【解析】本题考查指令系统基础知识。

指令顺序执行时，每条指令需要 9ΔT (4ΔT+2ΔT+3ΔT)，执行完 600 条指令需要 5400ΔT,若采用流水方式，则在分析和执行第 1 条指令时，就可以读取第 2 条指令，当第 1 条指令执行完成，第 2 条指令进行分析和执行，而第 3 条指令可进行读取操作。因此，第 1 条指令执行完成后，每 4ΔT 就可以完成 1 条指令，600 条指令的总执行时间为 9ΔT+599X4ΔT=2405ΔT。

若用 256K×8bit 的存储器芯片，构成地址 40000000H 到 400FFFFFH 且按字节编址的内存区域，则需（5）片芯片。

(5)A.4　　B.8　　C.16　　D.32

【答案】A

【解析】本题考查计算机系统中存储器知识。

地址 400000000H 到 4000FFFFFH 共有 FFFFFH (即 220)个以字节为单位的编址单元，而 256KX8bit 的存储器芯片可提供 218 个以字节为单位的编址单元，因此需要 4 片 (220/218)这种芯片来构成上述内存区域。

以下关于进度管理工具 Gantt 图的叙述中，不正确的是（6）。

(6)A.能清晰地表达每个任务的开始时间、结束时间和持续时间

B.能清晰地表达任务之间的并行关系

C.不能清晰地确定任务之间的依赖关系

D.能清晰地确定影响进度的关键任务

【答案】D

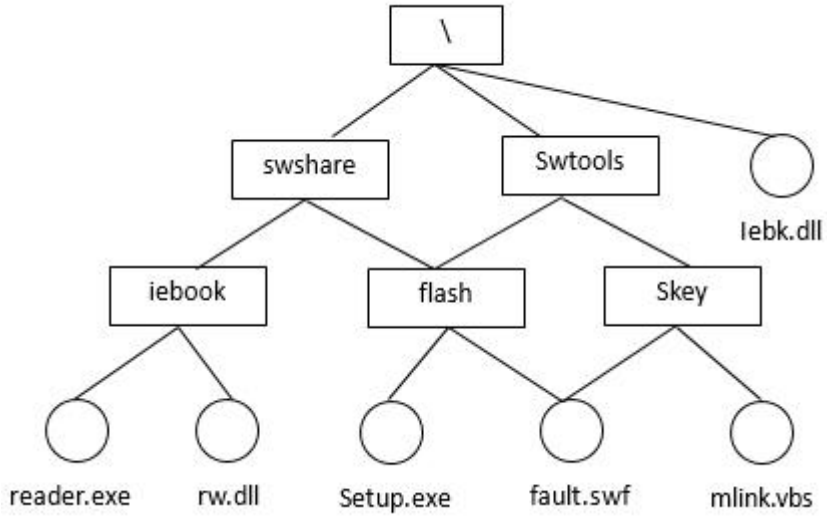
【解析】本题考查软件项目管理的基础知识。

Gantt 图是一种简单的水平条形图，以日历为基准描述项目任务。水平轴表示日历时间线，如天、周和月等，每个条形表示一个任务，任务名称垂直的列在左边的列中，图中水平条的起点和终点对应水平轴上的时间，分别表示该任务的开始时间和结束时间，水平条的长度表示完成该任务所持续的时间。当日历中同一时段存在多个水平条时，表示任务之间的并发。

Gantt 图能清晰地描述每个任务从何时开始，到何时结束，任务的进展情况以及各个任务之间的并行性。但它不能清晰地反映出各任务之间的依赖关系，难以确定整个项目的关键

所在，也不能反映计划中有潜力的部分。

若某文件系统的目录结构如下图所示，假设用户要访问文件 fault.swf，且当前工作目录为 swshare，则该文件的全文件名为（7），相对路径和绝对路径分别为（8）。



(7)A.fault.swf　　B.flash\fault.swf

C.swshare\flash\fault.swf　　D.\swshare\flash\fault.swf

(8)A.swshare\flash\和\flash\　　B.flash\和\swshare\flash\

C.\swshare\flash\和 flash\　　D.\flash\和\swshare\flash\

【答案】D　B

【解析】本题考查对操作系统文件管理方面的基础知识。

路径名是指操作系统查找文件所经过的目录名以及目录名之间的分隔符构成的。通常，操作系统中全文件名是指路径名+文件名。

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

在引用调用方式下进行函数调用，是将（9）。

(9)A.实参的值传递给形参　　B.实参的地址传递给形参

C.形参的值传递给实参　　D.形参的地址传递给实参

【答案】B

【解析】本题考查程序语言基础知识。

值调用和引用调用是实现函数调用时传递参数的两种基本方式。在值调用方式下，是将实参的值传给形参，在引用调用方式下，是将实参的地址传递给形参。

王某买了一幅美术作品原件，则他享有该美术作品的（10）。

(10)A.著作权　　B.所有权　　C.展览权　　D.所有权与展览权

【答案】D

【解析】本题考查知识产权基本知识。

绘画、书法、雕塑等美术作品的原件可以买卖、赠与。但获得一件美术作品并不意味着获得该作品的著作权。我国著作权法规定：“美术等作品原件所有权的转移，不视为作品著作权的转移，但美术作品原件的展览权由原件所有人享有。”这就是说作品物转移的事实并不引起作品著作权的转移，受让人只是取得物的所有权和作品原件的展览权，作品的著作权仍然由作者享有。

路由器连接帧中继网络的接口是（11），连接双绞线以太网的接口是（12）。

(11)A.AUI 接口　　B.RJ-45 接口　　C.Console 接口　　D.Serial 接口

(12)A.AUI 接口　　B.RJ-45 接口　　C.Console 接口　　D.Serial 接口

【答案】D　B

【解析】

路由器有以下几种联网接口 ：

①RJ45 端在这种端口上通过双绞线连接以太网。10Base-T 的 RJ~45 端口标识为“ETH”，而 100Base-TX 的 RJ45 端 LJ 标识为 10/100bTX”，这是因为快速以太网路由器采用 10/100Mb/s 自适应电路。

②AUI 端口:这是一种 D 型 15 针连接器，用在令牌环网或总线型以太网中。路由器经 AUI 端口通过粗同轴电缆收发器连接 10Base-5 网络，也可以通过外接的 AUI-to-RJ-45 适配器连接 10Base-T 以太网，还可以借助其他类型的适配器实现与 10Basc-2 细同轴电缆或 10Base-F 光缆的连接。

③高速同步串口 ：在路由器与广域网的连接中，应用最多的是高速同步串行口(Synchronous Serial Port),这种端口用于连接 DDN、帧中继、X.25 和 PSTN 等网络。通过这种端口所连接的网络两端要求同步通信，以很高的速宰进行数据传输。

④ISDN BR1 端口：这种端口通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。ISDN BRI 三个通道（2B+D)的总带宽为 144 kb/s,端口采用 RJ-45 标准，与 ISDN NT1 的连接使用 RJ-45-to-RJ~45 直通线。

⑤Console 端口：Console 端口通过配置专用电缆连接至计算机串行口，利用终端仿真程序（如 Windows 中的超级终端）对路由器进行本地配置。路由器的 Console 端 U 为 RJ-45U。Console 端口不支持硬件流控。

⑥AUX 端口：对路由器进行远程配置时要使用“AUX”端口（Auxiliary Prot)。AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行电路转换。AUX 端口支持硬件流控。

⑦异步串口：异步串口（ASYNC)主要应用于与 Modem 或 Modem 池的连接，以实现远程计算机通过 PSTN 拨号接入。异步端口的速率不是很高，也不要求同步传输，只要求能连续通信就可以了。

在地面上相距 2000 公里的两地之间通过电缆传输 4000 比特长的数据包，数据速率为 64Kb/s，从开始发送到接收完成需要的时间为（13）。

(13)A.48ms　　B.640ms　　C.32.5ms　　D.72.5ms

【答案】D

【解析】

从开始发送到接收完成的时间包含数据包的发送（或接收）时间，以及信号在电缆中的传播延迟时间。电信号在电缆中的传播速度是 200m/μs，所以传播延迟时间为 2000Km÷200m/μs=10ms,而发送(或接收)数据包的时间为4000bit÷64Kb/s=62.5ms,总共是72.5ms。

海明码是一种纠错编码，一对有效码字之间的海明距离是（14)，如果信息为 6 位，要求纠正 1 位错，按照海明编码规则，需要增加的校验位是（15)位。

(14)A.两个码字的比特数之和　　B.两个码字的比特数之差

C.两个码字之间相同的比特数　　D.两个码字之间不同的比特数

(15)A.3　　B.4　　C.5　　D.6

【答案】D　B

【解析】

海明距离是把一个有效码字变成另一个有效码字所要改变的位数。如果对于 m 位的数据，增加 k 位冗余位，则组成 n=m+k 位的纠错码。对于 2m 个有效码字中的任意一个，都有 n 个无效但可以纠错的码字。这些可纠错的码字与有效码字的距离是 1，含单个错误位。这样，对于一个有效码字总共有 n+1 个可识别的码字。这 n+1 个码字相对于其他 2m-1 个有效码字的距离都大于 1。这意味着总共有 2m (n+1)个有效的或是可纠错的码字。显然这个数应小于等于码字的所有可能的个数，即 2n。于是，我们有

$2^m (n+1) < 2^n$

因为 n=m+k，我们得出

$m+k+1<2^k$

对于给定的数据位 m，上式给出了 k 的下界，即要纠正单个错误，A 必须取的最小值。本题中 m=6，所以 k=4。

IPv4 的 D 类地址是组播地址，用作组播标识符，其中 224.0.0.1 代表（16），224.0.0.5 代表（17）

(16)A.DHCP 服务器　　B.RIPv2 路由器

C.本地子网中的所有主机　　D.OSPF 路由器

(17)A.DHCP 服务器　　B.RIPv2 路由器

C.本地子网中的所有主机　　D.OSPF 路由器

【答案】C　D

【解析】

IPv4 的 D 类地址是组播地址，用作一个组的标识符，其地址范围是 224.0.0.0～239.255.255.255。按照约定，D 类地址被划分为 3 类：

224.0.0.0～224.0.0.255:保留地址，用于路由协议或其他下层拓扑发现协议、以及维护管理协议等，例如 224.0.0.1 代表本地子网中的所有主机，224.0.0.2 代表本地子网中的所有路由器，224.0.0.5 代表所有 OSPF 路由器，224.0.0.5 代表所有 RIP2 路由器，224.0.0.12 代表 DHCP 服务器或中继代理，224.0.0.13 代表所有支持 PIM 的路由器等。

224.0.1.0～238.255.255.255:用于全球范围的组播地址分配，可以把这个范围的 D 类地址动态地分配给一个组播组，当一个组播会话停止时，其地址被回收，以后还可以分配给新出现的组播组。

239.0.0.0～239.255.255.255:在管理权限范围内使用的组播地址，限制了组播的范围，可以在本地子网中作为组播地址使用。

按照 IETF 定义的区分服务(Diffserv)技术规范,边界路由器要根据 IP 协议头中的(18)字段为每一个 IP 分组打上一个称为 DS 码点的标记，这个标记代表了改分组的 QoS 需求。

(18)A.目标地址　　B.源地址　　C.服务类型　　D.段偏置值

【答案】C

【解析】

区分服务（DiffServ)将具有相同特性的若干业务流汇聚起来，为整个汇聚流提供服务，而不是面向单个业务流来提供服务。

每个 IP 分组都要根据其 QoS 需求打上一个标记,这种标记称为 DS 码点(DSCode Point, DSCP),可以利用 IPv4 协议头中的服务类型(Type of Service)字段，或者 IPv6 协议头中的通信类别（Traffic Class)字段来实现，这样就维持了现有的 IP 分组格式不变。

在使用 DiffServ 服务之前，服务提供者与用户之间先要建立一个服务等级约定 (Service Level Agreement, SLA)。这样，在各个应用中就不再需要类似的机制，从而可以保持现有的应用不变。

Internet 中能实现区分服务的连续区域被称为 DS 域（DS Domain),在一个 DS 域中，服务提供策略（Service Provisioning Policies)和逐跳行为（Per-Hop Behavior，PHB)都 是一致的。PHB 是（外部观察到的）DS 结点对一个分组的转发行为。

ICMP 协议属于因特网中的（19）协议，ICMP 协议数据单元封装在（20）中传送。

(19)A.数据链路层　　B.网络层　　C.传输层　　D.会话层

(20)A.以太帧　　B.TCP 段　　C.UDP 数据报　　D.IP 数据报

【答案】B　D

【解析】

ICMP (Internet control Message Protocol)与 IP 协议同属于网络层，用于传送有关通信问题的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送,因而不保证可靠的提交。ICMP 报文有 11 种之多，报文格式如下图所示。其中的类型字段表示 ICMP 报文的类型，代

码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

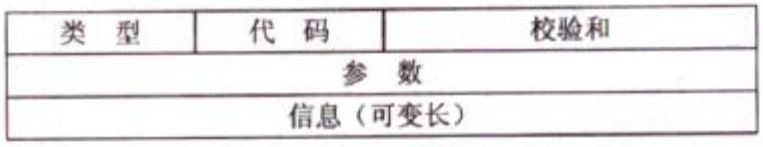


图 ICMP 报文格式

TCP/IP 网络中最早使用的动态路由协议是（21）协议，这种协议基于（22）算法来计算路由。

(21)A.RIP　　B.OSPF　　C.PPP　　D.IS-IS

(22)A.路由信息　　B.链路状态　　C.距离矢量　　D.最短通路

【答案】A　C

【解析】

路由协议（routingprotocol)是路由器之间实现路由信息共享的一种机制，它允许路由器之间通过交换路由信息动态地维护各自的路由表。IP 协议是根据路由表进行分组转发的协议，按照业内的说法，应该叫做被路由的协议（routedprotocol)。

最早使用的路由协议是路由信息协议（Routing Information Protocol，RIP)。RIP 的原型出现在 UNIX Berkley 4.3 BSD 中，它采用 Bellman-Ford 的距离矢量路由算法，用于在 ARPAnet 中计算最佳路由，现在的 RIP 作为内部网关协议运行在基于 TCP/IP 的网络中。RIP 适用于小型网络，因为它允许的跳步数不超过 15 步。

动态划分 VLAN 的方法中不包括（23）。

(23)A.网络层协议　　B.网络层地址　　C.交换机端口　　D.MAC 地址

【答案】C

【解析】

在交换机上实现 VLAN,可以采用静态的或动态的方法：

①静态分配 VLAN：为交换机的各个端口指定所属的 VLAN。这种基于端口的划分方法是把各个端口固定地分配给不同的 VLAN，任何连接到交换机的设备都属于接入端口所在的 VLAN。

②动态分配 VLAN:动态 VLAN 通过网络管理软件包来创建，可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播域或管理策略来划分 VLAN。根据 MAC 地址划分 VLAN 的方法

应用最多，一般交换机都支持这种方法。无论一台设备连接到交换网络的任何地方，接入交换机根据设备的MAC地址就可以确定该设备的VLAN成员身份。这种方法使得用户可以在交换网络中改变接入位置，而仍能访问所属的VLAN。

但是当用户数量很多时，对每个用户设备分配VLAN的工作量是很大的管理负担。

在局域网中划分VLAN，不同VLAN之间必须通过（24）连接才能互相通信，属于各个VLAN的数据帧必须同时打上不同的（25）。

(24)A.中继端口　　B.动态端口　　C.接入端口　　D.静态端口

(25)A.VLAN优先级　　B.VLAN标记　　C.用户标识　　D.用户密钥

【答案】A　B

【解析】

在划分成VLAN的交换网络中，交换机端口之间的连接分为两种：接入链路(Access-Link Connection)和中继连接（Trunk Connection)。接入链路只能连接具有标准以太网卡的设备，也只能传送属于单个VLAN的数据包。任何连接到接入链路的设备都属于同一广播域，这意味着，如果有10个用户连接到一个集线器，而集线器被插入到交换机的接入链路端口，则这10个用户都属于该端口规定的VLAN。

中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个VLAN。在进入中继端口时，交换机在数据包中加入VLAN标记（IEEE802.11q)。这样，在中继链路另一端的交换机就不仅根据目标地址、而且要根据数据包所属的VLAN进行转发决策。

为了与接入链路设备兼容，在数据包进入接入链路连接的设备时，交换机要删除VLAN标记，恢复原来的帧结构。添加和删除VLAN标记的过程是由交换机中的专用硬件自动实现的，处理速度很快，不会引入太大的延迟。从用户角度看，数据源产生标准的以太帧，目标接收的也是标准的以太帧，VLAN标记对用户是透明的。

城域以太网在各个用户以太网之间建立多点第二层连接，IEEE802.1ad定义运营商网桥协议提供的基本技术是在以太网帧中插入（26）字段，这种技术被称为（27）技术。

(26)A.运营商VLAN标记　　B.运营商虚电路标识

C.用户VLAN标记　　D.用户帧类型标记

(27)A.Q-in-Q　　B.IP-in-IP　　C.NAT-in-NAT　　D.MAC-in-MAC

【答案】A　A

【解析】

城域以太网论坛（Metro Ethernet Forum, MEF)提出以太局域网服务（E-LAN services)是指，由运营商建立一个城域以太网，在用户以太网之间提供多点对多点的第二层连接，任意两个以太网用户之间都可以通过成域以太网通信。

提供 E-LAN 服务的基本技术是 802.1q 的 VLAN 帧标记。我们假定，各个用户的以太网称为 C-网，运营商建立的城域以太网称为 S-网。如果不同 C-网中的用户要进行通信，以太顿在进入用户网络接口（User-Network Interface, UNI)时被插入一个 S-VID (Server Provider-VLAN ID)字段，用于标识 S-网中的传输服务，而用户的 VLAN 帧标记（C-VID)则保持不变，当以太帧到达目标 C-网时，S-VID 字段被删除，如下图所示。这样就解决了两个用户以太网之间透明的数据传输问题。这种技术定义在 lEEE802.1ad 的运营商网桥协议（Provider Bridge Protocol)中，被称为 Q-in-Q 技术。

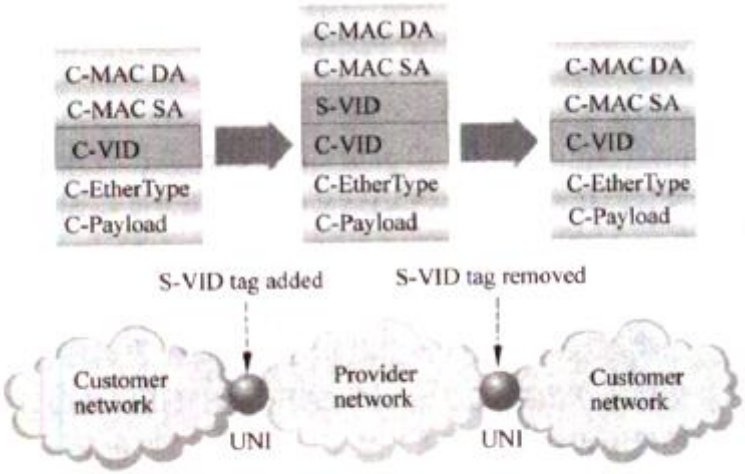


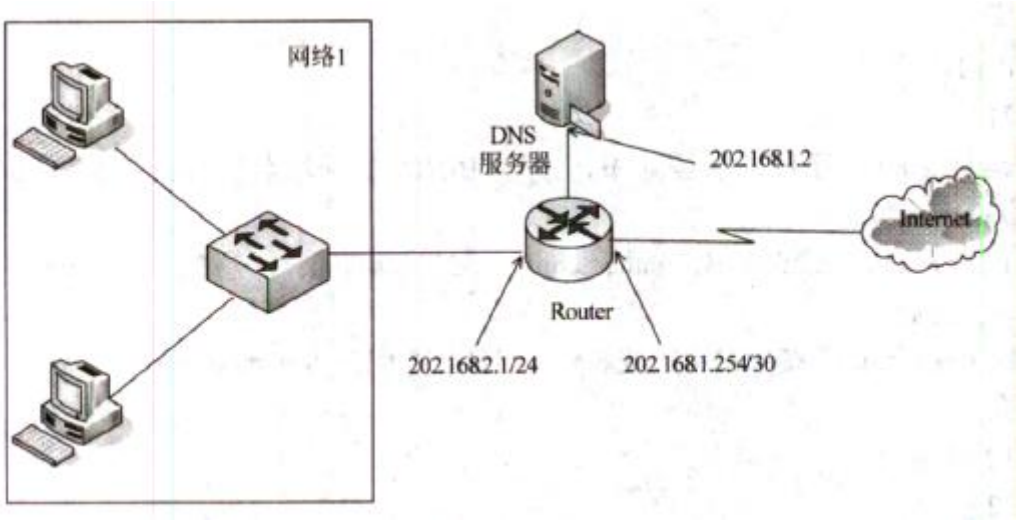
图 802.1ad 的帧格式

Q-in-Q 实际上是把用户 VLAN 嵌套在城域以太网的 VLAN 中传送，由于其简单性和有效性而得到电信运营商的青睐。但是这样以来，所有用户的 MAC 地址在城域以太网中都是可见的，任何 C-网的改变都会影响到 S-网的配置，增加了管理的难度。而且 S-VID 字段只有 12 位，只能标识 4096 个不同的传输服务，网络的可扩展性也受到限制。从用户角度看，网络用户的 MAC 地址都暴露在整个城域以太网中，使得网络的安全性受到威胁。

为了解决上述问题，IEEE 802.1 ah 标准提出了运齊商主干网桥(Provider Backbone Bridge, PBB)协议。所谓主干网桥就是运营商网络边界的网桥，通过 PBB 对用户以太帧再封装一层运营商的 MAC 帧头，添加主干网目标地址和源地址（B-DA，B-SA)、主干网 VLAN 标识（B-VID)，以及服务标识（I-SID)等字段。由于用户以太帧被封装在主干网以太帧中，所以这种技术被

称为 MAC-in-MAC 技术。

网络配置如下图所示，在路由器 Router 中配置网络 1 访问 DNS 服务器的命令是（28），网络 1 访问 Internet 的默认路由命令是（29）。



(28)A. ip route 202.168.1.2 255.255.255.0 202.168.1.2

B. ip route 202.168.1.2 255.255.255.255 202.168.1.2

C. ip route 0.0.0.0 0.0.0.0 202.168.1.253

D. ip route 255.255.255.255 0.0.0.0 202.168.1.254

(29)A. ip route 202.168.1.2 255.255.255.0 202.168.1.2

B. ip route 202.168.1.2 255.255.255.255 202.168.1.2

C. ip route 0.0.0.0 0.0.0.0 202.168.1.253

D. ip route 255.255.255.255 0.0.0.0 202.168.1.254

【答案】B　C

【解析】本试题考查静态路由配置命令。

网络 1 访问 DNS 服务器时目的网络是 DNS 服务器单个 IP，地址为 202.168.1.2,路由器转发的是下一跳即为 202.168.1.2,故命令为 ip route 202.168.1.2 255.255.255.255 202.168.1.2。

网络 1 访问 Internet 时,地址任意,路由时下一跳为 202.168.1.253,故默认路由为 ip route 0.0.0.0 0.0.0.0 202.168.1.253。

与 HTTP1.0 相比，HTTP1.1 的优点不包括（30）。

(30)A.减少了 RTTs 数量　　B.支持持久连接

C.减少了 TCP 慢启动次数　　D.提高了安全性

【答案】D

【解析】

与 HTTP1.0 相比，HTTP 1.1 最大的改进是支持持久连接，从而减少了 TCP 慢启动的次数，进而减少了 RTTs 数量。

在运行 Linux 系统的服务器中，使用 BIND 配置域名服务器，主配置文件存放在（31）。

(31)A.name.conf　　B.named.conf　　C.dns.conf　　D.dnsd.conf

【答案】B

【解析】

BIND 是 Linux 系统中常用的域名配置组件，主配置为 named.conf。

在 Linux 系统中，root 用户执行 shutdown－rnow 命令，系统将会（32）。

(32)A.重新启动　　B.进入单用户模式　　C.休眠　　D.关机

【答案】A

【解析】

Linux 系统中采用 shutdown -rnow 命令重新启动系统。

结构化综合布线系统中的干线子系统是指（33）。

(33)A.管理楼层内各种设备的子系统　　B.连接各个建筑物的子系统

C.工作区信息插座之间的线缆子系统　　D.实现楼层设备间连接的子系统

【答案】D

【解析】

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统，如下图所示。

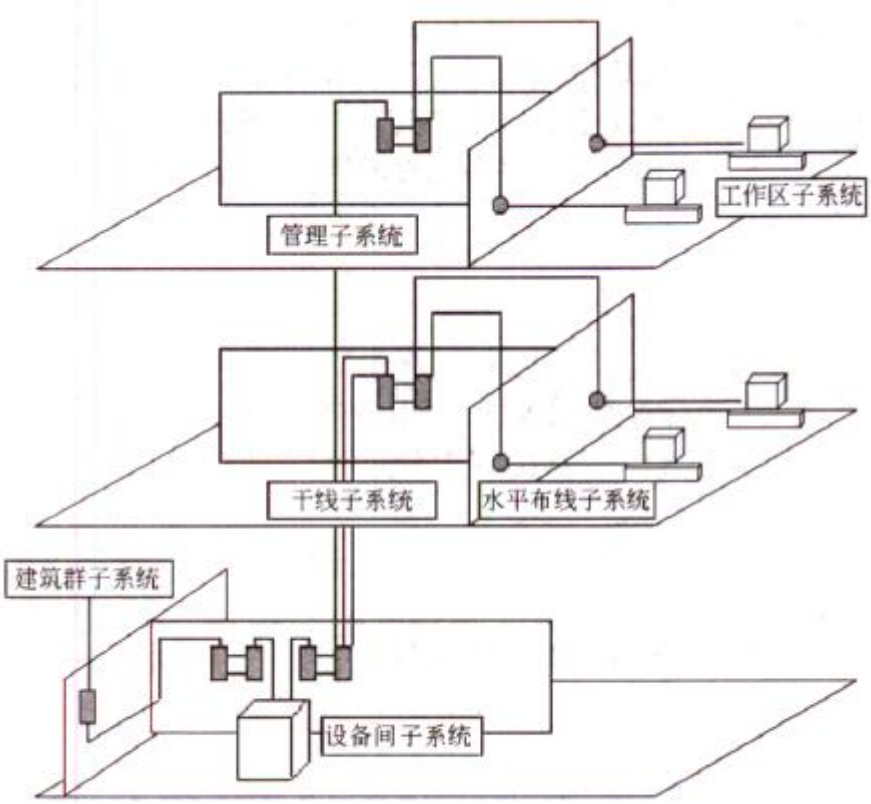


图　结构化布线示意图

①工作区子系统（Work Location）

工作区子系统是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区。工作区应支持电话、数据终端、计算机、电视机、监视器以及传感器等多种终端设备。

②水平布线子系统（Horizontal）

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平子系统的作用是将干线子系统线路延伸到用户工作区。在进行水平布线时，传输介质中间不宜有转折点，两端应直接从配线架连接到工作区的信息插座。水平布线的布线通道有两种：一种是暗管预埋、墙面引线方式，另一种是地下管槽、地面引线方式。前者适用于多数建筑系统，一旦铺设完成，不易更改和维护；后者适合于少墙多柱的环境，更改和维护方便。

③管理子系统（Administration）

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。交连设备通过水平布线子系统连接到各个工作区的信息插座，集线器或交换机与交连设备之间通过短线缆互连，这些短线被称为跳线。通过跳线的调整，可以对工作区的信息插座和交换机端

口之间进行连接切换。

④干线子系统（Backbone）

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头端接于设备间的主配线架上，另一头端接在楼层接线间的管理配线架上。主干子系统在设计时，对于旧建筑物，主要采用楼层牵引管方式铺设，对于新建筑物，则利用建筑物的线井进行铺设。

⑤设备间子系统（Equipment）

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如 PBX、网络设备和监控设备等）之间的连接。

⑥建筑群子系统（Campus）

建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。大楼之间的布线方法有三种，一种是地下管道敷设方式，管道内敷设的铜缆或光缆应遵循电话管道和入孔的各种规定，安装时至少应预留 1 到 2 个备用管孔，以备扩充之用。第二种是直埋法，要在同一个沟内埋入通信和监控电缆，并应设立明显的地面标志。最后一种是架空明线，这种方法需要经常维护。

假设网络的生产管理系统采用 B/S 工作方式，经常上网的用户数为 100 个，每个用户每分钟平均产生 11 个事务，平均事务量大小为 0.06MB，则这个系统需要的传输速率为（34）。

(34)A.5.28Mb/s　　B.8.8Mb/s　　C.66Mb/s　　D.528Mb/s

【答案】B

【解析】

应用总信息传输速率=平均事务量大小 X 每字节位数 X 每个回话事务数 X 平均用户数/平均会话长度

系统需要的信息传输速率 R=0.06MBX8X11X100÷60= 8.8Mb/s

在 windows 命令行窗口中进入 nslookup 交互工作方式，然后键入 set type=mx,这样的设置可以（35）。

(35)A.切换到指定的域名服务器　　B.查询邮件服务器的地址

C.由地址查找对应的域名　　D.查询域名对应的各种资源

【答案】B

【解析】

Nslookup 命令用于显示 DNS 查询信息，诊断和排除 DNS 故障，有交互式和非交互式两种工作方式。

所谓非交互式工作就是只使用一次 Nslookup 命令后又返回到 Cmd.exe 提示符下。Nslookup 命令后面可以跟随一个或多个命令行选项，用于设置查询参数。每个命令行的各选项由一个连字符后跟选项的名字，有时还要加一个等号“=”和一个数值。例如应用默认的 DNS 服务器由域名查找 IP 地址。

```
C:\>nslookup ns1.isi.edu
Server: ns1.domain.com
Address: 202.30.19.1
Non-authoritative answer:    #给出应答的服务器不是该域的权威服务器
Name: ns1.isi.edu
Address: 128.9.0.107         #查出的 IP 地址
```

如果需要查找多项数据，可以使用 Nslookup 的交互工作方式。在 Cmd.exe 提示符下输入 nslookup 后回车，就进入了交互工作方式，命令提示符变成“>”。在命令提示符 “>”下输入 help 或?，会显示可用的命令列表，如果输入 exit，则返回 Cmd.exe 提示符。

在交互方式下，可以用 set 命令设置选项，满足指定的查询需要。例如查询本地域的邮件交换器信息的过程如下。

```
C:\> nslookup
Default Server: ns1.domain.com
Address: 202.30.19.1
> set type=mx
> 163.com.cn
Server: ns1.domain.com
Address: 202.30.19.1

Non-authoritative answer:
163.com.cn      MX preference = 10, mail exchanger =mx1.163.com.cn
163.com.cn      MX preference = 20, mail exchanger =mx2.163.com.cn
mx1.163.com.cn  internet address = 61.145.126.68
mx2.163.com.cn  internet address = 61.145.126.30
>
```

FTP 提供了丰富的命令，用来更改本地计算机工作目录的命令是（36）。

(36)A.get　　B.list　　C.!cd　　D.!list

【答案】C

【解析】

FTP 用来更改本地计算机工作目录的命令是!cd。

在进行域名解析过程中，由（37）获取的解析结果耗时最短。

(37)A.主域名服务器　　B.辅域名服务器　　C.本地缓存　　D.转发域名服务器

【答案】C

【解析】

域名解析的过程是先查本地缓存，再查主域名服务器；若主域名服务器查找不到记录，转到转发域名服务器进行查询；若主域名服务器不工作，启用辅域名服务器进行查询。不论是主域名服务器、转发域名服务器还是辅域名服务器，都需要在资源记录数据库中去匹配，时间较本地缓存要长。

DNS 通知是一种推进机制，其作用是使得（38）。

(38)A.辅助域名服务器及时更新信息　　B.授权域名服务器向管区内发送公告

C.本地域名服务器发送域名解析申请　　D.递归查询迅速返回结果

【答案】A

【解析】

DNS 通知机制的作用是使得辅助域名服务器及时更新信息。

在 DNS 资源记录中，（39）记录类型的功能是把 IP 地址解析为主机名。

(39)A.A　　B.NS　　C.CNAME　　D.PTR

【答案】D

【解析】

在 DNS 资源记录中，记录类型 A 的功能是域名映射为 IP 地址；记录类型 NS 的功能是给出区域的授权服务器；记录类型 CNAME 的功能是为正式主机名（canonical name）定义了一个别名（alias)；记录类型 PTR 的功能是把 IP 地址解析为主机名。

以下关于 DHCP 的描述中，正确的是（40）。

(40)A.DHCP 客户机不可能跨越网段获取 IP 地址

B.DHCP 客户机只能收到一个 dhcpoffer

C.DHCP 服务器可以把一个 IP 地址同时租借给两个网络的不同主机

D.DHCP 服务器中可自行设定租约期

【答案】D

【解析】

DHCP 客户机可通过配置 DHCP 中继跨网段获取 IP 地址；DHCP 客户机可能收到一个 dhcpoffer，通常选择最先到达的 dhcpoffer 提供的地址；DHCP 服务器把一个 IP 地址只能租借给一台主机；DHCP 服务器中可自行设定租约期。

高级加密标准 AES 支持的 3 种密钥长度中不包括（41）。

(41)A.56　　B.128　　C.192　　D.256

【答案】A

【解析】本题考查数据加密算法的基础知识。

1997 年 1 月，美国国家标准与技术局（NIST)为高级加密标准征集新算法。最初从许多响应者中挑选了 15 个候选算法，经过了世界密码共同体的分析，选出了其中的 5 个。经过用 ANSI C 和 Java 语言对 5 个算法的加/解密速度、密钥和算法的安装时间，以及对各种攻击的拦截程度等进行了广泛的测试后，2000 年 10 月，NIST 宣布 Rijndael 算法为 AES 的最佳候选算法，并于 2002 年 5 月 26 日发布正式的 AES 加密标准。

AES 支持 128，192 和 256 位三种密钥长度，能够在世界范围内免版税使用，提供的安全级别足以保护未来 20～30 年内的数据，可以通过软件或硬件实现。

在报文摘要算法 MD5 中，首先要进行明文分组与填充，其中分组时明文报文摘要按照（42）位分组。

(42)A.128　　B.256　　C.512　　D.1024

【答案】C

【解析】本题考查报文摘要算法的基础知识。

报文摘要算法 MD5 的基本思想就是用足够复杂的方法把报文位充分“弄乱”，使得每一个输出位都受到每一个输入位的影响。具体的操作分成下列步骤：

①分组和填充：把明文报文按 512 位分组，最后要填充一定长度的“1000....”，使得报文

长度=448 (mod512)

②附加。域后加上 64 位的报文长度字段，整个明文恰好为 512 的整数倍。

③初始化。置 4 个 32 位长的缓冲区 ABCD 分别为：

A=01234567 B=89ABCDEF C=FEDCBA98 D=76543210

④处理。用 4 个不同的基本逻辑函数（F，G，H，I)进行 4 轮处理，每一轮以 ABCD 和当前 512 位的块为输入，处理后送入 ABCD (128 位)，产生 128 位的报文摘要。

以下关于 IPsec 协议的描述中，正确的是（43）。

(43)A.IPsec 认证头(AH)不提供数据加密服务

B.IPsec 封装安全负荷（ESP）用于数据完整性认证和数据源认证

C.IPsec 的传输模式对原来的 IP 数据报进行了封装和加密，再加上了新的 IP 头

D.IPsec 通过应用层的 Web 服务器建立安全连接

【答案】A

【解析】本题考查 IPsec 协议的基础知识。

IPsec 的功能可以划分为三类：①认证头（Authentication Header, AH)：用于数据 完整性认证和数据源认证。②封装安全负荷（Encapsulating Security Payload，ESP)： 提供数据保密性和数据完整性认证，ESP 也包括了防止重放攻击的顺序号。③Internet 密钥交换协议（Internet Key Exchange, IKE)：用于生成和分发在 ESP 和 AH 中使用的 密钥，IKE 也对远程系统进行初始认证。

IPsec 在传输模式，IP 头没有加密，只对 IP 数据进行了加密；在隧道模式，IPSec 对原来的 IP 数据报进行了封装和加密，加上了新的 IP 头。

IPSec 的安全头插入在标准的 IP 头和上层协议（例如 TCP)之间，任何网络服务和网络应用可以不经修改地从标准 IP 转向 IPSec,同时 IPSec 通信也可以透明地通过现有的 IP 路由器。

防火墙的工作层次是决定防火墙效率及安全的主要因素，下面叙述中正确的是（44）。

(44)A.防火墙工作层次越低，工作效率越高，安全性越高

B.防火墙工作层次越低，工作效率越低，安全性越低

C.防火墙工作层次越高，工作效率越高，安全性越低

D.防火墙工作层次越高，工作效率越低，安全性越高

【答案】D

【解析】本题考查防火墙的基础知识。

防火墙的性能及特点主要由以下两方面所决定。

①工作层次。这是决定防火墙效率及安全的主要因素。一般来说，工作层次越低，则工作效率越高，但安全性就低了；反之，工作层次越高，工作效率越低，则安全性越高。

②防火墙采用的机制。如果采用代理机制，则防火墙具有内部信息隐藏的特点，相对而言，安全性高，效率低；如果采用过滤机制，则效率高，安全性却降低了。

在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法中不包括（45）。

(45)A.匹配模式　　B.密文分析　　C.数据完整性分析　　D.统计分析

【答案】B

【解析】本题考查入侵检测系统的基础知识。

入侵检测系统由 4 个模块组成：事件产生器、事件分析器、事件数据库和响应单元。其中，事件分析器负责接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其分析方法有三种：

①模式匹配：将收集到的信息与已知的网络入侵数据库进行比较，从而发现违背安全策略的行为。

②统计分析：首先给系统对象（例如用户、文件、目录和设备等）建立正常使用时的特征文件（Profile),这些特征值将被用来与网络中发生的行为进行比较。当观察值超出正常值范围时，就认为有可能发生入侵行为。

③数据完整性分析：主要关注文件或系统对象的属性是否被修改，这种方法往往用于事后的审计分析。

在 Windows Server 2003 环境中有本地用户和域用户两种用户，其中本地用户信息存储在（46）。

(46)A.本地计算机的 SAM 数据库　　B.本地计算机的活动目录

C.域控制器的活动目录　　D.域控制器的 SAM 数据库中

【答案】A

【解析】本题考查 Windows Server 2003 的相关网络管理知识。

在 Windows Server 2003 环境中有本地用户和域用户两种用户。本地用户信息存储在本

地计赏机的安全账户管理器（Security Accounts Manager，SAM)数据库内，当本地计算机用户尝试本地登录时，SAM 数据库中的账户信息要经过验证。域用户信息存储在域控制器的活动目录中。活动目录是网络中的一个中央数据库，存储各种资源信息。

管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理产生一个新行，其状态对象值为（47）。

(47)A.createRequest　　B.underCreate　　C.valid　　D.invalid

【答案】A

【解析】本题考查 RMON 的基本知识。

管理站用 Set 命令在 RMON 表中增加新行，遵循的规则是：管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理产生一个新行，其状态对象的值为 createRequest。

SNMPc 支持各种设备访问方式，在 SNMPc 支持的设备访问方式中，只是用于对 TCP 服务轮询的方式是（48）。

(48)A.无访问模式　　B.ICMP（Ping）　　C.SNMPv1 和 v2c　　D.SNMPv3

【答案】A

【解析】本题考查网络管理软件 SNMPc 的设备访问模式。

SNMPc 支持各种设备访问方式，包括 TCP、ICMP (Ping), SNMPv1、SNMPv2C 和 SNMPv3。其中无访问模式（仅对 TCP):无访问模式只是用于对 TCP 服务的轮询，
当 ICMP/SNMP 访问受防火墙限制时使用这种方式。ICMP (Ping)： ICMP (Ping)用于不支持 SNMP 但仍可通过 Ping 测试其是否有响应的设备。此类设备也可能包括服务器和工作站。SNMPv1 和 v2C: SNMPv1 和 SNMP v2C 是非常相似的 SNMP 代理协议，目前部署的网络设备大多数都使用这两种协议。任何支持 v2C 的设备一般同样也支持 v1。SNMPc 根据需要在两种方式之间自动智能切换。因此在多数情况下总是会选择 SNMPv1 作为设备的访问方式。SNMPv3: SNMP v3 是安全的 SNMP 代理协议，支持身份验证和加密功能。

下列数据类型中，SNMPv2 支持而 SNMPv1 不支持的是（49）。

(49)A.OCTET STRING　　B.OBJECT descriptor　　C.Unsigned32　　D.Gauge32

【答案】C

【解析】本题考查 SNMPv1 和 SNMPv2 的数据类型。

SNMPv2 增加了两种新的数据类型 Unsigned32 和 Counter64。这两种是 SNMPv2 支持而 SNMPv1 不支持的数据类型。

某实验室使用无线路由器提供内部上网，无线路由器采用固定 IP 地址连接至校内网，实验室用户使用一段时间后，不定期出现不能访问互联网的现象，经测试无线路由器工作正常，同时有线接入的用户可以访问互联网，分析以上情况，导致这一故障产生的最可能的原因是（50）.

(50)A.无线路由器配置错误　　B.无线路由器硬件故障

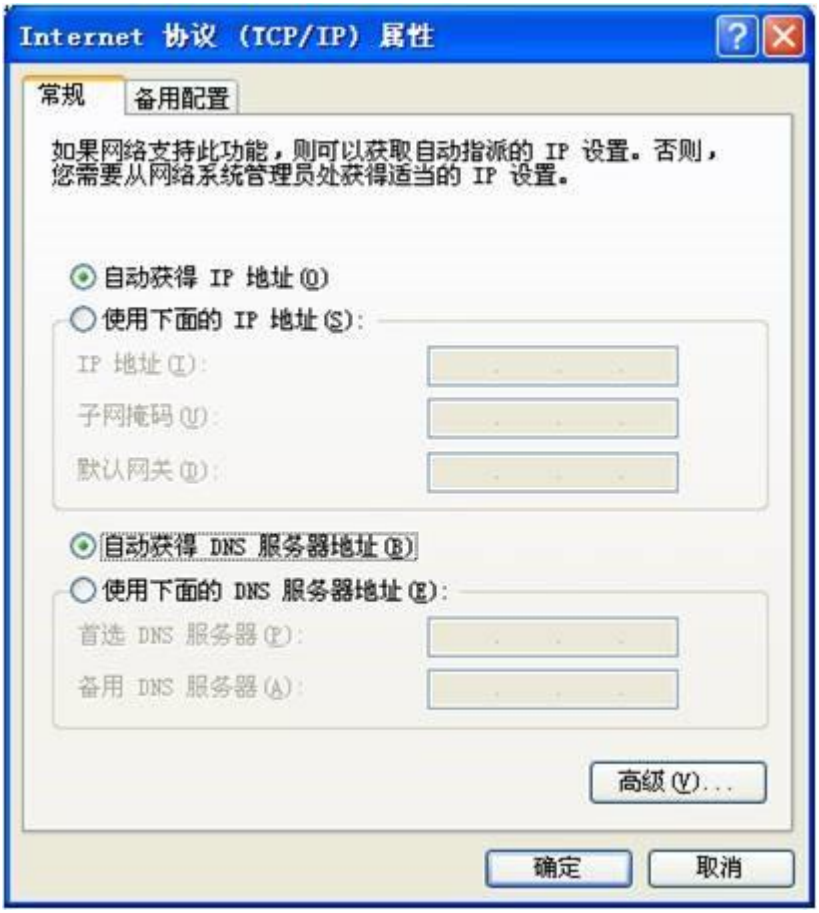
C.内部或者外部网络攻击　　D.校园网接入故障

【答案】C

【解析】本题考查网络故障分析的相关知识。

根据题目经测试无线路由器工作正常则说明无线路由器硬件无故障，而如果是配置错误则不会出现实验室用户使用一段时间后，不定期出现不能访问互联网的现象。另外 题目说同时有线接入的用户可以访问互联网，说明校园网接入服务正常。而如果有在该路由器受到实验室内部或者外部的网络攻击时则很有可能产生此现象。

校园网连接运营商的 IP 地址为 202.117.113.3/30，本地网关的地址为 192.168.1.254/24，如果本地计算机采用动态地址分配，在下图中应如何配置？（51）。



(51)A.选取“自动获得 IP 地址”

B.配置本地计算机的 IP 地址为 192.168.1.X

C.配置本地计算机的 IP 地址为 202.115.113.X

D.在网络 169.254.X.X 中选取一个不冲突的 IP 地址

【答案】A

【解析】

如果采用动态地址分配方案，本地计算机应设置为“自动获得 IP 地址”。

下面的选项中，不属于网络 202.113.100.0/21 的地址是（52）。

(52)A.202.113.102.0　　B.202.113.99.0　　C.202.113.97.0　　D.202.113.95.0

【答案】D

【解析】

网络地址 202.113.100.0/21 的二进制为：11001010 01110001 01100100 00000000

地址 202.113.102.0 的二进制为：11001010 01110001 01100110 00000000

地址 202.113.99.0 的二进制为：11001010 01110001 01100011 00000000

地址 202.113.97.0 的二进制为：11001010 01110001 01100001 00000000

地址 202.113.95.0 的二进制为：11001010 01110001 01011111 00000000

可以看出，地址 202.113.95.0 不属于网络 202.113.100.0/21。

IP 地址块 112.56.80.192/26 包含了（53）个主机地址，不属于这个网络的地址是（54）。

(53)A.15　　B.32　　C.62　　D.64

(54)A.112.56.80.202　　B.112.56.80.191

C.112.56.80.253　　D.112.56.80.195

【答案】C　B

【解析】

地址块 112.56.80.192/26 包含了 6 位主机地址，所以包含的主机地址为 62 个。

网络地址 112.56.80.192/26 的二进制为：01110000 00111000 01010000 11000000

地址 112.56.80.202 的二进制为：01110000 00111000 01010000 11001010

地址 112.56.80.191 的二进制为：01110000 00111000 01010000 10111111

地址 112.56.80.253 的二进制为：01110000 00111000 01010000 11111101

地址 112.56.80.195 的二进制为：01110000 00111000 01010000 11000011

可以看出，地址 112.56.80.191 不属于网络 112.56.80.192/26

下面的地址中属于单播地址的是（55）。

(55)A.125.221.191.255/18　　B.192.168.24.123/30

C.200.114.207.94/27　　D.224.0.0.23/16

【答案】C

【解析】

地址 125.221.191.255/18 的二进制为：01111101111001101 10111111 11111111

地址 192.168.24.123/30 的二进制为：11000000 10101000 00011000 01111011

地址 200.114.207.94/27 的二进制为：11001000 00111000 01110010 11011110

地址 224.0.0.23/16 二进制为：11100000 00000000 00000000 00010111

可以看出 125.221.191.255/18 和 192.168.24.123/30 都是广播地址，而 224.0.0.23/16 是组播地址，只有 200.114.207.94/27 是单播地址。

IPv6 地址的格式前缀用于表达地址类型或子网地址，例如 60 位地址 12AB00000000CD3 有多种合法的表示形式，下面的选项中，不合法的是（56）。

(56)A. 12AB:0000:0000:CD30:0000:0000:0000:0000/60

B. 12AB::CD30:0:0:0:0/60

C. 12AB:0:0:CD3/60

D. 12AB:0:0:CD30::/60

【答案】C

【解析】

IPv6 地址的格式前缀（Format Prefix, FP)用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可表示为“IPv6 地址/前缀长度”的形式。例如 60 位的地址前缀 12AB00000000CD3 有下列儿种合法的表示形式：

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

下面的表示形式是不合法的：

12AB:0:0:CD3/60 (在 16 比特的字段中可以省掉前面的 0,但不能省掉后面的 0)

12AB::CD30/60 (这种表示可展开为 12AB:0000:0000:0000:0000:0000:0000:CD30)

12AB::CD3/60 (这种表示可展开为 12AB:0000:0000:0000:0000:0000:0000:0CD3)

IPv6 新增加了一种任意播地址，这种地址（57）。

(57)A. 可以用作源地址，也可以用作目标地址

B. 只可以作为源地址，不能作为目标地址

C. 代表一组接口的标识符

D. 可以用作路由器或主机的地址

【答案】C

【解析】

任意播（AnyCast)地址是一组接口（可属于不同结点的）的标识符。发往任意播地址的分组被送给该地址标识的接口之一，通常是路由距离最近的接口。对 IPv6 任意播地址存在下列限制：

•任意播地址不能用作源地址，而只能作为目标地址；

•任意播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。

所谓移动 IP 是指（58）；实现移动 IP 的关键技术是（59）。

(58)A.通过地址翻译技术改变主机的 IP 地址

B.一个主机的 IP 地址可以转移给另一个主机

C.移动主机通过在无线通信网中漫游来保持网络连接

D.移动主机在离开家乡网络的远程站点可以联网工作

(59)A.移动主机具有一个可以接入任何网络的通用 IP 地址

B.移动主机具有一个家乡网络地址并获取一个外地转交地址

C.移动主机通过控制全网的管理中心申请网络接入服务

D.移动主机总是通过家乡网络地址来获取接入服务

【答案】D　B

【解析】

通常在联网的计算机中，有一类主机用铜缆或光纤连接在局域网中，从来不会移动，我们认为这些主机是静止的。可以移动的主机有两类，一类基本上是静止的，只是有时 候从一个地点移动到另一个地点，并且在任何地点都可以通过有线或无线连接进入 Internet；另一类是在运动中进行计算的主机，它通过在无线通信网中漫游来保持网络连 接。为解决前一类偶尔移动的主机异地联网的问题，IETF 成立了专门的工作组，并预设了下列研究目标：

•移动主机能够在任何地方使用它的家乡地址进行连网；

•不允许改变主机中的软件：

•不允许改变路由器软件和路由表的结构；

•发送给移动主机的大部分分组不需要重新路由；

•移动主机在家乡网络中的上网活动无须增加任何开销。

IETF 给出的解决方案是 RFC 3344 (IP Mobility Support for IPv4)和 RFC 3775 (Mobility Support in IPv6)。RFC 3344 增强了 IPv4 协议，使其能够把 IP 数据报路由到移动主机当前所在的连接站点。按照这个方案，每个移动主机配置了一个家乡地址（home address)作为永久标识。当移动主机离开家乡网络时，通过所在地点的外地代理，它被 赋予了一个转交地址（care-of address)。协议提供了一种注册机制，使得移动主机可以通过家乡地址获

得转交地址。家乡代理通过安全隧道可以把分组转发给外地代理，然后被提交给移动主机。

中国自主研发的3G通信标准是（60）。

(60)A.CDMA 2000　　B.TD-SCDMA　　C.WCDMA　　D.WiMAX

【答案】B

【解析】

1985年，ITU提出了对第三代移动通信标准的需求，1996年正式命名为IMT-2000(International Mobile Telecommunications-2000),其中的2000有3层含义：

•使用的频段在2000MHz附近

•通信速率于约为2000kb/s（即2Mb/s)

•预期在2000年推广商用，1999年ITU批准了五个IMT-2000的无线电接口，这五个标准是：

> IMT-DS(Direct Spread)：即W-CDMA，属于频分双工模式，在日本和欧洲制定的UMTS系统中使用。

> IMT-MC(Multi-Carrier)：即CDMA-2000,属于频分双工模式，是第二代CDMA系统的继承者。

> IMT-TC(Time-Code)：这一标准是中国提出的TD-SCDMA,属于时分双工模式。

> IMT-SC(Single Carrier)：也称为EDGE，是一种2.75G技术。

> lMT-FT(Frequency Time)：也称为DECT。

2007年10月19日，ITU会议批准移动WiMAX作为第6个3G标准，称为IMT-2000 OFDMATDD WMAN,即无线城域网技术。

第三代数字蜂窝通信系统提供第二代蜂窝通信系统提供的所有业务类型，并支持移动多媒体业务。在高速车辆行驶时支持144kb/s的数据速率，步行和慢速移动环境下支持384kb/s的数据速率，室内静止环境下支持2Mb/s的高速数据传输，并保证可靠的服务质量。

IEEE802.11规定了多种WLAN通信标准，其中（61）与其他标准采用的频段不同，因而不能兼容。

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

【答案】A

【解析】

1990年，IEEE802.11小组正式从事制定WLAN的物理层和MAC层标准的工作。1997 年

颁布的IEEE802.11标准运行在2.4GHz 的ISM (Industrial Scientific and Medical) 频段，采用扩频通信技术，支持IMb/s和2Mb/s数据速率。1998年推出的IEEE802.11b 标准也是运行在ISM频段，采用CCK (Complementary Code Keying)调制技术，支持 llMb/s 的数据速率。1999 年推出的lEEE802.11a 标准运行在U-NII (Unlicensed National Information Infrastructure)频段，采用OFDM调制技术，支持最高达54Mb/s的数据速率，但是与IEEE802.11b/g不兼容。2003年推出的IEEE802.11g标准运行在ISM频段，与IEEE802.11b兼容，数据速率提高到54Mb/s。早期的WLAN标准主要有4种，如下表所示。

IEEE 802.11 标准

名 称	发布时间	工 作 频 段	调制技术	数 据 速 率
802.11	1997 年	2.4GHz ISM 频段	DB/SK DQPSK	1Mb/s 2Mb/s
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mb/s，11Mb/s
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mb/s
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mb/s

2009年9月11日IEEE 802.1 In标准的正式发布。802.1 In可以将WLAN的传输速率由目前802.11a/802.11g的54Mb/s提高到300Mb/s，甚至600Mb/s。这个成就主要得益于MIMO与OFDM技术的结合。应用先进的无线通信技术，不但提高了传输速率，也极大地提升了传输质量。

IEEE802.11定义的AdHoc网络是由无线移动结点组成的对等网,这种网络的特点是(62)，在这种网络中使用的DSDV(Destination-sequenced Distance Vector)路由协议是一种(63)。

(62)A.每个结点既是主机，又是交换机

B.每个结点既是主机，又是路由器

C.每个结点都必须通过中心结点才能互相通信

D.每个结点都发送IP广播包来与其他结点通信

(63)A.洪泛式路由协议　　B.随机式路由协议

C.链路状态路由协议　　D.距离矢量路由协议

【答案】B　D

【解析】

IEEE 802.11标准定义的Ad Hoc网络是由无线移动结点组成的对等网，无须网络基础设施的支持，能够根据通信环境的变化实现动态重构，提供基于多跳无线连接的分组 数据

传输服务。在这种网络中，每一个结点既是主机，又是路由器，它们之间相互转发分组，形成一种自组织的MANET (Mobile Ad Hoc Network)网络。

路由算法是MANET网络中重要的组成部分,传统有线网络的路由协议不能直接应用于MANET。目标排序的距离矢域协议（Destination-Sequenced Distance Vector, DSDV）是一种扁平式路由协议。这是由传统的Bellman-Ford算法改进的距离矢量协议，利用序列号机制解决了路由环路问题，对后来的协议设计有很大影响。

OSPF协议将其管理的网络划分为不同类型的若干区域（Area），其中标准区域特点是（64）；存根区域（stub）的特点是（65）。

(64)A.不接受本地AS之外的路由信息，也不接受其他区域的路由汇总信息

B.不接受本地AS之外的路由信息，对本地AS之外的目标采用默认路由

C.可以接收任何链路更新信息和路由汇总信息

D.可以学习其他AS的路由信息，对本地AS中的其他区域采用默认路由

(65)A.不接受本地AS之外的路由信息，也不接受其他区域的路由汇总信息

B.不接受本地AS之外的路由信息，对本地AS之外的目标采用默认路由

C.可以接收任何链路更新信息和路由汇总信息

D.可以学习其他AS的路由信息，对本地AS中的其他区域使用默认路由

【答案】C　B

【解析】

为了适应大型网络配置的需要，OSPF协议引入了“分层路由”的概念。如果网络规模很大，则路由器要学习的路由信息很多，对网络资源的消耗很大，所以典型的链路状态协议都把网络划分成较小的区域（Area)，从而限制了路由信息传播的范围。每个区域就如同一个独立的网络，区域内的路由器只保存该区域的链路状态信息，使得路由器的链路状态数据库可以保持合理的大小，路由计算的时间和报文数量都不会太大。OSPF的区域分为以下5种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同:

•标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。

•主千区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。

•存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由0.0.0.0。

•完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。

•不完全存根区域（NSAA):类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

NAT 技术解决了 IPv4 地址短缺的问题,假设内网的地址数是 m,而外网地址数 n,若 m>n，则这种技术叫做（66），若 m>n，且 n=1，则这种技术这叫做（67）。

(66)A.动态地址翻译　　B.静态地址翻译　　C.地址伪装　　D.地址变换

(67)A.动态地址翻译　　B.静态地址翻译　　C.地址伪装　　D.地址变换

【答案】A　C

【解析】

NAT 技术主要解决 IP 地址短缺问题，最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部和外部地址的转换。局部地址 是在子网内部独立编址的,可以与外部地址重叠。后来根据这种技术又开发出两种最主要的应用。第一种应用是动态地址翻译（Dynamic Address Translation)。假定：

• m：需要翻译的内部地址数。

• n：可用的全局地址数（NAT 地址）。

当 m:n 翻译满足条件（m≥1 and m≥n)时，可以把一个大的地址空间映像到一个小的地址空间。所有 NAT 地址放在一个缓冲区中，并在存根域的边界路由器中建立一个局部地址和全局地址的动态映像表。这种 NAT 地址重用有如下特点：只要缓冲区中存在尚未使用的全局地址，任何从内向外的连接请求都可以得到响应，并且在边界路由器的 动态 NAT 表为之建立一个映像表项;如果内部主机的映像存在，就可以利用它建立连接；从外部访问内部主机是有条件的，即动态 NAT 表中必须存在该主机的映像。

另外一种特殊的 NAT 应用是 m:1 翻译，这种技术也叫做伪装（masquemding)，因为用一个路由器的 IP 地址可以把子网中所有主机的 IP 地址都隐蔽起来。如果子网中有多个主机同时都要通信，那么还要对端口号进行翻译，所以这种技术更经常被称为网络地址和端口翻译(Network Address Port Translation, NAPT)。在很多 NAPT 实现中专门保留一部分端口号给伪装使用，叫做伪装端口号。这种方法有如下特点。

①出口分组的源地址被路由器的外部 IP 地址所代替，出口分组的源端口号被一个未使用的

伪装端口号所代替。

②如果进来的分组的目标地址是本地路由器的 IP 地址，而目标端口号是路由器的伪装端口号，则 NAT 路由器就检查该分组是否为当前的一个伪装会话，并试图通过伪装表对 IP 地址和端口号进行翻译。

伪装技术可以作为一种安全手段使用，借以限制外部网络对内部主机的访问。另外，还可以用这种技术实现虚拟主机和虚拟路由，以便达到负载均衡和提高可靠性的目的。

CIDR 技术解决了路由缩放问题，例如 2048 个 C 类网络组成一个地址块，网络号从 192.24.0.0~192.31.255.0 这样的超网号应为（68），其地址掩码应为（69）。

(68)A.192.24.0.0　　B.192.31.255.0　　C.192.31.0.0　　D.192.24.255.0

(69)A.255.255.248.0　　B.255.255.255.0　　C.255.255.0.0　　D.255.248.0.0

【答案】A　　D

【解析】

2048 个 C 类网络 192.24.0.0～192.31.255.0 组成的超网号应为 192.24.0.0/13。

网络系统设计过程中，物理网络设计阶段的任务是（70）。

(70)A.依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B.分析现有网络和新网络的各类资源分布，掌握网络所处的状态

C.根据需求规范和通信规范，实施资源分配和安全规划

D.理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

【答案】A

【解析】

网络开发过程的五阶段迭代周期模型可以用下图来描述。

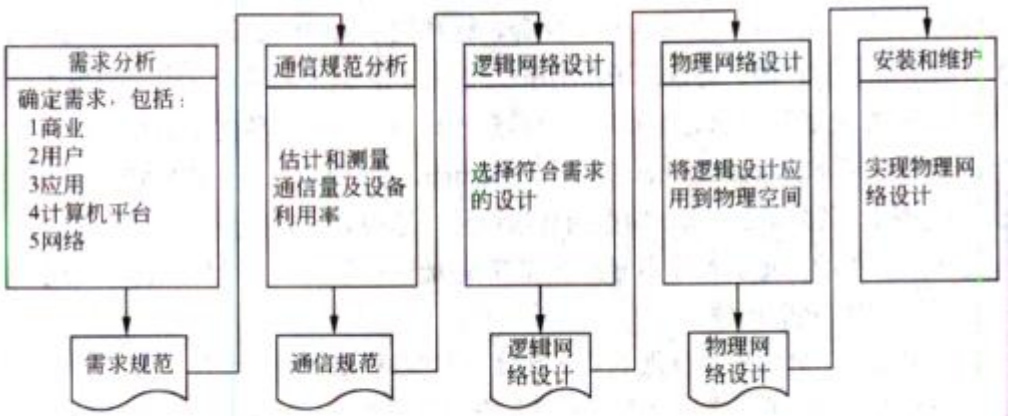


图　五阶段网络开发过程

①需求分析

需求分析是开发过程中最关键的阶段。通过和不同的用户（包括经理人员和网络管理员）交流，收集明确的需求信息。需求分析的输出是产生一份需求说明书，也就是需 求规范。

②现有网络系统的分析

如果当前的网络开发过程是对现有网络的升级和改造，就必须进行现有网络系统的分析工作。现有网络系统分析的目的是描述资源分布，以便于在升级时尽量保护已有的 投资。在这一阶段，应给出一份正式的通信规范说明文档，作为下一个阶段的输入。

③确定网络逻辑结构

网络逻辑结构设计是根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。这个阶段最后应该得到一份逻辑设计

文档。

④确定网络物理结构

物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确 定具体的软硬件、连接设备、布线和服务的部署方案。

⑤安装和维护

这个阶段是根据前面的工程成果实施环境准备、设备安装调试的过程。网络安装完成网络投入运行后，还需要做大量的故障监测和故障恢复，以及网络升级和性能优化等 维护工作。

The traditional way of allocating a single channel among multiple competing users is to chop up its (71) by using one of the multiplexing schemes such as FDM (Frequency Division Multiplexing). If there are N users, the bandwidth is divided

into N equal-sized portions, with each user being assigned one portion. Since each user has a private frequency (72), there is no interference among users.When there is only a small and constant number of users, each of which has a steady stream or a heavy load of (73), this division is a simple and efficient allocation mechanism. A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most of the time to broadcast its signal.However, when the number of senders is large and varying or the traffic is (74), FDM presents some problems. If the spectrum is cut up into N regions while fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. If more than N users want to communicate, some of them will be denied (75) for lack of bandwidth.……

(71)A.capability　B.capacity　C.ability　D.power

(72)A.band　B.range　C.domain　D.assignment

(73)A.traffic　B.date　C.bursty　D.flow

(74)A.continuous　B.steady　C.bursty　D.flow

(75)A.allowance　B.connection　C.percussion　D.permission

【答案】B　A　A　C　D

【解析】

在多个竞争的用户之间分配单一信道（例如电话干线）的传统方法就是通过一种多路方案（例如FDM)将其带宽分解开来。如果有N个用户，带宽就被分成N个相等的部分，每一个用户都得到了自己的一份。因为每个用户都有一个专用的频带，所以用户之间没有干扰。当仅有少量的、固定数量的用户，而且每个用户都有一个稳定的流量或者大量的通信负载时，这种划分才是简单而有效的分配机制。无线通信中的FM广播系统就是这样的例子。每一个广播台都得到一部分FM频带，并使用这个频带经常性地进行无线广播。然而，当发送者的数量是大景的、变化的、或者突发式通信时，FDM就会出问题。如果频谱被分成N个部分，而且划分的数最少于需要通信的用户数量时，一大片有价值的频谱就会被浪费。如果超过N个用户需要通信，某些用户就会因没有带宽而被拒绝进入连接，即使某些用户曾经被赋予频带，发送或接收过一些信息。

试题一（共 20 分）

阅读以下说明，回答问题 1 至问题 3,将解答填入答题纸对应的解答栏内。

【说明】

某单位计划部署园区网络，该单位总部设在 A 区，另有两个分别设在 B 区和 C 区，各个地区之间距离分布如图 1-1 所示。

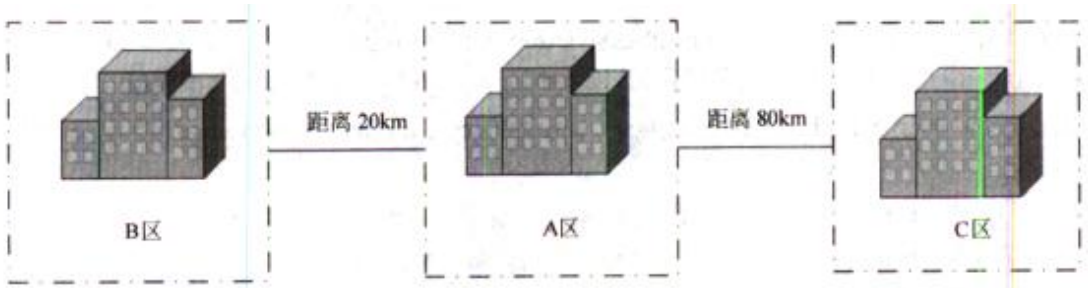


图 1-1

该单位的主要网络业务需求在 A 区，在网络中心及服务器机房亦部署在 A 区；B 的网络业务流量需求远大于 C 区；c 区的虽然业务流量小，但是网络可靠性要求高。根据业务需要，要求三个区的网络能够互通并且都能够访问互联网，同时基于安全考虑单位要求采用一套认证设备进行身份认证和上网行为管理。

【问题 1】

为了保障业务需求，该单位采用两家运营商接入 internet。根据题目需求，回答下列问题；

1. 两家运营商的 internet 接入线路应部署在哪个区？为什么？
2. 网络运营商提供的 mpls vpn 和千兆裸光纤两种互联方式，哪一种可靠性高？为什么？
3. 综合考虑网络需求及运营成本，在 AB 区之间与 AC 区之间分别采用上述那种方式进行互联？

【参考答案】

1. 部署在 A 区。网络业务主体在 A 区，采用一套认证和上网行为管理。
2. MPLSVPN 可靠性比较高，线路有冗余。
3. AB 区之间采用千兆裸光纤，AC 区之间采用 MPLS VPN。

【试题分析】

本题考查的是网络规划的基本知识。

本问题考查广域网接入及网络互联的问题。

1. 两家运营商的 Internet 接入线路应部署在 A 区。其主要原因有两点：首先，根据题目描述该单位的主要网络业务需求在 A 区，网络中心及服务器机房亦部署在 A 区，另外，该单位要求采用一套认证设备进行身份认证和上网行为管理，所以出口线路应集中在一个业务需求大的区域（A 区）。这时，由于三个区域是互通的，其他区域也可通过 A 区出口与互联网连接。

2. 网络运营商提供了 MPLS VPN 和千兆裸光纤两种互联方式。这两种互联方式中 MPLS VPN 的可靠性大于千兆裸光纤，这是由于当千兆裸光纤是物理链路，当其出现链路故障时，互联业务就会中断。MPL SVPN 属于逻辑链路。当单个物理链路出现故障时，只要其他链路可达，MPLS VPN 还可提供互联服务。

3. 综合考虑网络需求及运行成本，AB 区之间应采取千兆裸光纤互联模式，AC 区之间应采用 MPLS VPN 互联方式。

根据题目描述，B 区的网络业务流景需求远大于 C 区：C 区虽然业务量小，但是网络可靠性要求高。所以，AB 区之间采取千兆裸光纤以适应大业务量，AC 区之间采用 MPLS VPN 在业务量不大但安全性要求较高时是合理的。

【问题 2】

该单位网络部署接入点情况如表 1-1 所示

表 1-1

区　域	汇 聚 点	接 入 点	备　注
A	办公楼	124	所有区域采用三层局域网结构部署，其中 A 区采用双核心交换机冗余。所有汇聚点采用单模光纤上联至核心交换机。所有接入交换机采用双绞线上联至汇聚交换机
	资料室	86	
	网管中心	78	
	设计中心	200	
	生产区	115	
B	办公楼	106	
	培训中心	126	
	宿舍	198	
C	办公楼	86	
	营销中心	54	

根据网路部署需求，该单位采购了相应的网络设备，请根据题目说明及表所规定 1-2 所示的设备数量及合理的部署位置（注：不考虑双绞线的距离限制）。

表 1-2

设备类型	设备数量	部署区域
核心交换机	(1)	A 区
核心交换机	1	B 区
核心交换机	1	C 区
汇聚交换机	5	A 区
汇聚交换机	3	B 区
汇聚交换机	2	C 区
SFP 单模模块	5	(2) 区
SFP 单模模块	7	(3) 区
SFP 单模模块	22	(4) 区
24 口接入交换机	(5)	A 区
24 口接入交换机	(6)	B 区
24 口接入交换机	(7)	C 区
千兆服务器接入交换机	1	A 区
服务器	3	A 区
路由器	1	(8) 区
认证及流控设备	1	A 区
防火墙	1	A 区

【参考答案】

(1) 2 (2) C (3) B (4) A

(5) 28 (6) 20 (7) 7 (8) A

【试题分析】

本问题考查的是网络设备选型的基础知识。

1.根据题目描述可知，A 区采用双核心交换机冗余，所以 A 区核心交换机的数量为 2 台。

2. 根据题目描述可知，所有汇聚点采用单模光纤上联至核心交换机 SFP 单模模块。A、B、C 区的汇聚交换机分别有 5、3、2 台，其中 A 区是双核心交换机，故核心与汇聚相连需要 20 个 SFP 单模模块，另外 A 区需要和 B、C 区核心交换机互联，所以还需要 2 个 SFP 单模模块，共计 22 个。同样可以推算出 B 区需要 7 个 SFP 单模模块，C 区需要 5 个 SFP 单模模块。

3. A、B、C 区的接入点数参见表 1-1，不考虑双绞线的距离限制，只需要计算同一个楼内需要的 24 口接入交换机数量即可。根据计算可知，A 区需要 24 口接入交换机 28 个，B 区需要 24 口接入交换机 20 个，C 区需要 24 口接入交换机 7 个。

4. 由前述可知，Internet 接入线路部署在 A 区，所以路由器应部署在 A 区。

【问题 3】

根据题目要求，在图 1-2 的方框中画出该单位 A 区网络拓扑示意图（汇聚层以下不画）。

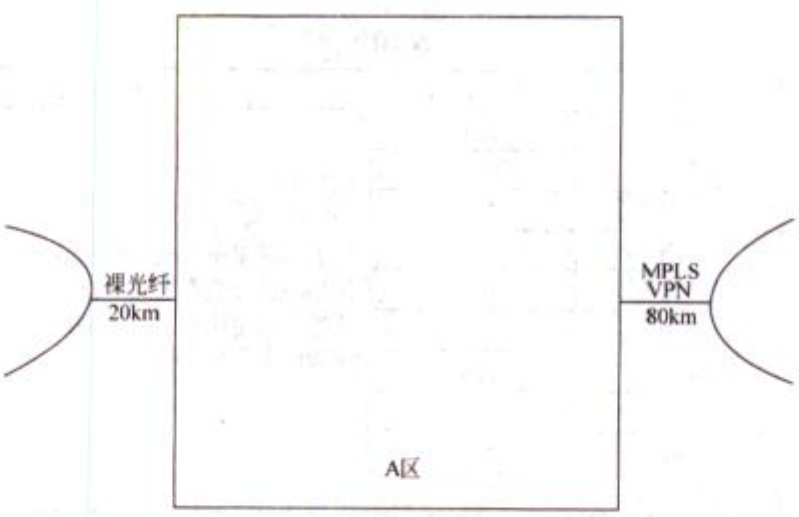
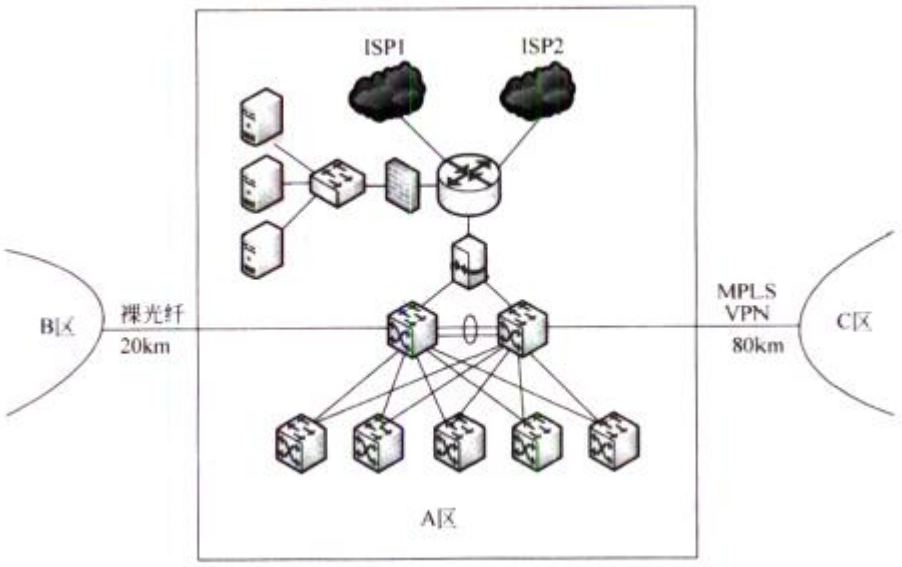


图 1-2

【参考答案】



【试题分析】

本问题考查的是网络拓扑的基础知识。根据题目的描述和设备配置表，注意 A 区双核心的链路冗余的情况，另外注意 B 区和 C 区与 A 区互联分别采用裸光纤和 MPLS VPN，所以网络拓扑结构图如上。

试题二（共 15 分）

阅读以下说明，回答问题 1 至问题 5,将解答填入答题纸对应的解荇栏内。

【说明】

某公司采用 winserver2003 操作系统搭建该公司的企业网站,要求用户在浏览器地址必须输入 https://www.gongsi.com/index,.html 或 https://117.112.89.67/index.html 来访问该公司的网站。其中，index.html 文件存放在网站服务器 E:\gsdata 目录中。在服务器上安装完成 iis6.0 后网站属性窗口[网站]，[主目录]选项卡分别如图 2-1

图2-1

图2-2

【问题 1】

1.按照题目说明。图 2-1 中的‘ip 地址’文本框中的内容为（1）：SSL 端口文本框内容为（2）

2.按图 2-2 中，本地路径文本框中的内容为（3）；同时要保障用户通过题目要求的方式来访问网址，必须至少勾选（4）复选框。

（4）备选答案

A,脚本资源访问　　B,读取　C,写入　D.目录浏览

【参考答案】

（1）117.112.89.67 或者 全部未分配

（2）443

（3）E：\gsdata

（4）B

【试题分析】

本题考查的是利用 Windows Server 2003 操作系统搭建安全的 Web 网站的相关知识。

本问题主要考查的是利用 IIS 搭建 web 站点的配置过程。

在图 2-1 可从“IP 地址”下拉框中指定一个 IP 地址或者输入用于访问该站点的 IP 地址。如果没有分配指定的 IP 地址，即选中“全部未分配”选项，那么此站点将响应分配给该服务器但没有分配给其他站点的所有 IP 地址，并使它成为默认网站的 IP 地址。“SSL 端口”文本框是可选项目，用于指派与该网站标识相关联的 SSL 端口。默认的 SSL 端口号是 443。只有使用 SSL 加密时才需要 SSL 端口号。题目要求用户在浏览器地址栏必须输入 https://www.gongsi.com/index.html 或 https://l 17.112.89.67/index.html 来访问该公司网站。所以在图 2-1 中的“IP 地址”文本框中的内容应为 117.112.89.67 或者全部未分配 1，“SSL 端口”文本框中的内容应为 443。

另外，根据题目要求 index.html 文件存放在网站所在服务器 E:\gsdata 目录中。所以在图 2-2 中所示的“主目录”选项卡中“本地路径”文本框中的内容应为“E:\gsdata”，以指明网站首页文档的物理存放路径。为保障用户对网站的访问，在图 2-2 中应该至少勾选“读取”复选框，并单击“确定”或者“应用”按钮。

【问题 2】

1.配置该网站时，要在如图 2-3 所示【目录安全性】选项卡中单击【服务器证书】来获取服务器证书，其中获取服务器证书的步骤顺序如下：①生产证书请求文件，②（5），③从 CA 导出证书文件④在 IIS 服务器上导入并安装证书。

配置完成后，当用户登陆该网站时，通过验证 CA 的签名来确认数字证书的有效性，从而（6）。CA 颁发给 web 网站的数字证书不包括（7）。

图 2-3

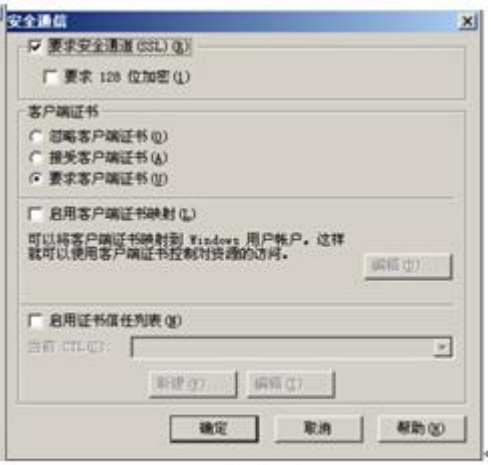


图 2-4

6-7 备选答案：

（6）A.验证网站的真伪 B.判断用户的权限，C.加密发完服务器的数据 D.解密所接受的客户端数据

（7）A.证书的有效期 B.网站的公钥 C.证书的序列号 D.网站的私钥

【参考答案】

（5）CA 颁发证书

（6）A

（7）D

【试题分析】

本问题主要考查的是配置安全的 Web 网站时的步骤。

为了配置安全的 Web 网站，获取并安装服务器证书的步骤依次为：①从“管理工具”中进入“Internet 服务管理器”，右击需要配置的站点，在弹出的快捷菜单中选择“域性”命令，接着单击“目录安全性”选项卡中的“安全通信”组件框中“服务器证书”按钮，通过 IIS 证书向导生成证书请求文件。②向证书颁发机构（CA)提交证书请求文件，证书颁发机构颁发相应的证书。③在申请证书的计算机浏览器上输入 http://根 CA 的 IP/certsrv，进入证书申请页面。单击“检查挂起的证书”链接，选择已经提交的证书申请。如果颁发机构已将证书颁发，则可单击“安装此证书”按钮，即从证书颁发机构导出证书文件。④在“目录安全性”选项卡中再次单击“安全通信”组件框中的“服务器证书”按钮。在 IIS 证书向导中进入“挂起的证书清求”页面，选择“处理挂起的 请求，并安装证书”单选按钮，接着选择刚才导出的 CER 文件。完成在 IIS 服务器上导入并安装证书。⑤在“目录安全性”选项卡中单击“安全通信”组件框中的“编辑”按钮，打开“安全通信”对话框。在该对话框中可根据所需要的安全要求配置相应的身份验证方式和 SSL 安全通道。

综上所述，为配置安全的 Web 网站，获取并安装服务器证书的步骤顺序如下：①生成证书请求文件；②CA 颁发证书：③从 CA 导出证书文件；④在 IIS 服务器上导入并安装证书。

数字证书能够验证一个实体身份，而这是在保证数字证书本身有效性的前提下才能够实现的。验证数字证书的有效性是通过验证 CA 的签名实现的。某网站向 CA 申请了数字证书，当用户登录该网站时通过验证 CA 对其的签名来确认该数字证书的有效性，从而验证该网站的真伪。CA 颁发给网站的数字证书包含多项内容（如证书的版本号、 序列号、网站的公钥、CA 的签

名、证书的有效期等)，但是不包括网站的私钥。

【问题 3】

配置该网站时，在图 2-3 的窗口中单击【安全通信】栏目中的【编辑】按钮，弹出如图 2-4 所示窗口，按题目要求。客户端浏览器只能通过 https 方式访问服务器，此时应勾选图 2-4 中的（8）框，如果要求客户端和服务器进行双向认证，此时应勾选图 2-4 的（9）框。

【参考答案】

（8）要求安全通信（SSL）

（9）要求客户端证书

【试题分析】

本问题主要考查配置安全的 Web 网站的过程。

配置安全的 Web 站点时，在图 2-3 中的“目录安全性”选项卡中单击“安全通信”组件框中的“编辑”按钮，系统将打开图 2-4 中“安全通信”对话框。如果要求客户只能通过使用 HTTPS 服务访问该网站，则应该选中“要求安全通道（SSL）”复选框。

在“客户端证书”下，选择以下某一选项以启用客户端证书验证：接受客户端证书，用户可以使用客户端证书访问资源，但证书并不必需。若要求客户端证书，则服务器在将用户与资源连接之前要请求客户端证书，将拒绝没有有效客户端证书的用户的访问。若忽略客户端证书，无论用户是否拥有证书，都将被授予访问权限。如果要求客户端和服务器进行双向认证，则应该选中“要求客户端证书”复选框。

【问题 4】

HTTPS 用于在客户计算机和服务器之间提供安全通信，广泛用于因特网上安全敏感的应用，例如（10）应用。

HTTPS 使用安全套接字层(SSL)进行信息交换。SSL 目前版本是 3.0，被 IETFf 定义在 RFC6101 中。IETF 对 SSL 进行升级后的继任者是（11）。

（10）备选答案如下：

A.网络聊天　　B.网络视频　　C.网上交易　　D.网络下载

【参考答案】

（10）C

（11）TLS 或 Transport Layer

【试题分析】

本问题主要考查的是 HTTPS 的基本知识。

Https 是基于安全目的的 Http 通道，其安全基础由 SSL 层来保证。最初由 netscape 公司研发，主要提供了通讯双方的身份认证和加密通信方法。现在广泛应用于互联网上对安全敏感的通讯，如网上交易、在线支付等。

安全套接层(Secure Sockets Layer，SSL)，一种安全协议，是网景公司(Netscape) 在推出 Web 浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL 在传输层对网络连接进行加密。

SSL 采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信小被攻击者窃听。它在服务器和客户机两端可同时被支持，目前已成为互联网上保密通讯的工业标准。现行 Web 浏览器亦普遍将 HTTP 和 SSL 相结合，从而实现安全通信。此协议的继任者是 TLS。

IETF (www.ietf.org)将 SSL 作了标准化，即 RFC2246,并将其称为 TLS (Transport Layer Security),其最新版本是 RFC5246,版本 1.2。从技术上讲，TLS1.0 与 SSL3.0 的差异非常微小。TLS 利用密钥算法在互联网上提供端点身份认证与通讯保密，其基础是公钥基础设施（public key infrastructure，PKI)。

【问题 5】

使用 https 能不能确保服务器自身安全？

【参考答案】

不能

【试题分析】

Https 的限制主要是它的安全保护依赖浏览器的正确实现以及服务器软件、实际加密算法的支持。这里面一种常见的误解是“银行用户在线使用 https:就能充分彻底保障他们的银行卡号不被偷窃。”实际上，与服务器的加密连接中能保护银行卡号的部分，只有用户到服务器之间的连接及服务器自身。并不能绝对确保服务器自己是安全的，这点甚至已被攻击者利用，常见例子是模仿银行域名的钓鱼攻击。少数罕见攻击在网站传输客户数据时发生，攻击

者尝试窃听数据于传输中。商业网站被人们期望迅速尽早引入新的特殊处理程序到金融网关，仅保留传输码（transaction number)。不过他们常常存储银行卡号在同一个数据库里。那些数据库和服务器少数情况有可能被未授权用户攻击和损害。因此使用 HTTPS 不能确保服务器自身的安全。

试题三（共 20 分）

阅读以下说明，回答问题 1 至问题 4,将解答填入答题纸对应的解答栏内。

【说明】

某单位网络拓扑结构如图 3-1 所示，在 linux 系统下构建 DNS 服务器，在 DHCP 服务器和 web 服务器。要求如下。

1. 路由器连接各个子网的接口信息如下：

（1） 路由器 e0 的 ip 地址 192.168.1.1/25

（2） 路由器 e1 的 ip 地址 192.168.1.129/25

（3） 路由器 e2 的 ip 地址 192.168.2.1/25

（4） 路由器 e3 的 ip 地址 192.168.2.33/25

2.子网 1 和子网 2 内的客户机通过 DHCP 服务器动态分配 ip 地址：

3.服务器设置固定的 IP 地址，其中

（1）DNS 服务器采用 bind 构建，IP 地址为 192.168.2.2

（2）DHCP 服务器 IP 地址为 192.168.2.3

（3）web 服务器网卡 eth0 的 IP 地址为 192.168.2.4,eth1 的 IP 地址为 192.168.2.34

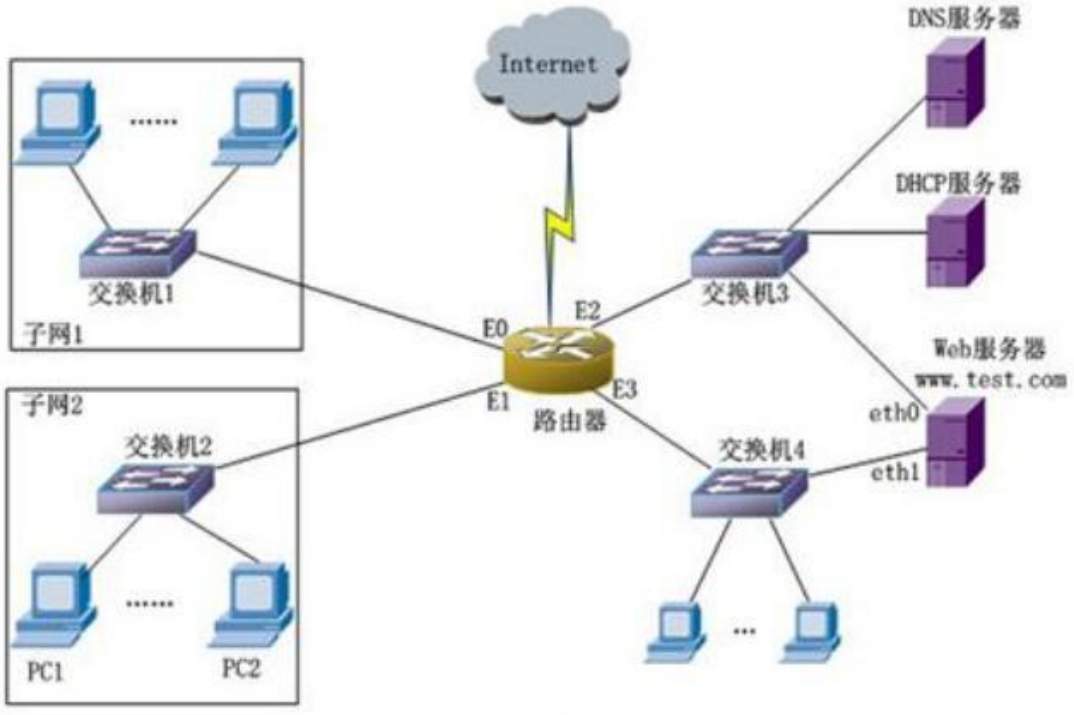


图 3-1

【问题 1】

请完成图 3-1 中 web 服务器 eth1 的配置。

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:24:F8:9B
NETMASK=__(1)__
IPADDR=__(2)__
GATEWAY=__(3)__
TYPE=Ethernet
NAME="System eth1"
IPV6INIT=no
```

【参考答案】

(1) 255.255.255.248

(2)192.168.2.34

(3)192.168.2.33

【试题分析】

本题考查网络地址子网掩码计算、Linux 系统下网络配置、DNS 服务配置和 DHCP 服务配置方面的知识。

本问题考查网络地址规划和 Linux 系统下网卡网络配置的基本知识。

2 种表示方式的子网掩码换算，29 位的子网掩码换算后为 255.255.255.248。

Linux 系统下网络配置参数中 NETMASK 代表子网掩码，IPADDR 代表 IP 地址，GATEWAY 代表子网网关地址。

【问题 2】

请完成图 3-1 中 DNS 服务器网卡的配置。

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:21:A1:78
NETMASK=__(4)__
IPADDR=__(5)__
GATEWAY=__(6)__
TYPE=Ethernet
NAME="System eth0"
IPV6INIT=no
```

【参考答案】

(4) 255.255.255.248

(5) 192.168.2.2

(6)192.168.2.1

【试题分析】

本问题考查网络地址规划和 Linux 系统下网卡网络配置的基本知识和两种表示方式的子网掩码换算。

Linux 系统下网络配置参数中 NETMASK 代表子网掩码，IPADDR 代表 IP 地址，GATEWAY 代表子网网关地址。

【问题 3】

在（7）（8）（9）处填写恰当的内容。

在 Linux 系统中设置域名解析服务器，已知域名服务器上文件 named.conf 的部分内容如下：

test.com.zone.A 文件的部分配置如下: WWW IN A 192.168.2.4

test.com.zone.B 文件的部分配置如下:WWW IN A 192.168.2.34

IP 地址(7)不允许使用该 DNS 进行递归查询,子网 1 和子网 2 中的客户端访问 www.test.com 时，该 DNS 解析返回的 IP 地址分别为（8）和（9）。

(7) 备选答案：

A. 192.168.1.8 B.192.168.1.133

C. 192.168.2.10 D.192.168.2.6

(8) 和 (9)备选答案：

A. 192.168.2.4 B.192.168.2.34

C. 192.168.2.4 或者 192.168.2.34 D.192.168.2.3 和 192.168.2.34

【参考答案】

(7) C

(8) A

(9) B

【试题分析】

本问题考查 Linux 系统下基于 BIND 的 DNS 服务配置。

通过 allow-recursion{A;B;C;D}命令，可以看出 acl A、B、C、D 允许递归查询，选项 A、B、D 对应的 IP 地址分别在定义的 acl A、B、C 子网中，选项 C 对应的 IP 地址不在 acl A、B、C、D 任何子网中，故选 C。

客户端访问 www.test.com 时，子网 1 的客户端对应 acl A,会访问 view A 中的域名配置文件 test.com.zone.A，故解析出的 IP 地址为 192.168.2.4;子网 2 的客户端不在 acl A 中，则会访问 view B 中的域名配置文件 test.com.zone.B，故解析出的 IP 地址为 192.168.2.34。

【问题 4】

DHCP 服务器配置文件如下所示：

```
authoritative;
ddns-updates off;
max-lease-time 604800;
default-lease-time 604800;
allow unknown-clients;
option domain-name-servers 192.168.2.2
ddns-update-style none;
allow client-updates;
subnet 192.168.2.32 netmask 255.255.255.248 {
    option routers 192.168.2.33;
    range 192.168.2.35 192.168.2.38;
}
```

根据这个文件内容。该 DHCP 服务器默认租期是（10）天，DHCP 客户机能获得 IP 地址范围是从（11）到（12），获得 DNS 服务器 IP 地址为（13）。

【参考答案】

(10) 7

(11) 192.168.2.35

(12) 192.168.2.38

(13) 192.168.2.2

【试题分析】

本问题考查 Linux 系统下 DHCP 服务配置的基础知识。

配置文件中 default-lease-time 604800 代表 DHCP 服务器设置的默认租期为 604800 秒，转换成天数应为 7 天。

配置文件中 option routers 192.168.2.33 代表 DHCP 客户机的子网网关地址，range 192.168.2.35 192.168.2.38 代表 DHCP 客户机能获得的 IP 地址范围。

配置文件中 option domain-name-servers 192.168.2.2 代表 DNS 服务器 IP 地址为 192.168.2.2。

试题四（共 20 分）

阅读以下说明，回答问题 1 至问题 4,将解答填入答题纸对应的解答栏内。

【说明】

某企业总部设立在 A 地，在 B 地有分支机构，分支机构和总部需要在网络上进行频繁的数据传输，该企业采用 IPSec VPN 虚拟专用技术实现分支机构和总部之间安全，快捷，经济的跨区域网络连接。

该企业网络拓扑结构如图 4-1 所示：

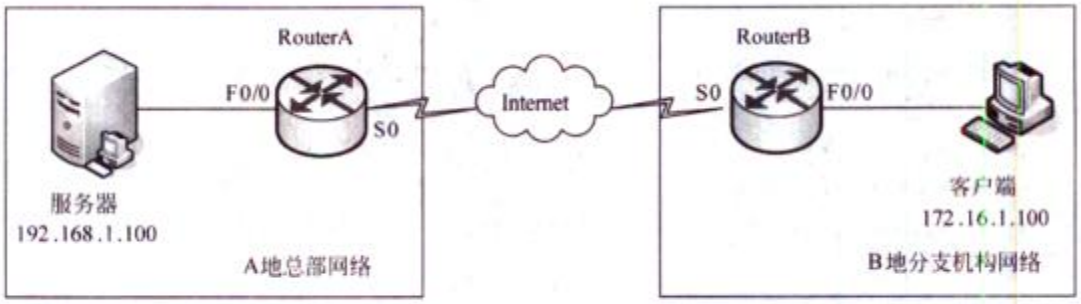


图 4-1

该企业网络地址规划与配置如表 4-1 所示。

表 4-1 网络规划地址配置表

设　备	IP 地址	设　备	IP 地址
RouterA	F0/0:192.168.1.1/24 S0:202.102.100.1/30	RouterB	F0/0:172.16.1.1/24 S0:202.102.100.2/30
总部服务器	192.168.1.100/24	分支机构客户端	172.16.1.100/24

【问题 1】

为了完成对 routerA 和 routerB 远程连接管理，以 routerA 为例，完成初始化路由器，并配置 routerA 的远程管理地址（192.168.1.20），同时开启 routerA 的 telent 功能并设置全局模式访问密码，请补充下列配置命令。

```
RouterA >enable
RouterA#configure terminal
RouterA(config)#interface  f0/0          //进入 F0/0 的___(1)___子模式
RouterA(config-if)#ip addr ___(2)___     //为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut//__(3)__F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter ___(4)___       //进入 loopback 0 的接口配置子模式
RouterA(config-if)#ip addr ___(5)___     //为 loopback 0 接口配置 IP 地址
……
RouterA(config)#____(6)_____             //进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001 //配置 vty 口令为"abc001"
RouterA(config)#enable password abc001//配置全局配置模式的明文密码为"abc001"
RouterA(config)# enable__(7)__ abc001//配置全局配置模式的密文密码为"abc001"
……
```

【参考答案】

(1) 接口配置

(2) 192.168.1.1 255.255.255.0

(3) 开启

(4) loopback 0

(5) 192.168.1.20 255.255.255.255

(6) line vty 0 4

(7) secret

【试题分析】

本题考查企业网 IPSec VPN 相关的配置知识。

本问题考查路由器的基本配置命令，主要完成对路由器的基础配置，如地址、加密等。

```
RouterA >enable
RouterA#configure terminal
RouterA(config)#interface  f0/0
//进入 F0/0 的接口配置子模式
RouterA(config-if)#ip addr 192.168.1.1  255.255.255.0
//为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut
//开启 F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter loopback 0
//进入 loopback 0 的接口配置子模式
RouterA(config-if)#ip addr 192.168.1.20 255.255.255.255
// 为 loopback 0 接口配置 IP 地址
……
RouterA(config)# line vty 0 4
// 进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001
// 配置 vty 口令为"abc001"
RouterA(config)#enable password abc001
// 配置全局配置模式的明文密码为"abc001"
RouterA(config)# enable secret abc001
// 配置全局配置模式的密文密码为"abc001"
```

【问题 2】

VPN 是建立在两个局域网出口之间的隧道连接，所以两个 VPN 设备必须能够满足内网访问互联网的要求，以及需要配置 NAT。按照题目要求以 RouterA 为例，请补充完成下列配置命令。

```
RouterA(config)#access-list101 (8) ip192.168.1.00.0.0.255172.16.1.0
0.0.0.255
RouterA(config)# access-list 101 (9) ip 192.168.1.0 0.0.0.255 any
//定义需要被 NAT 的数据流
RouterA(config)#ip nat inside source list 101 interface (10) overload
//定义 NAT 转换关系
RouterA(config)#int (11)
RouterA(config-if)#ip nat inside
RouterA(config)#int (12)
RouterA(config-if)#ip nat outside    //定义 NAT 的内部和外部接口
……
```

【参考答案】

(8) deny

(9) permit

(10) s0 或者 serial 0

(11) f0/0 或者 fastethemet 0/0

(12) s0 或者 serial 0

【试题分析】

本问题考查路由器配置 NAT 转换的相关命令操作。

```
RouterA(config)# access-list 101 deny ip 192.168.1.0 0.0.0.255 172.16.1.0
0.0.0.255
RouterA(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 any
//定义需要被 NAT 的数据流（即除去通过 VPN 要传输的数据流）
RouterA(config)#ip nat inside source list 101 interface s0 overload
//定义 NAT 转换关系
RouterA(config)#int  f0/0
RouterA(config-if)#ip nat inside
RouterA(config)#int s0
RouterA(config-if)#ip nat outside
//在路由器上定义 NAT 的内部和外部接口
…
```

【问题 3】

配置 IPSec VPN 时要注意隧道两端的设备配置参数必须对应匹配，否则 VPN 配置将会失败。以 RouterB 为例配置 IPSec VPN，请完成相关配置命令。

```
RouterB(config)# access-list 102 permit ip __(13)__ //定义需要通过 VPN 加
密传输的数据流
RouterB(config)#crypto isakmp __(14)__    //启用 ISAKMP(IKE)
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#group 2
RouterB(config)#crypto isakmp identity address
RouterB(config)#crypto isakmp key abc001 address __(15)__ //指定共享密
钥和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
RouterB(cfg-crypto-trans)#model tunnel
RouterB(config)#crypto map abc001 10 ipsec-isakmp
……
RouterB(config)#int  __(16)__
RouterB(config-if)#crypto map abc001 //在外部接口上应用加密图
……
```

【参考答案】

(13) 172.16.1.0　　0.0.0.255　　192.168.1.0　　0.0.0.255

(14) enable

(15) 202.102.100.1

(16) s0 或者 serial 0

【试题分析】

本问题考查配置 IPSec VPN 的具体过程。

```
RouterB(config)#  access-list  102  permit  ip  172.16.1.0    0.0.0.255
192.168.1.0 0.0.0.255
//定义感兴趣的数据流，即需要通过 VPN 加密传输的数据流
RouterB(config)#crypto isakmp enable
//启用 ISAKMP(IKE) 策略
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
//认证方法使用预共享密钥
RouterB(config-isakmp)#encryption des
//加密方法使用 des
RouterB(config-isakmp)#hash md5
//散列算法使用 md5
RouterB(config-isakmp)#group 2
//DH 模长度为 1024
RouterB(config)#crypto isakmp identity address
RouterB(config)#crypto isakmp key abc001 address 202.102.100.1
//将 ISAKMP 预共享密钥和对等体关联，指定共享密钥和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
RouterB(cfg-crypto-trans)#model tunnel
//设置 IPsec 转换集
RouterB(config)#crypto map abc001 10 ipsec-isakmp
……
RouterB(config)#int  s0
RouterB(config-if)#crypto map abc001
//在外部接口上应用加密图
……
```

【问题 4】

根据题目要求，企业分支机构与总部之间采用 IPSec VPN 技术互连，IPSec (IP Security)是 IETF 为保证在 Internet 上传送数据的安全保密性而制定的框架协议，该协议应用在 （17）层，用于保证和认证用户 IP 数据包。

IPSec VPN 可使用的模式有两种，其中（18）模式的安全性较强，(19)模式的安全性较弱。IPSec 主要由 AH、ESP 和 IKE 组成，在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由（20）进行定义。

【参考答案】

(17) 网络层

(18) 隧道

(19) 传输

(20) SA 或者安全关联

【试题分析】

本问题考查 IPSec VPN 的基础知识。

IPSec (IP Security)是 IETF 为保证在 Internet 上传送数据的安全保密性而制定的框架协议，该协议应用在网络层，用于保证和认证用户 IP 数据包。IPSec 本身是开放的框架式协议，包含的各种算法之间是相互独立的，而且可以确保信息的机密性、数据的完整性、用户的验证和防重发保护，所以在架设 VPN 时通常会使用 IPSec 协议来提供数据
安全。

IPSecVPN 可使用的模式有两种，隧道模式和传输模式。使用隧道模式，IPSec 对整个 IP 数据包进行封装和加密，隐蔽了源和目的 IP 地址，从外部看不到数据包的路由过 程，比较安全。而传输模式，IPSec 只对 IP 有效数据载荷进行封装和加密，IP 源和目的 IP 地址不加密传送，安全程度较低。

IPSec 主要由 AH、ESP 和 IKE 组成，在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由 SA（安全关联）进行定义。配置 SA 是配置其他 IPSec 的前提，它定义了通信双方保护数据流的策略。