析：**个人防火墙技术通过限制**未经验证（unauthorized）**的数据进出你的系统，以**防止（prevent）**入侵者通过因特网或另一网络访问你 PC 机上的数据。

黑客们网络**攻击（attacks）**的目标不只是对准国家的安全机构。他们要你的纳税申报单、网络口令、或者银行账号。你也不想要联邦调查局来踢你的家门，因为有人盗用了你的 PC 机**参与（participate）**最新的一次因特网拒绝服务攻击。由于诸如电缆调制解调器和（电话）数字用户线实现的"始终在线"连接越来越流行，家庭用户也有风险。幸运的是你也能保护自己的数据。防火墙能阻断**恶意（malicious）**攻击，以保护你的 PC 机免受外部威胁。