●在安装Linux操作系统的机器中，若需要添加一条默认路由，网关地址为 192.168.1.1，那么正确的命令是（1）

（1）A. route 0.0.0.0 gw 192.168.1.1

B. route 255.255.255.255 gw 192.168.1.1

C. route add 0.0.0.0 gw 192.168.1.1

D. route add 255.255.255.255 192.168.1.1

查看答案

C

查看分析

分析：在 Linux 中，我们可以使用 route 命令来查看和设置 Linux 系统的路由信息，以实现与其他网络的通讯。而以下就是几个 route 的常用命令：

- 增加一个默认路由：route add 0.0.0.0 gw 网关地址
- 删除一个默认路由：route del 0.0.0.0 gw 网关地址
- 指定一个路由：route add 目标网络 gw 网关地址

●对于一个只有3个人的小公司，其Windows网络的组网形式应该选择(2)，在Windows中文件与打印共享功能是基于(3)协议实现的。

(2) A. 工作组　　B. 域　　C. 活动目录　　D. 均不合适

(3) A. TCP　　B. UDP　　C. IPX　　D. NetBIOS

查看答案

A, D

查看分析

分析：这是一道基础知识题，主要考查。在Windows中，可将基于不同平台客户机和服务器松散地组成工作组，也可组成为一个可管理的域。

●如果我们需要在路由表中设置一条默认路由，那么目标地址应为（4），子网掩码应为（5）。

（4）A．127.0.0.0　B．127.0.0.1　C．1.0.0.0　D．0.0.0.0

（5）A．0.0.0.0　B．255.0.0.0

C．0.0.0.255　D．255.255.255.255

查看答案

D,A

查看分析

分析：略

●新购买的交换机进行第一次配置时，我们应该（6）；当使用超级终端连接交换机时，COM口的“端口速率、数据位、停止位、流控”的正确配置是（7）。

（6）A．通过 Console 口连接　　B．通过 AUX 口连接
　　C．通过 Telnet 连接　　D．通过浏览器访问

（7）A．2400bps,8,1，无　　B．9600bps,7,1,Xon/Xoff
　　C．9600bps,8,1,无　　D．2400bps,8,1,Xon/Xoff

查看答案

A, C

查看分析

分析：连接交换机的方法有五种：通过 Console 口连接终端、通过 AUX 口连接 Modem、通过 Telnet、通过浏览器（只是部分）、通过专用的网管协议，但首次使用时只能使用第一种，即通过 Console 口连接。一般而言，交换机自带有 Console 连接线，一端是连接在交换机的 Console 口；而另一端则是连接在 PC 的 COM 口上。在连接时，需将端口属性的配置设置为以下参数：端口速率为 9600b/s、数据位为 8、无奇偶校验、停止位为 1、无流控。

●小李在另一个在线商城购买了一台MP3，结果汇出钱后，商场却否认该物品是其销售的物品，而且其转账的账号也不是他们的，我们通常将其归为（8）问题。

（8）A．有效性　　B．数据完整性　C．不可抵赖性　　D．不可审查性

查看答案

C

查看分析

分析：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。有效性是指要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、地点是有效的。而不可抵赖性则是防止交易的某方否认曾经发生的交易行为。

●在以下事件中，会触发Trap报文的是（9），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（10）。

（9）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

（10）A．从代理回应的 Get-Response 报文中获得

B．从代理主动发出的 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：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。

●以下路由选择协议中，属于在两个自治系统之间使用的路由选择协议是（11），其主要的功能是（12）。

（11）A．BGP　　B．IGRP　　C．EIGRP　　D．OSPF

（12）A．完成自治系统管理　　B．生成跨自治系统的路由包

C．控制路由策略　　D．维护路由数据库

查看答案

A, C

查看分析

分析：本题的前一道是概念比较题，后一道是工作原理题。IGRP、EIGRP、OSPF 都是内部网关协议，只有 BGP 是外部网关协议，是两个自治系统间使用的路由选择协议。

BGP 是“边界网关协议”的缩写，处理各 ISP 之间的路由传递。其特点是有丰富的路由策略，这是 RIP、OSPF 等协议无法做到的，因为它们需要全局的信息计算路由表。BGP 通过 ISP 边界的路由器加上一定的策略，选择过滤路由，把 RIP、OSPF、BGP 等的路由发送到对方。全局范围的、广泛的 Internet 是 BGP 处理多个 ISP 间的路由的实例。BGP 的出现，引起了 Internet 的重大变革，它把多个 ISP 有机的连接起来，真正成为全球范围内的网络。带来的副作用是 Internet 的路由爆炸，现在 Internet 网的路由大概是 60000 条，这还是经过“聚合”后的数字。

●在下述路由选择协议中，能够实现自动路由汇总（汇聚）功能的是（13），它属于一种（14）协议。

（13）A．RIP　　B．IGRP　　C．OSPF　　D．EIGRP

（14）A．距离向量　B．链路状态　　C．平衡型　　D．外部网关

查看答案

D,B

查看分析

分析：EIGRP 协议是一种链路状态协议，使用一种散射更新算法，实现很高的路由性能。支持 VLSM、不连续子网，支持自动路由汇总功能，支持多种网络层协议。

●假设在如图a所示的透明网桥中，它在X端口收到一个数据包，该数据包的源地址是“00-0D-56-E1-40-35”，目的地址是“00-0F-73-E1-2F-35”，则（15）；如果源地址是“00-0E-23-D5-40-35”，目标地址是“00-0D-56-E1-40-37” 则（16）。

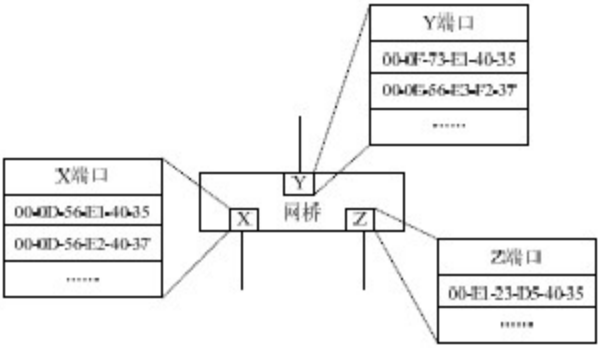

图 a

（15） A．丢弃该帧　　B．从 Y 端口转发
C．向 Y 和 Z 两个端口转发　　D．向所有端口转发

（16） A．丢弃该帧　　B．从 Y 端口转发
C．向 Z 两个端口转发　　D．向 Y 和 Z 两个端口转发

查看答案

C, A

查看分析

分析：本题最主要容易迷惑的地方是题目中同时给出了源 MAC 地址和目标 MAC 地址，而转发机制只需要根据目标 MAC 地址就可以进行判断了，但容易混淆。其实要记住这个区别并不难，由于网桥是分隔网络的广播包的，主要是减少不必要的广播，因此显然是根据目标地址判断的。

透明网桥的帧转发规则如图 b 所示：

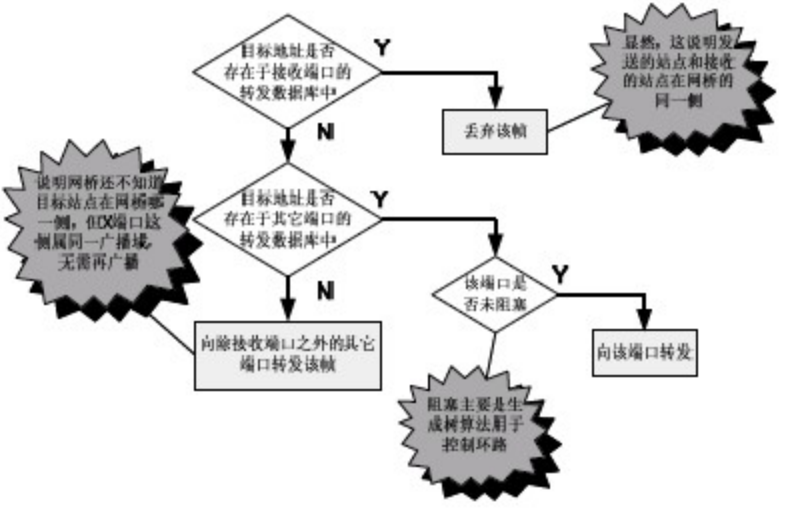

图 b　透明网桥帧转发规则

在前一个问题中，由于网桥三个端口的转发数据库中都不包括“00-0F-73-E1-2F-35”（目地地址），因此根据图 D-3 的规则显然应该是“向除接收端口之外的其他端口转发该帧”，即应“向 Y 和 Z 两个端口转发”。

而后一个问题中，由于目标地址“00-0D-56-E1-40-37” 就处于 X 端口的转发数据库中，因此当然应该“丢弃该帧”。

●在Linux中，如果要将某一个文件改名，那么可以使用（17）命令，如果要修改Apache的配置文件，则可以使用（18）命令。

（17）A．rm　　B．cp　　C．mv　　D．rename

（18）A．more　　B．tail　　C．cat　　D．vi

查看答案

D,D

查看分析

分析：在 Linux 中没有提供直接的文件改名命令，rename 并不存在。而 rm 是删除目录，cp 是复制文件或目录，mv 是移动文件或目录，因此我们如果需要对文件进行改名，那么实际上可以通过 mv 命令来实现。

要修改配置文件，必须采用可以编辑的工具：more 命令只是分页显示，cat 类似于 type 命令，tail 则适合于日志文件的查看（只显示文件尾的一部分）。而 vi 则类似于 Windows 下的 notepad，虽然不是可视化的字处理软件，但也是一个功能强大、应用广泛的最简单的文本编辑工具。

●某公司的网络结构图如a所示，假设文件服务器为员工日常备份数据之用，无需外部使用，程序测试服务器主要是用于内部的软件开发测试时使用，而Web服务器承载的是企业外部网站、E-Mail服务器公司的邮件服务器，OA服务器暂不提供外网访问接口，那么在这个结构中，服务器位置放置不恰当的有（19），WEB服务器的位置（20）。

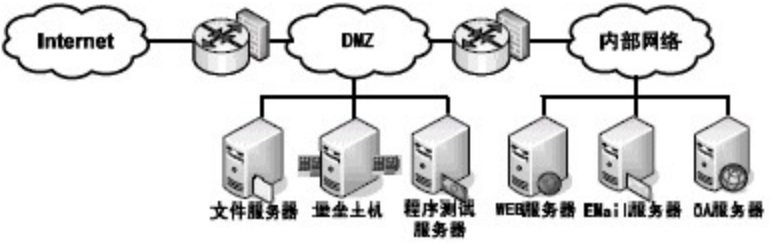

图 a

（19）A. 1 台　　B. 2 台　　C. 3 台　　D. 4 台

（20）A. 正确，无需调整位置　　B. 有问题，应该放置在 DMZ 子网

C. 有问题，应该放置在 Internet 上　　D. 可不变，也可以放置到 DMZ 子网中

查看答案

D,B

查看分析

分析：在图 a 所示的网络结构中，显然采用的是单 DMZ 防火墙结构（也称为屏蔽子网结构）。在这种结构中，DMZ 通常比较小，处于 Internet 和内部网络之间，一般情况下，配置成使用 Internet 和内部网络系统对其访问会受限制的系统，例如：堡垒主机、信息服务器、Modem 组以及其他公用服务器。

因此，我们可以发现“文件服务器”、“程序测试服务器”、“OA 服务器”根据题目的描述，是不属于公用服务器的，仅限于内部网络访问，因此应该连接在“内部网络”上。而“Web 服务器”、“E-Mail 服务器”都应该是公用服务器，因此应该连接在“DMZ 网络”上。即共有 4 台服务器的位置不恰当。另外，Web 服务器虽然可以放在 Internet 上（即托管出去），那就离开了本网络中防墙的保护范围，因此也是不合适的。

●在如图a所示的网络中使用的路由选择协议是RIP，在路由器R5 连接到网络之前，路由器R1 的路由表中，到网络 10.4.0.0 的跳数是（21），而连接之后跳数则变成了（22）。下面关于RIP路由选择的描述不正确的是（23）。

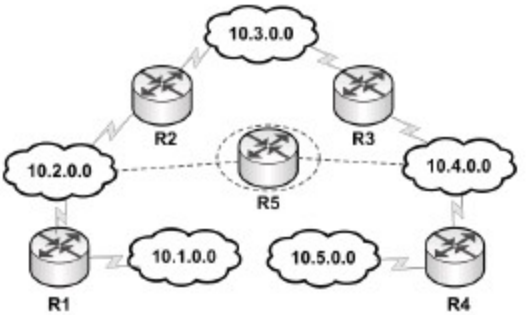

图 a

（21），（22）A．1 跳　　B．2 跳　　C．3 跳　　D．4 跳

（23）A．RIP 使用广泛、配置简单，支持 CIDR，VLSM 及连续子网

B．RIP 最大跳数是 15 跳，也就是在一条链路上不能超过 15 个路由器

C．RIP 能够支持对链路速度的度量，并根据速度的不同来优化路由

D．RIP 的路由更新时间是 30 秒，收敛慢，网络规模加大后性能表示不佳

查看答案

B, A, C

查看分析

分析：RIP 是一个距离矢量路由选择协议，它的度量单位是“跳”，每经过一个路由器，就将跳数加 1。因此，在路由器 R5 连接到网络之前，R1 到网络 10.4.0.0 需要经过路由器 R2，R3，因此跳数为 2；而当路由器 R5 连接到网络之后，R1 到网络 10.4.0.0 则只需要经过路由器 R5 一个，因此跳数变成了 1。

RIP 路由选择协议具有以下特点：使用广泛，简单、可靠，支持 CIDR、VLSM 及连续子网，最大跳数是 15（隔一个路由器为一跳），每隔 30 秒广播一次路由信息。但其收敛慢，网络规模受限。它并不能够根据链路的速度进行度量（IGRP 可以），因此不正确的描述是 C。

● 在Windows操作系统中，用来配置IP地址的命令是（24），而（25）可以打印出本机的路由表。

（24）A. ipconfig　　B. netstat　　C. winipcfg　　D. ping

（25）A. netstat -r　　B. netstat -a　　C. ipconfig　　D. netstat -s

查看答案

C, A

查看分析

分析：这是一道实际应用题，主要考查了 Windows 下常见的网络配置命令。在 Windows 操作系统中，ipconfig 是用来显示 TCP/IP 配置的，ping 是用来验证远程主机的可达性的，netstat 则是一个强大的网络状态查看命令，只有 winipcfg 是用来对 IP 地址进行配置的。不过要注意的是，winipcfg 在 Windows XP 中已经取消了。

要列出本机的路由表，大家可能会想到 route print，但是在供选择的答案中并没有这个选项，而 ipconfig 只是列出 TCP/IP 的配置，我们只能通过 netstat 命令。-a 是指显示所有连接和监听端口，-s 是显示每个协议的统计，-r 则是指 route，即列出所有的路由表。

● NetBIOS协议为了实现在整个网络上进行传输，必须借助其它的相关协议，这些协议中，__（26）__是采用了桥接机制，__（27）__是采用TCP/IP作为传输层和网络层。

（26）A. NetBEUI　　B. NWLINK　　C. NBT　　D. IPX

（27）A. NetBEUI　　B. NWLINK　　C. NBT　　D. IPX

查看答案

A, C

查看分析

分析：这是一道工作原理题，主要考查了 NetBIOS 的相关知识。NetBIOS 必须实现在整个网络上的传输，通常可以通过“桥接和路由”两种方式实现，支持桥接的是 NetBEUI，而支持路由的是 IPX 和 IP。如果使用是的纯 IPX 网络，则应该使用 NWLINK 在 IPX 中封装 NetBIOS，而在基于 IP 的大型网络，则应在 NBT 上安装 NetBIOS。

- NetBEUI：它是传输层和网络层协议，但不包含逻辑寻址方案，直接使用 MAC 地址访问数据链路层，并对数据链层广播依赖。因此应用该协议的网络扩展性差，仅适于小型 LAN。
- NWLINK：即 IPX 上的 NetBIOS，适合于与 Novell 网络互联。

NBT：它是使用 TCP/IP 作为传输层和网络层。

● 假设在某Linux机器上，/etc/hosts.conf的内容是“order hosts,dns”，而/etc/hosts文件中有一行“www.abc.com 212.101.101.102”，而在nslookup命令中，输入www.abc.com时回应值为202.101.101.103。那么当执行ping www.abc.com命令时，它连接的是__（28）__；而域名服务器的IP地址应该存放在__（29）__。

（28）A．212.101.101.102　　B．202.101.101.103
　　C．不一定，将轮流使用这两个解析　　D．将因为找不到IP地址而报错

（29）A．named.conf　　B．hosts.conf　　C．resolv.conf　　D．bind.conf

查看答案

A, C

查看分析

分析：这是一道实际应用题，主要考查了Linux下域名解析的相关设置。在Linux中可以采用hosts文件、DNS、NIS三种域名解析方法，当同时使用时，就会根据/etc/hosts.conf中的配置来决定其顺序。在本题中，其顺序是hosts,dns，也就是先使用/etc/hosts文件中的配置，因此当使用ping命令时，连接的就是这个文件中指定的IP地址，即212.101.101.102。

在Linux中named.conf是DNS服务器Bind的主配置文件，host.conf是用来配置域名解析方法的优先顺序的，并不存在bind.conf这个配置文件。而用来存储域名服务器的IP地址的文件就是/etc/resolv.conf。

● 根据攻击手段不同，可以将网络安全攻击分为多种不同的类别。小张在其免费提供下载的软件中嵌入会盗取用户电脑敏感信息的程序，这种行为通常称为__（30）__，拒绝服务攻击则属于__（31）__。

（30） A．被动攻击　　B．主动攻击　　C．分发攻击　　D．内部人员攻击

（31） A．主动攻击　　B．分发攻击　　C．内部人员攻击　　D．物理临近攻击

查看答案

C,A

查看分析

分析：这是一道基础知识题，主要考查了常见的网络安全威胁的知识。对于网络安全而言，大都是针对网络安全漏洞，进行网络攻击。其中安全漏洞包括物理安全隐患、软件安全漏洞、搭配的安全漏洞；网络攻击可分为被动攻击、主动攻击、物理临近攻击、内部人员攻击、分发攻击等，如表 a 所示。

表 a 主要的网络攻击类型

攻击类型	说明
被动攻击	包括分析通信流，监视未被保护的通信，解密弱加密通信，获取鉴别信息。被动攻击可能造成在没有得到用户同意的情况下，将信息或文件泄露给攻击者，如泄露个人的信用卡号码和医疗档案等。
主动攻击	包括试图阻断或攻破保护机制、引入恶意代码、偷窃或篡改信息。主动进攻可能造成数据资料的泄露和散播，或导致拒绝服务以及数据的篡改。
物理临近攻击	是指未被授权的个人，在物理意义上接近网络、系统或设备，试图改变，收集信息或拒绝他人对信息的访问。
内部人员攻击	可以分为恶意或无恶意攻击。前者指内部人员对信息的恶意破坏或不当使用，或使他人的访问遭到拒绝；后者指由于粗心、无知以及其他非恶意的原因而造成的破坏。
分发攻击	指在工厂生产或分销过程中对硬件和软件进行的恶意修改，这种攻击可能是在产品里引入恶意代码，比如后门。

从表 a 不难看出，“在免费提供下载的软件中嵌入会盗取用户电脑敏感信息的程序”应属分发攻击，拒绝服务攻击则属于主动攻击。

● 当（34）时，并不需要吊销数字证书。而大家可以通过CA中心维护的（35）来查询这些已吊销的数字证书。

（34）A．数字证书到了有效期　　B．用户私钥已泄露
　　C．用户公钥已泄露　　D．用户放弃使用

（35）A．CRL 列表　　B．中心网站　　C．专用程序　　D．证书通告

查看答案

C, A

查看分析

分析：这是一道工作原理题，主要考查了不同数字证书的吊销管理。通常，只有当数字证书到了有效期，或者在此期间出现用户私钥已泄露、用户放弃使用原 CA 中心的服务、CA 中心私钥泄露等情况，才需吊销证书。这时 CA 中心会维护一个证书吊销列表 CRL，供大家查询。而在本题中，故意将“用户公钥已泄露”作为一个陷阱，实际上用户公钥是公开的，本来就不存在什么泄露问题。

● IPSec包括了安全协议、__（36）__、安全关联、认证和加密算法四个部分组成。其中在IPSec中定义了通信实体间身份认证、创建安全关联、协商加密算法、共享会话密钥方法的__（36）__是__（37）__。

（36）A. 密钥管理协议　B. 交互协议　C. 隧道协议　D. 会话协议

（37）A. AH　B. ESP　C. IKE　D. DES

查看答案

A, C

查看分析

分析：这是一道工作原理题，主要考查了 IPSec 的协议组成。IPSec 是包括安全协议、密钥管理协议、安全关联、认证和加密算法四部分构成的安全结构。

■ 安全协议在 IP 协议中增加两个基于密码的安全机制—认证头（AH）和封装安全载荷（ESP），前者支持了 IP 数据项的可认证性和完整性，后者实现了通信的机密性。

密钥管理协议（密钥交换手工和自动 IKE）定义了通信实体间身份认证、创建安全关联、协商加密算法、共享会话密钥的方法。

● 堡垒主机是指（38），如果一个网络中仅采用了一台堡垒主机作为防火墙，那么这种防火墙结构称为（39）。

（38）A. 安装了两张网卡，分别连接外网和内网，并运行代理服务器的主机

B. 安装了最高安全等级操作系统的主机，黑客难以攻破

C. 实际上就是一个带包过滤功能的路由器

D. 用于监控网络内容，及时发现入侵的主机

（39）A. 双宿网关防火墙　　B. 包过滤型防火墙

C. 屏蔽主机防火墙　　D. 屏蔽子网防火墙

查看答案

A, A

查看分析

分析：这是一道基础知识题，考查了堡垒主机和双穴主机防火墙结构的基本概念。堡垒主机，又称为双穴主机，它是由一台至少装有两块网卡的堡垒主机作防火墙，位于内外网络之间，分别与内外网络相离，实现物理上的隔开。它有两种服务方式：一是用户直接登录到双宿主机上；二是在双宿主机上运行代理服务器。

而在前面我们已经说过，在内部网络和外网间放置一个双穴主机，运行代理协议的防火墙结构称为双宿网关防火墙。

● 历史悠久的Sendmail服务器的主配置文件是__（40）__，其配置功能十分强大，但也十分复杂，包括许多不同的小节，其中“定义在发送邮件时可忽略发送者地址的用户”的小节是__（41）__。

（40） A. sendmail.conf B. sendmail.cf C. mail.conf D. mail.cf

（41） A. Trusted Users B. User List C. Rewriting Rules D. Option

查看答案

B, A

查看分析

分析：这是一道实际应用题，考查了 Sendmail 的配置文件相关知识。Sendmail 的主配置文件是/etc/sendmail.cf，其中基本包含了 Sendmail 的全部配置信息，该文件的内容非常复杂。其中一些相对较重要的小节包括：

- Local Information：定义有关个人主机的信息
- General Macros：定义有关本地网络的宏
- Option：定义 Sendmail 选项
- Message Precedence：定义 Sendmail 所用的各种消息的优先级值
- Trusted Users：定义在发送邮件时可忽略发送者地址的用户
- Format of Headers：定义 Sendmail 插入的邮件首部格式

Rewriting Rules：定义用于重写邮件地址的规则

● 在Linux操作系统中，Apache服务器的守候进程是__（42）__，如果需要使该进程在系统启动时，自动启动则应该使用__（43）__命令。

（42）A. named　　B. apached　　C. inetd　　D. httpd

（43）A. autorun　　B. services　　C. chkconfig　　D. startmode

查看答案

D,C

查看分析

分析：这是一道实际应用题，考查了 Web 服务器 Apache 的守候进程名称。在 Linux 系统中，Apache 服务器是由一个名为 httpd 的守候进程来提供服务的。如果需要让这个守候进程在系统启动时自动启动，那么最简单的方法就是使用 chkconfig 命令。Chkconfig 命令是用来设置是否在系统启动时自动启动相应服务的命令，其命令格式为“chkconfig 服务名 on/off”，因此要使其自启动，只需执行 chkconfig httpd on 命令。

● 在Linux系统中，通常使用Wu-ftpd来架设FTP服务器。对于这种服务器而言，如果想停止FTP服务，那么可以使用__（44）__命令；在以下关于配置文件/etc/ftpusers的描述中，正确的是__（45）__。

（44） A. ftpd stop　　B. ftpstop　　C. ftpclose　　D. ftpshut

（45） A. 设定系统中哪些用户允许使用 FTP 传送文件

B. 设定系统中哪些用户不允许使用 FTP 传送文件

C. 设定 FTP 用户的权限与可使用的最大容量

D. 设定 FTP 用户的可登录时间、次数

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 Wu-ftpd 的基本命令与配置文件。Wu-ftpd 的常有的配置文件有 4 个，如表 a 所示：

表 a Wu-ftpd 的配置文件

配置文件	作用
/etc/ftpaccess	最重要的配置，决定 FTP 是否正常工作和权限访问
/etc/ftpusers	设定系统中哪些用户不允许使用 FTP 传送文件
/etc/ftphosts	设定哪些主机不允许连接本 FTP 服务器
/etc/ftpconversions	设定当用户下载文件时应该作哪些操作（如压缩、解压）

另外，它还提供了几个很方便的命令：用来关闭 FTP 守候程序的 ftpshut，用来统计当前登录 FTP 的人数的 ftpcount，用来查看当前 ftp 服务器连线用户的 ftpwho。

● 当DHCP客户机首次启动时，将向DHCP服务器发送一个服务请求包；当DHCP服务器收到后，将通过（46）报文返回一个未分配的IP地址。当客户机获得了IP地址后，会在租约时间过了（47）时开始更新租约。

（46） A. Dhcpoffer　　B. Dhcpack　　C. Dhcpdiscover　　D. Dhcpquest

（47） A. 50%　　B. 75%　　C. 87.5%　　D. 95%

查看答案

A, A

查看分析

分析：这是一道工作原理题，主要考查了 DHCP 的工作流程。DHCP 的整个工作流程如图 a 所示，通过该图就不难得出答案了：

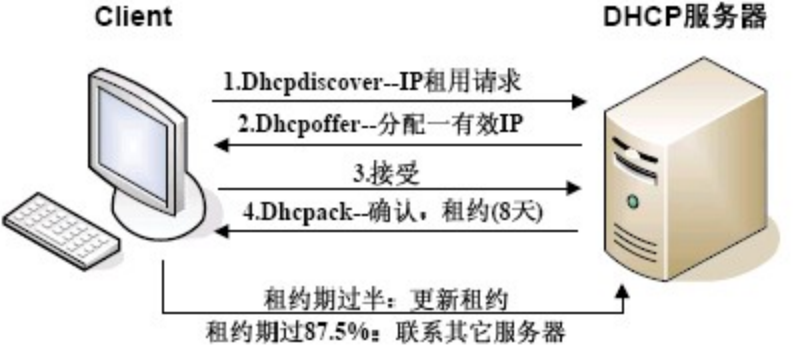

图 a DHCP 工作流程示意图

● 在DNS中，正向解析是指（48），记录类别（49）不是用于正向解析的，而是用于反向解析的。

（48） A. 根据 IP 地址解析域名　　B. 根据域名来解析 IP 地址
　　C. 服务端响应客户端的请求　　D. 客户端响应服务端的请求

（49） A. MX　　B. PTR　　C. SRV　　D. NS

查看答案

B, B

查看分析

分析：这是一道工作原理题，主要考查了 DNS 中正向解析的概念以及常用的指针。DNS 正向解析是指域名→IP 地址的解析工作，反向解析则是指 IP 地址→域名的解析工作。DNS 记录的类别如表 a 所示：

表 a　DNS 记录类别

类别名称	说明
A	主机记录，普通主机
MX	邮件服务器记录
NS	域名服务器记录
PTR	指针记录，用于反向域名解析
SRV	用于活动目录，仅限于 Windows 操作系统

●透明网桥的基本功能有学习、帧过滤和帧转发及生成树算法等功能，因此它可以决定网络中的路由，而网络中的各个站点均不负责路由选择。网桥从其某一端口收到正确的数据帧后，在其地址转发表中查找该帧要到达的目的站，若查找不到，则会__（50）__；若要到达的目的站仍然在该端口上，则会__（51）__。

图a为两个局域网 LAN1 和 LAN2 通过网桥 1 和网桥 2 互连后形成的网络结构。设站 A 发送一个帧，但其目的地址均不在这两个网桥的地址转发表中，这样结果会是该帧__（52）__。为了有效地解决该类问题，可以在每个网桥中引入生成树算法，这样一来__（53）__。

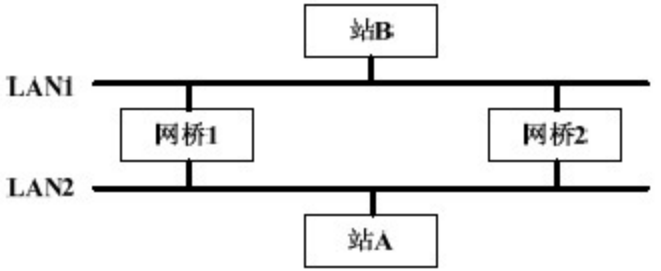

图 a 拓扑图 1

图b为一 10Mbps 数据传输率下的以太网，其上连接有 10 个站，在理想状态下每个站的平均数据传输率为 1Mbps。若通过网桥连接后成为图b所示的结构时，每个站的实际有效数据传输率为__（54）__Mbps。

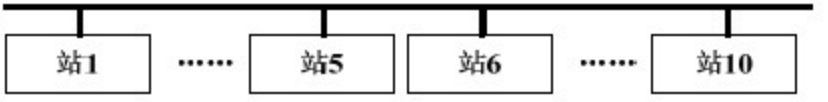

图 b 拓扑图 2

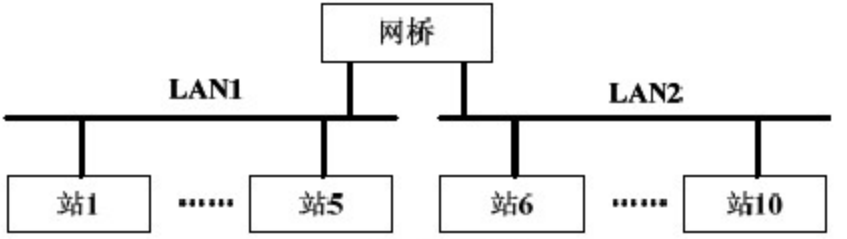

图 c 拓扑图 3

（50）A. 向除该端口以外的桥的所有端口转发此帧

B. 向桥的所有端口转发此帧

C. 仅向该端口转发此帧

D. 不转发此帧，而由桥保存起来

（51）A. 向该端口转发此帧　　B. 丢弃此帧

C. 将此帧作为地址探测帧　　D. 利用此帧建立该端口的地址转换表

（52）A. 经桥 1（或桥 2）后被站 B 接收　　B. 被桥 1（或桥 2）丢弃

C. 在整个网络中无限次地循环下去

D. 经桥 1（或桥 2）到达 LAN2，再经桥 2（或桥 1）返回 LAN1 后被站 A 吸收

（53）A. 网络资源也会得到充分利用　　B. 网络的最佳路由也会得到确定

C. 也限制了网络规模　　D. 也增加了网络延时

（54）A. 1 至 2　　B. 1　　C. 2　　D. 0 至 1

查看答案

A, B, C, D, A

查看分析

分析：网桥是用来在数据链路层上将两个网段隔开，最基本的网桥是两个端口，一个端口接在一个网段。因此，网桥就要根据端口来判断转发策略。显然，当收到一个包，其目的地址还不在数据库中，那么说明网桥不知道它在哪个网段，因此显然应该“向除该端口以外的桥的所有端口转发此帧”；而如果该地址就是接收端口的地址表中，那么显然说明发送者和接收者是同一个网段上，当然要“丢弃此帧”。

如果理解这一机制，就不难进行分析与推导。由于目的地址在两个网桥中均没有记录，那么当帧转到网桥时，它会同时向 LAN1 和 LAN2 转发，因此如果没有重建端口地址表，结果必须会造成其在网络无限循环下去。通过生成树算法，就能够动态地建立和周期性更新，避免死循环问题，但它显然会“增加网络延时”。

在图 c 中，共有 10 个站，它们是总线串联起来的，因此是分享带宽的，因此理想状态就是 10/10=1Mbps。而网桥则将网络分成两个网段，因此理想状态下的速率就是 10/5=2Mbps，但题目问的是有效数据传输率，因此往往是达不到这个理想速率，因此应该是 1-2Mbps。

●IPv6 使用了更大的地址空间，每个地址占有 128 比特，为方便网络管理人员阅读和管理，采用（55）进制加冒号的表示方法。（56）是IPv6 的测试床，实际上是一个基于IPv4 的虚拟网络，用于研究和测试IPv6 的标准、实现以及IPv4 向IPv6 的转变过程。

（55）A. 16　　B. 10　　C. 8　　D. 2

（56）A. 6bone　　B. 6bed　　C. 6backbone　　D. 6plane

查看答案

A, A

查看分析

分析：IPv6 已经广泛受到重视，近年来也不断有相关的产品与应用出现，因此这方面的基础知识是需要去了解的。

●通过代理服务器使内部局域网中的客户机访问Internet时，（57）不属于代理服务器的功能。

（57）A. 共享 IP 地址　　B. 信息缓存　　C. 信息转发　　D. 信息加密

查看答案

D

查看分析

分析：这是一道关于代理服务器的题目，虽然大家平时也经常使用，但这类题目在解答时还是需要注意分析的。要实现代理，显然需要共享 IP 地址，实现信息转发；为了提高访问速度，通常还应该进行信息的缓存；但是代理服务器只是负责实现网络连接，本质上是不参与应用的，因此显然不会去承担“信息加密”的功能。

● 交换以太网与共享以太网比较，硬件变化的核心就是__（58）__，它有效地解决了网络负载带来的负载问题，办法的核心是__（59）__。

（58） A．用交换式网卡替换共享式网卡　　B．用光纤替换非屏蔽双绞线
C．用双网卡替换单网卡　　D．用交换机 替换 集线器

（59） A．使每个端口都处于一个独立的广播域中
B．使每个端口都处于一个独立的冲突域中
C．实现了智能信道仲裁，从而降低了冲突的机率
D．通过频分复用，扩大了可用通道，降低了冲突

查看答案

D,B

查看分析

分析：这是一道基础知识题，主要考查了交换式以太网的基础知识。以太网使用的CSMA/CD 是一种竞争式的介质访问控制协议，因此从本质上说它在网络负载较低的时候性能不错，但如果网络负载很大时，冲突会很常见，因此而导致了网络性能的大幅下降。为了解决这一瓶颈问题，“交换式以太网”应运而生，这种系统的核心是使用交换机代替集线器。它是由一个高速的背板来连接各个网络接口，每个网络接口都互不相关，处于单独的冲突域中，就像将每个网络节点分在一个子网中，这样就使得以太网的效率得到了彻底的解决。

● IEEE 802.11 标准中定义了两种无线网络的拓扑结构：一种是特殊网络（Ad Hoc），它是一种点对点连接；另一种是基础设施网络，它是通过（60）将其连到现有网络中的，如果要防止未授权的用户连接到（60）上来，最简单的方法是（61）。

（60） A. 无线网卡　　B. 天线　　C. 无线接入点　　D. 无线集线器

（61） A. 设置登录口令　　B. 设置 MAC 地址过滤

C. 设置 WEP 加密　　D. 使用 Windows 域控制

查看答案

C, C

查看分析

分析：这是一道原理应用题，考查的无线局域网组建的一些基本知识。IEEE 802.11 标准中定义的两种无线网络的拓扑结构如图 a 所示：

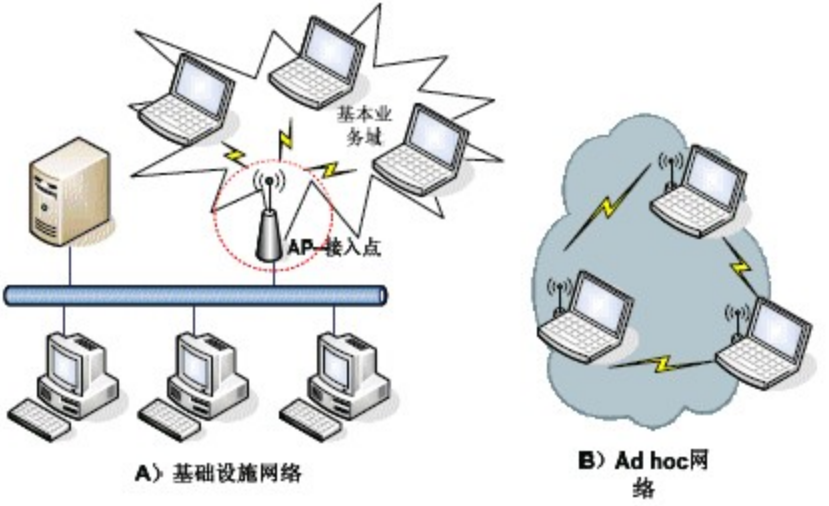

图 a 无线局域网组网示意

显然，我们可以发现在基础设施网络中，连接到现有网络中要使用的设备是 AP（无线接入点，图中用红色虚线圈黑色虚线圈是否更好？起来的部分）。

为了无线网络的连接安全，我们通常最简单的方式就是在无线 AP 上启用 WEP。其配置过程包括两个部分：一是在 AP 端将 WEP 开启，二是根据 AP 端的配置设置每台无线局域网用户的无线网卡属性。

在 AP 端实际上就是将 AP 配置中 WEP 的配置项改为“开启”，并输入相应的密码。然后将这个密码告知合法用户，合法用户如图 b 所示，在无线网卡属性中设置其 WEP 连接密码：

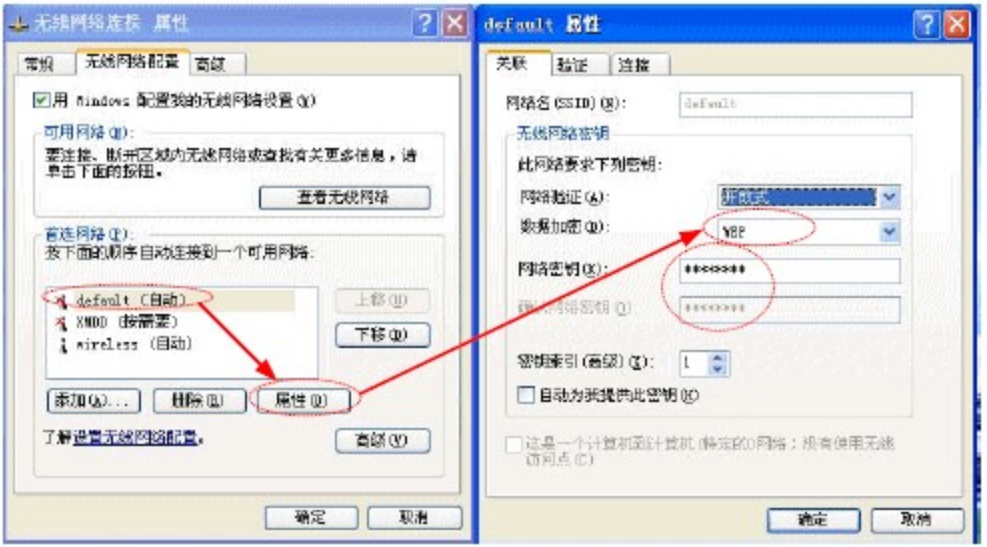

图 b 设置 WEP 连接密码

●码是一些码字组成的集合。一对码字之间的海明距离是（62），一个码的海明距离是所有不同码字的海明距离的（63），如果要检查出d位错，那么码的海明距离是（64）。如果信息长度为5位，要求纠正1位错，按照海明编码，需要增加的校验位是（65）位。以太网中使用的校验码标准是（66）。

（62）A. 码字之间不同的位数　　B. 两个码字之间相同的位数
　　C. 两个码字的校验和之和　　D. 两个码字的校验和之差

（63）A. 平均值　　B. 最大值　　C. 最小值　　D. 任意值

（64）A. d-1　　B. d+1　　C. 2d-1　　D. 2d+1

（65）A. 3　　B. 4　　C. 5　　D. 6

（66）A. CRC-12　　B. CRC-CCITT　　C. CRC-16　　D. CRC-32

查看答案

A, C, B, B, D

查看分析

分析：这题是校验码相关考题的一个典型代表，主要考查的是海明码距。在复习时，一定要掌握以下几个要点：将一个码字变成另一个码字时必须改变的最小位数就是码字之间海明距离，简称码距，没有加冗余校验码的任何编码，它们的码距就是1，可以发现“≤码距-1”位的错误，可以纠正“＜码距/2”位的错误（即为了纠d位错，就需要使用海明码距为2d+1的编码）。以及表a中所列出的CRC校验码标准：

表a 主要CRC校验码标准应用

网络协议	CRC位	应用点
HDLC	CRC16/CRC32	除帧标志位外的全帧
FR（帧中继）	CRC16/	除帧标志位外的全帧
ATM	CRC8	帧头校验
以太网（802.3）	CRC32	帧头（不含前导和帧启始符）
令牌总线（802.4）	CRC32	帧头（不含前导和帧启始符）
令牌环（802.5）	CRC32	帧头（从帧控制字段到LLC）
FDDI	CRC32	帧头（从帧控制字估到INFO）

码距是指两个码字逐位比较，其不同字符的个数就是两个码字的距离。所以一个码制的距离定义为：在这个编码制中各个码字之间的最小距离称为码距。例如，4 位二进制数中 16 个代码的码距为 1，若合法地增大码距，可提高发现错误的能力。d 个单比特错就可以把一个码字转换成另一个码字。为了检查出 d 个错（单比特错），需要使用海明距离为 $d+1$ 的编码；为了纠正 d 个错，需要使用海明距离为 $2d+1$ 的编码。

设信息位长度为 K，监督码长度为 r，若要指示一位错的 N（$N=K+r$）个可能位置，即纠正一位错，则必须满足如下关系：

$$2^r-1 \geqslant N=K+r$$

故当信息位为 5 时，满足 $2^r-1 \geqslant K+r=5+r$，则 $r=4$。

● 根据Boehm划分法，__（67）__是属于计划阶段的工作，在《GB/T8566-1995 信息技术—软件生存期过程》的定义的七大过程中，不包括__（68）__。

（67）A．可行性研究　　B．需求分析　　C．详细设计　　D．编码

（68）A．获取过程　　B．开发过程　　C．供应过程　　D．环境过程

查看答案

A, D

查看分析

分析：这是一道基本概念题，考查了软件生命周期的一些基本概念。对于软件生命周期的活动划分有两种标准。一是 Boehm 划分法，它将整个软件开发过程分为计划（问题定义、可行性研究）、开发（需求分析、总体设计、详细设计、编码、测试）、运行（维护）三大阶段。

而另一种则是国标划分法，GB/T8566-1995 信息技术—软件生存期过程》定义了获取过程、供应过程、开发过程、运行过程、维护过程、管理过程、支持过程七个部分。

● 不同的需求分析方法论，有不同的需求分析工具。其中（69）不属于需求分析工具，它是一种（70）。

（69）A. Petri 网　　B. 状态迁移图　　C. 用例分析　　D. PERT 图

（70）A. 软件设计　　B. 软件测试　　C. 项目管理　　D. 配置管理

查看答案

D,C

查看分析

分析：这是一道基本概念题，考查了常见的需求分析工具。用例分析是 OOSE 方法论中引入的一种最佳需求分析工具，Petri 网和状态迁移图是在需求分析中用于建立动态模型的工具。

而 PERT 是计划评审技术的简称，它是采用网络图来描述一个项目的任务网络。通常有两张图：一张图给出某一特定项目的所有任务，另一张图给出应按照什么次序来完成这些任务，给出各个任务之间的衔接。它可以用于确定关键路径、应用统计模型、计算边界时间。它和甘特图是两种最主要的项目管理工具。

● IPv6 is（71）for “Internet Protocol Version 6”。IPv6 is the “next generation” protocol designed by the IETF to（72）the current version Internet Protocol，IP Version 4（“IPv4”）。

Most of today's internet uses IPv4，which is now nearly twenty years old。IPv4 has been remarkably resilient in spite of its age，but it is beginning to have problems。Most importantly，there is a growing（73）of IPv4 addresses，which are needed by all new machines added to the Internet。

IPv6 fixes a number of problems in IPv4，such as the（74）number of available IPv4 addresses。It also adds many improvements to IPv4 in areas such as routing and network autoconfiguration。IPv6 is expected to gradually replace IPv4，with the two coexisting for a number of years during a transition（75）。

（71）A. short　B. abbreviate　C. abbreviation　D. initial
（72）A. substitution　B. replace　C. switchover　D. swap
（73）A. scarcity　B. lack　C. deficiency　D. shortage
（74）A. restrict　B. limited　C. confine　D. imprison
（75）A. days　B. period　C. phase　D. epoch

查看答案

B, D, D, B, B

查看分析

分析：IPv6 是“Internet Protocol Version 6”的**缩写（abbreviate）**。IPv6 是 IETF 设计来**替代（swap）**当前版本的 Internet 协议——Ipv4——的“下一代协议”。

现在在 Internet 上最常用的 IPv4，已经有接近 20 年的历史了。虽然 IPv4 应用很久了，其弹性还是很明显的，但现在开始出现问题了。最重要的是，当很多新的机器添加到 Internet 上来时，IPv4 地址日益**缺乏（shortage）**。

IPv6 修正了 IPv4 中的许多问题，例如受限的**（limited）**可用 IPv4 地址数量。它还加入了一些对 IPv4 的改进，诸如路由和网络自动配置。IPv6 将逐渐替代 IPv4，在转换**期（period）**内它们还将共存许多年。