若某条无条件转移汇编指令采用直接寻址，则该指令的功能是将指令中的地址码送入(1)。

(1)A.PC（程序计数器）　　B.AR（地址寄存器）

C.AC（累加器）　　D.ALU（算逻运算单元）

【答案】A

【解析】本题考查指令系统基础知识。

直接寻址是指操作数存放在内存单元中，指令中直接给出操作数所在存储单元的地址。而跳转指令中的操作数即为要转向执行的指令地址，因此，应将指令中的地址码送入程序计数器（PC)，以获得下一条指令的地址，从而实现程序执行过程的自动控制功能。

若某计算机系统的I/O接口与主存采用统一编址，则输入输出操作是通过(2)指令来完成的。

(2)A.控制　　B.中断　　C.输入输出　　D.访存

【答案】D

【解析】本题考查计算机系统输入输出系统基础知识。

常用的I/O接口编址方法有两种：一是与内存单元统一编址，二是单独编址。

与内存单元统一编址方式下，是将I/O接口中有关的寄存器或存储部件看作存储器单元，与主存中的存储单元统一编址。这样，内存地址和接口地址统一在一个公共的地址空间里，对I/O接口的访问就如同对主存单元的访问一样，可以用访问内存单元的指令访问I/O接口。I/O接口单独编址是指通过设置单独的I/O地址空间，为接口中的有关寄存器或存储部件分配地址码，需要设置专门的I/O指令进行访问。这种编址方式的优点是不占用主 存的地址空间，访问主存的指令和访问接口的指令不同，在程序中容易使用和辨认。

在程序的执行过程中，Cache与主存的地址映像由(3).

(3)A.专门的硬件自动完成　　B.程序员进行调度

C.操作系统进行管理　　D.程序员和操作系统共同协调完成

【答案】A

【解析】本题考查存储系统基础知识。

高速缓存(Cache)的出现主要有两个因素：首先是由于CPU的速度和性能提高很快而主存速度较低且价格高，其次就是程序执行的局部性特点。因此，才将速度比较快而容量有限

的静态存储器芯片构成 Cache，以尽可能发挥 CPU 的高速度。因此，必须用硬件来实现 Cache 的全部功能。

总线复用方式可以(4)。

(4)A.提高总线的传输带宽　　B.增加总线的功能

C.减少总线中信号线的数量　　D.提高 CPU 利用率

【答案】C

【解析】本题考查总线基础知识。

总线是一组能为多个部件分时共享的信息传送线，用来连接多个部件并为之提供信息交换通路，通过总线复用方式可以减少总线中信号线的数量，以较少的信号线传输更多的信息。

确定软件的模块划分及模块之间的调用关系是(5)阶段的任务。

(5)A.需求分析　　B.概要设计　　C.详细设计　　D.编码

【答案】B

【解析】本题考查软件工程中的软件开发过程和软件开发阶段的基础知识。

需求分析确定软件要完成的功能及非功能性要求；概要设计将需求转化为软件的模块划分，确定模块之间的调用关系；详细设计将模块进行细化，得到详细的数据结构和算法；编码根据详细设计进行代码的编写，得到可以运行的软件，并进行单元测试。

利用结构化分析模型进行接口设计时，应以(6)为依据。

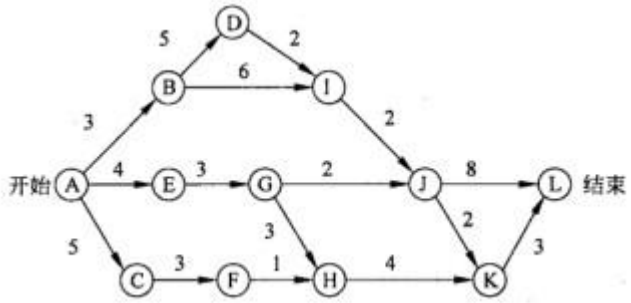
(6)A.数据流图　　B.实体-关系图　　C.数据字典　　D.状态-迁移图

【答案】A

【解析】本题考查结构化分析与设计基础知识。

软件设计必须依据软件的需求来进行，结构化分析的结果为结构化设计提供了最基本的输入信息，其关系为：根据加工规格说明和控制规格说明进行过程设计；根据数据字典和实体关系图进行数据设计；根据数据流图进行接口设计；根据数据流图进行体系结构设计。

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的值表示完成活动所需要的时间，则关键路径长度为(7)。



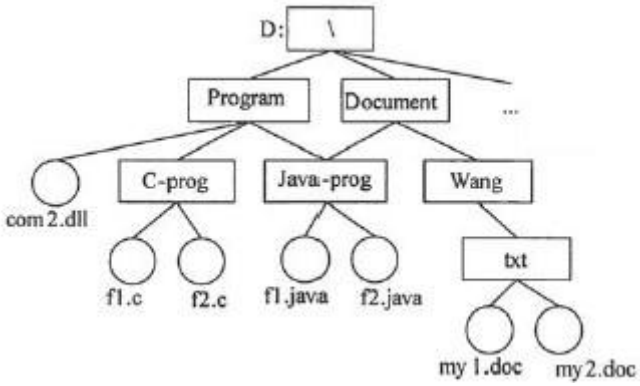
(7)A.20　　B.19　　C.17　　D.16

【答案】A

【解析】本题考查软件项目管理的相关知识。

关键路径是从开始到结束的最长路径，也是完成项目所需要的最短时间。根据上述活动图，路径 A-B-D-I-J-L 是关键路径，其长度为 20。

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 f1.java,且当前工作目录为 Program，则该文件的全文件名为(8),其相对路径为(9)。



(8)A.f1.java　　B.\Document\Java-prog\f1.java

C.D:\Program\Java-prog\f1.java　　D.\Program\Java-prog\f1.java

(9)A.Java-prog\　　B.\Java-prog\

C.Program\Java-prog　　D.\Program\Java-prog\

【答案】C　A

【解析】

文件的全文件名应包括盘符及从根目录开始的路径名，所以从题图可以看出文件 f1.java 的全文件名为 D:\Program\Java-prog\f1.java。

文件的相对路径是当前工作目录下的路径名,所以从题图可以看出文件 f1.java 的相对路径名为 Java-prog\。

(10)指可以不经著作权人许可，无需支付报酬，使用其作品。

(10)A.合理使用　　B.许可使用　　C.强制许可使用　　D.法定许可使用

【答案】A

【解析】本题考查知识产权方面的基础知识。

合理使用是指在特定的条件下,法律允许他人自由使用享有著作权的作品而不必征得著作权人的同意，也不必向著作权人支付报酬，但应当在指明著作权人姓名、作品名称，并且不侵犯著作权人依法享有的合法权利的情况下对著作权人的作品进行使用。

许可使用是指著作权人将自己的作品以一定的古式、在一定的地域和期限内许可他人使用，并由此获得经济利益。

强制许可使用是指在一定条件下,作品的使用者基于某种正当理由需要使用他人已发表的作品，经申请由著作权行政管理部门授权即可使用该作品，无需征得著作权人同意，但应向其支付报酬。

法定许可是指除著作权人声明不得使用外，使用人在未经著作权人许可的情况下，向著作权人支付报酬，指明著作权人姓名、作品名称，并且不侵犯著作权人依法享有的合法权利的情况下进行使用。

两个自治系统(AS)之间的路由协议是(11)。

(11)A.RIP　　B.OSPF　　C.BGP　　D.IGRP

【答案】C

【解析】

自治系统(AS)是由一个管理部门控制的一组网络。自治系统用16位号码来唯一地标识。因特网地址授权机构（Internet Assigned Numbers Authority，IANA)指定了各个地区的注册机构负责AS号码的分配。在AS内部采用相同的路由技术，实现统一的路由策略，不同的AS采用的路由技术和路由策略可以不同。内部网关协议（IGP)用于在自治系统内部交换路由信息，例如RIP、OSPF都是内部网关协议。外部网关协议(EGP) 用于在两个自治系统之间交换路由信息，边界网关协议BGP (Border Gateway Protocol) 是现在广泛使用的外部网关协议。

一个以太网交换机，读取整个数据帧，对数据帧进行差错校验后再转发出去，这种交换方式称为(12)。

(12)A.存储转发交换　　B.直通交换　　C.无碎片交换　　D.无差错交换

【答案】A

【解析】

根据交换方式可以把交换机划分为3种：

①存储转发交换（Store and Forward):交换机对输入的数据包先进行缓存、验证、碎片过滤，然后再进行转发。这种交换方式延时大，但是可以提供差错校验，并支持不同速度的输入/输出端口间的交换（非对称交换)，是交换机的主流工作方式。

②直通式交换（Cut-through):直通式交换机在输入端口扫描到目标地址后立即开转发。这种交换方式的优点是延迟小、交换速度快。其缺点是没有检错能力；不能实现非对称交换；并且当交换机的端口增加时，交换矩阵实现起来比较困难。

③碎片过滤式交换（Fragment Free):也叫做无碎片交换，这是介于直通式和存储转发式之间的一种交换方式。这种交换机在开始转发前先检查数据包的长度是否够64个字节，如果小于64字节，说明是冲突碎片，则丢弃之；如果大于64字节，则转发该数据包。这种转发方式的处理速度介于前两者之间，被广泛应用于中低档交换机之中。

以下关于光纤通信的叙述中，正确的是(13)。

(13)A.多模光纤传输距离远，而单模光纤传输距离近

B.多模光纤的价格便宜，而单模光纤的价格较贵

C.多模光纤的包层外径较粗，而单模光纤的包层外径较细

D. 多模光纤的纤芯较细，而单模光纤的纤芯较粗

【答案】B

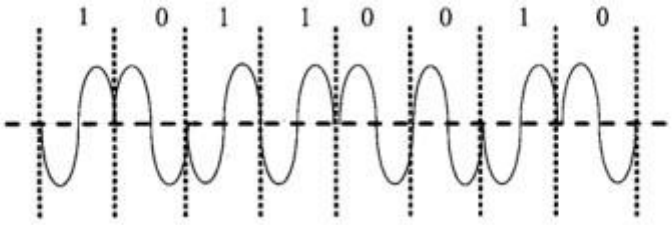
【解析】

光纤分为单模光纤和多模光纤。单模光纤（Single Mode Fiber)采用激光二极管作为光源，波长分为1310nm和1550mn两种。单模光纤的纤芯直径为8.3μm，包层外径为125μm，可表示为8.3/125μm。单模光纤色散很小，适用于远程通信。如果希望支持万兆传输，而且距离较远，应考虑采用单模光缆。

多模光纤（Multi Mode Fiber)采用发光二极管作为光源，波长分为850nm和1300nm两种。多模光纤的纤芯较粗，有50μm和62.5μm两种，包层外径125μm，分别表示为50/125μm

和 62.5/125μm。多模光纤可传多种模式的光，如果采用折射率突变的纤芯材料，则这种光纤称为多模突变型光纤；如果采用折射率渐变的纤芯材料，则这种光纤称为多 模渐变型光纤。多模光纤的色散较大，限制了传输信号的频率，而且随距离的增加这种限制会更加严重。所以多模光纤传输的距离比较近，一般只有几公里。但是多模光纤比 单模光纤价格便宜。对传输距离或数据速率要求不高的场合可以选择多模光缆。

可以用数字信号对模拟载波的不同参量进行调制，下图所示的调制方式称为(14)。



(14)A.ASK　　B.FSK　　C.PSK　　D.DPSK

【答案】C

【解析】

数字信号只有有限个离散值，使用数字信号对载波进行调制的方式称为键控(Keying)，分为幅度键控（ASK)、频移键控（FSK)和相移键控（PSK)。

幅度键控可以通过乘法器和开关电路来实现，在数字信号为“1”时电路接通，此时信道上有载波出现；数字信号为“0”时电路被关断，此时信道上无载波出现。在接收端可以根据载波的有无还原出数字信号的“1”和“0“。调幅技术实现简单，但抗干扰性能较差，在数据通信中已经很少使用了。

频移键控是利用两个不同频率（f1 和 f2)的载波信号分别代表数字信号“1”和“0”，即用数字信号“1”和“0”来控制两个不同频率的振荡源交替输出。这种调制技术抗干扰性能好，但占用带宽较大，频带利用率低，主要用于低速 Modem 中。

用数字数据的值调制载波的相位，这就是相移键控。例如用 180° 相移表示“1”；用 0° 相移表示“0”。这种调制方式抗干扰性能较好，而且相位的变化还可以作为定时信息来同步发送机和接收机的时钟。码元只取两个相位值的叫 2 相调制，码元取 4 个相位值的叫 4 相调制。

所谓 4 相相对相移键控(4DPSK)是利用前后两个码元之间的相对相位变化来表示二进制数据，其变化规律如下图所示，实线和虚线分别代表两种不同的调制方案，码元信号分布在

复平面的同心圆上。这样可以用一个码元代表两位二进制数，能提供较高的数据速率，但实现技术更复杂。

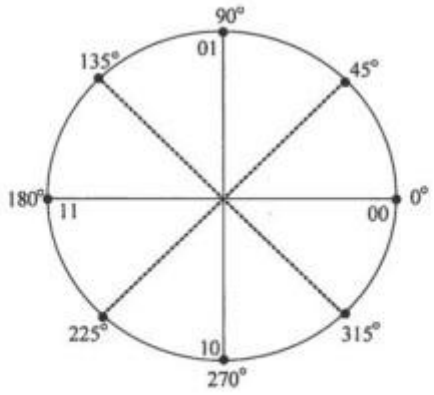
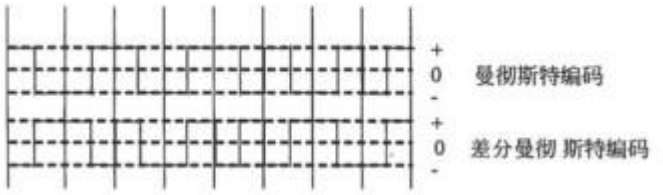


图　两种 4DPSK 调制方案

下图中画出了曼彻斯特编码和差分曼彻斯特编码的波形图，实际传送的比特串为(15)。



(15)A.10101100　　B.01110010　　C.01010011　　D.10001101

【答案】C

【解析】

曼彻斯特编码（ManchesterCode)是一种双相码。可以用高电平到低电平的转换边表示“0”，而用低电平到高电平的转换边表示“1”，相反的表示也是允许的。比特中间的电平转换边既表示了数据代码，同时也作为定时信号使用。曼彻斯特编码使用在低速以太网中。差分码又称相对码，在差分码中利用电平是否跳变来分别表示“1”或“0”，分为传号差分码和空号差分码。传号差分码是输入数据为“1”时，编码波型相对于前一代码电平产生跳变；输入为“0”时，波型不产生跳变。空号差分码是当输入数据为“0”时，编码波型相对于前一代码电平产生跳变；输入为“1”时，波型不产生跳变。

差分曼彻斯特编码兼有差分码和曼彻斯特编码的特点，与曼彻斯特编码不同的是，这种码元中间的电平转换边只作为定时信号,而不表示数据。差分曼彻斯特编码用在令牌环网中.

E1 信道的数据速率是(16),其中每个话音信道的数据速率是(17)。

(16)A.1.544Mb/s　　B.2.048Mb/s　　C.6.312Mb/s　　D.44.736Mb/s

(17)A.56Kb/s　　B.64Kb/s　　C.128Kb/s　　D.2048Kb/s

【答案】B　B

【解析】

时分多路复用（Time Division Multiplexing，TDM)要求各个子通道按时间片轮流地占用整个带宽。时间片的大小可以按一次传送一位、一个字节或一个固定大小的数据块所需的时间来确定。

时分多路复用按照子通道动态利用情况又可再分为两种：同步时分和统计时分。在同步时分制下，整个传输时间划分为固定大小时槽，各子通道都占有一个固定位置的时 槽。这样，在接收端可以按约定的时间关系恢复各子通道的信息流。当某个子通道的时槽来到时如果没有信息要传送，这一部分带宽就浪费了。

统计时分制是对同步时分制的改进。在发送端，集中器依次循环扫描各个子通道。若某个子通道有信息要发送则为它分配一个时槽，若没有信息就跳过，这样就没有空槽在线路上传播了。然而需要在每个时槽中加入一个控制字段，以便接收端可以确定该时槽是属于哪个子通道的。 ’

在美国和日本使用的一种通信标准是贝尔系统的T1 载波（见下图），它把 24 路话音信道按时分多路的原理复合在一条 1.544Mb/s 的高速信道上。该系统的工作是这样的，用一个编码解码器轮流对 24 路话音信道取样、量化和编码，一个取样周期（125μs）中得到的 7 位一组的数字合成一串，共 7×24 位长。这样的数字串在送入高速信道前要在每一个 7 位组的后面插入一个信令位，于是变成了 8×24=192 位长的数字串。这 192 位数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 125 叫传送一帧。每个子信道的数据速率为 56Kb/s。

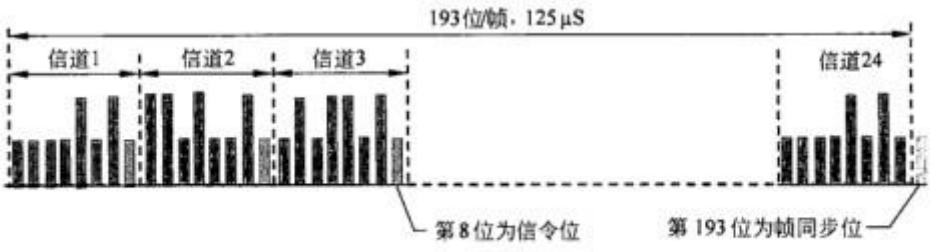


图　T1 载波

T1 载波还可以多路复用到更高级的载波上，4 个 1.544 Mb/s 的 T1 信道结合成 1 个 6.312Mb/s 的 T2 信道，7 个 T2 信道组合成 1 个 T3 信道，6 个 T3 信道组合成 1 个 T4 信道。

ITU-T 的 E1 信道的数据速率是 2.048Mb/s (参见下图 h 这种载波把 32 个 8 位一组的数据样本组装成 125 叫的基本帧，其中 30 个子信道用于话音传送数据，2 个子信道(CH0 和 CH16)用于传送控制信令，每个子信道的数据速率为 64Kb/s。除了北美和日本外，E1 载波在其他地区得到广泛使用。

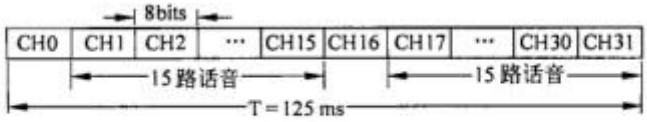


图 E1 帧

按照 ITU-T 的多路复用标准，E2 载波由 4 个 E1 载波组成，数据速率为 8.448Mb/s。E3 载波由 4 个 E2 载波组成，数据速率为 34.368Mb/s。E4 载波由 4 个 E3 载波组成，数据速率为 139.264Mb/s。E5 载波由 4 个 E4 载波组成，数据速率为 565.148Mb/s。

在各种 xDSL 技术中，能提供上下行信道非对称传输的是(18)

(18)A.ADSL 和 HDSL　　B.ADSL 和 VDSL　　C.SDSL 和 VDSL　　D.SDSL 和 HDSL

【答案】B

【解析】

数字用户线（Digital Subscriber Line，DSL)是基于普通电话线的宽带接入技术，可以在一对铜质双绞线上同时传送数据和话音信号。DSL 有多种模式，统称为 xDSL。
根据上、下行传输速率是否相同，可以把 DSL 划分为对称和不对称两种传输模式。对称 DSL 的上、下行传输速率相同，用于代替传统的 T1/E1 接入线路。对称数字用户线 SDSL (Symmetric Digital Subscriber Line)是一个通用的术语，涵盖了在一对或多对双绞线上提供不同数据速率的各种实现方式。SDSL 可以在一对双绞线上提供的对称速率范围为 128Kb/s～2.32Mb/s,最常见的是 768Kb/s,最大传输距离达 5km 以上。

高数据速率用户数字线（High-data-rate DSL, HDSL)采用两对双绞线提供全双工数据传输，支持 nX64Kb/s(n=1，2，3，…）的各种速率，最高可达 1.544Mb/s 或 2.048Mb/s，传输距离可达 3～5km。HDSL 在视频会议、远程教学、移动电话基站连接等方面得到了广泛应用。HDSL2 是 HDSL 的演进版本，可以在一对双绞线上提供 1.5Mb/s 数据速率。

非对称 DSL 的上、下行传输速率不同，适用于对双向带宽要求不一样的应用，例如 Web 浏览、多媒体点播、信息发布等。

速率自适应用户数字线（RateAdaptiveDSL，RADSL)支持同步和非同步传输方式，下行速率为640Kb/s～12Mb/s，上行速率为128Kb/s～IMb/s,也支持数据和语音同时传输。RADSL具有速率自适应的特点，可以根据双绞线的质量和传输距离动态调整用户访问速率。RADSL允许通信双方的Modem寻找流量最小的频道来传送数据，以保证一定的数据速率。_SL特别适用于线路质量千差万别的农村、山区等地区使用。

甚高比特率数字用户线（Very High Bit-rateDSL，VDSL)可在较短的距离上获得极高的传输速率，是各种DSL中速度最快的一种。在一对铜质双绞线上，VDSL的下行速率可以扩展到52Mb/s，同时支持1.5～2.3Mb/s的上行速率，但传输距离只有300～1000m。当下行速率降至13Mb/s时，传送距离可达到1.5km以上，此时上行速率为1.6～2.3Mb/s 左右。传输距离的缩短，会使码间干扰大大减少，数字信号处理过程就大为简化，所以其设备成本要比ADSL低。

ADSL (Asymmetrical Digital Subscriber Line)是一种非对称 DSL 技术，在一对铜线上可提供上行速率512Kb/s～IMb/s,下行速率1～8Mb/s,有效传输距离在3～5km左右。ADSL在进行数据传输的同时还可以使用第三个信道提供4KHz的语音传输。现在比较成熟的ADSL标准有两种，即GDMT和G.Lite。

采用ADSL虚拟拨号接入方式中，用户端需要安装(19)软件。

(19)A.PPP　　B.PPPoE　　C.PPTP　　D.L2TP

【答案】B

【解析】

点对点协议PPP (Point-to-PointProtocol)定义了一种封装机制，可以在点对点链路上传输多种协议的分组。PPP应用在许多场合，例如家庭用户拨号上网，在Modem和网络中心之间要运行点对点协议；又例如局域网远程联网时要租用公网专线，可以通过点对点协议来支持两个远程路由器之间的通信。

第2层随道协议L2TP (Layer 2 Tunneling Protocol)扩展了 PPP模型，允许第二层连接端点和PPP会话端点驻留在由分组交换网连接的不同设备中。在L2TP模型中，用户通过第二层连接访问集中器，而集中器则把PPP帧通过随道传送给网络访问服务器 NAS，从而把逻辑的PPP会话扩展到了帧中继或Internet这样的公共网络上。

PPTP (Point-to-Point Tunneling Protocol)是由 Microsoft、Ascend、3Com 和 ECI 等公司组成的 PPTP 论坛制定的第 2 层随道协议。PPTP 定义了由接入集中器（PAC)和网络服务器（PNS)组成的客户机/服务器结构，用以支持虚拟专用网。

PPPoE(PPP over Ethernet)是把 PPP 协议封装在以太帧中传送，类似地，PPPoACPPP over ATM)是把 PPP 协议封装在 ATM 虚电路中传送。ADSL 分为虚拟拨号和准专线两种接入方式。采用虚拟拨号方式的用户需要安装 PPPoE 或 PPPoA 客户端软件，以及类似于 Modem 的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门分配的静态或动态 IP 地址，开机即可接入 Internet。

ICMP 协议属于 TCP/IP 网络中的(20)协议，ICMP 报文封装在(21)包中传送。

(20)A.数据链路层　　B.网络层　　C.传输层　　D.会话层

(21)A.IP　　B.TCP　　C.UDP　　D.PPP

【答案】B　A

【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。

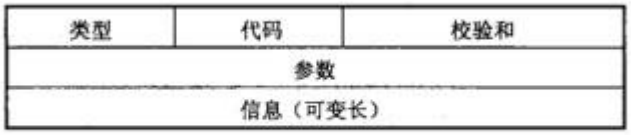


图　ICMP 报文格式

ARP 表用于缓存设备的 IP 地址与 MAC 地址的对应关系，采用 ARP 表的好处是(22)。

(22)A.便于测试网络连接数　　B.减少网络维护工作量

C.限制网络广播数量　　D.解决网络地址冲突

【答案】C

【解析】

IP 地址是分配给主机的逻辑地址（或称协议地址），同时每个主机还有一个在子网内部唯一的 MAC 地址，我们把这个地址叫做物理地址或硬件地址。从网络互连的角度看，协议地址在整个互连网络中有效，而物理地址只是在子网内部有效；从网络协议分层的角度看，协议地址由网络层使用，而物理地址由数据链路层使用。

由于有两种地址，因而需要一种映像关系把这两种地址对应起来。在 Internet 中用地址分解协议（Address Resolution Protocol，ARP)来实现协议地址到物理地址的映像。 ARP 分组的格式如下图所示。

<table>
<tr><td colspan="2">硬件类型</td><td>协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议地址长度</td><td>操作类型</td></tr>
<tr><td colspan="3">发送结点硬件地址</td></tr>
<tr><td colspan="3">发送结点协议地址</td></tr>
<tr><td colspan="3">目标结点硬件地址</td></tr>
<tr><td colspan="3">目标结点协议地址</td></tr>
</table>

图　ARP/RARP 分组格式

通常应用程序把要发送的报文交给 IP 协议，IP 当然知道接收方的协议地址（否则就不能通信了），但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路实体之前可以用两种方法得到目标结点的物理地址：

①检查本地内存中的 ARP 地址映像表，其逻辑结构如下图所示。可以看出这是 IP 协议地址和以太网 MAC 地址的对照表。

②如果在 ARP 表中查不到，就广播一个 ARP 请求分组，这种分组经过路由器进一步转发，可以到达所有连网的主机，其含义是：“如果你的 IP 地址是这个分组中的目标结点协议地址，请回答你的物理地址是什么”。收到该分组的主机一方面可以用分组中的两个源地址更新自己的 ARP 地址映像表，一方面用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的硬件地址，若不相符则不予回答。

可见，由于 ARP 表的存在，加速了 MAC 地址的查找，同时限制了网络播的 ARP 请求的数量。

IP 地址	以太网地址
130.130.87.1	08 00 39 00 29 D4
129.129.52.3	08 00 5A 21 17 22
192.192.30.5	08 00 10 99 A1 44

图　ARP 地址映像表

以下有关边界网关协议 BGP4 的叙述中，不正确的是(23).

(23)A.BGP4 网关向对等实体（Peer)发布可以到达的 AS 列表

B.BGP4 网关采用逐跳路由（hop-by-hop)模式发布路由信息

C.BGP4 可以通过路由汇聚功能形成超级网络（supernet)

D.BGP4 报文直接封装在 IP 数据报中传送

【答案】D

【解析】

边界网关协议 BGP (Border Gateway Protocol)是应用于自治系统（AS)之间的外部网关协议。BGP 基本上是一个距离矢量路由协议，但是与 RIP 协议采用的算法稍有区别。BGP 不但为每个目标计算最小通信费用，而且跟踪通向目标的路径；它不但把目标的通信费用发送给每一个邻居，而且也公告通向目标的最短路径（由 AS 的列表组成)。所以 BGP 采用的算法也叫做通路矢量路由（Path Vector Routing)算法。

BGP 算法没有距离矢量路由协议的不稳定性，可以避免路由循环。当 BGP 路由器收到一条路由信息时，首先检查它所在的自治系统是否在通路列表中。如果在列表中，则该路由信息被忽略，从而避免了出现路由循环。 •

BGP 支持无类别的域间路由（CIDR)。例如，某 ISP 有一个地址块，195.10.×.×，其中包含 256 个传统的 C 类网络，地址范围从 195.10.0.×到 195.10.255.×。BGP 协议可以把这 256 个 C 类网络组成一个超网（Supemet),与传统的 B 类网络一样大，并且向邻居发送一个有关地址块 195.10.×.×的公告，从而避免了发送 256 个 C 类网络的地址公告，同时也减小了路由表的大小。

BGP 邻居之间通过 TCP 连接交换路由信息，使用端口号 179。这意味着 BGP 不需要差错控制和流量控制。当检测到路由表改变时，BGP 只把改变了路由通过 TCP 连接发送给它的邻居。BGP 不需要周期地发送更新信息，BGP 路由更新公告通过最短的路径到达目标。

为了限制路由信息传播的范围，OSPF 协议把网络划分成 4 种区域(Area)，其中(24) 的作用是连接各个区域的传输网络，(25)不接受本地自治系统之外的路由信息。

(24)A.不完全存根区域　　B.标准区域　　C.主干区域　　D.存根区域

(25)A.不完全存根区域　　B.标准区域　　C.主干区域　　D.存根区域

【答案】C　D

【解析】

OSPF 定义了以下 5 种区域，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。

主干区域：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。

POP3 协议采用(26)模式，当客户机需要服务时，客户端软件(OutlookExpress 或 FoxMail)与 POP3 服务器建立(27)连接。

(26)A.Browaer/Server　　B.Client/Server

C.Peer to Peer　　D.Peer to Server

(27) A.TCP　　B.UDP　　C.PHP　　D.IP

【答案】B　A

【解析】

POP3 协议采用 Client/Server 模式，当客户机需要服务时，客户端软件(Outlook Express 或 FoxMail)与 POP3 服务器建立 TCP 连接。

SMTP 服务器端使用的端口号默认为(28)。

(28)A.21　　B.25　　C.53　　D.80

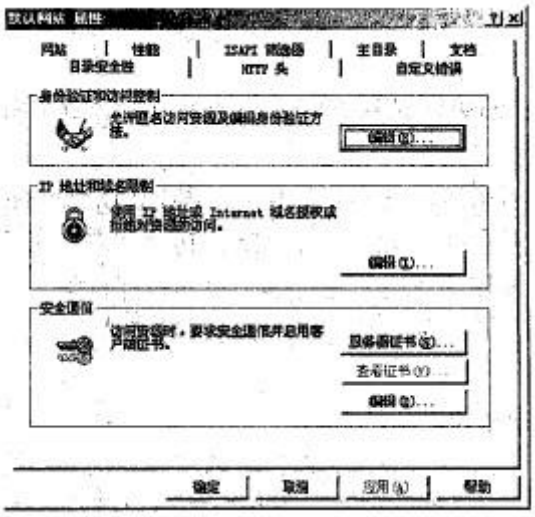
【答案】B

【解析】本题考查 TCP/IP 协议簇中几个重要的应用层协议相关知识。

TCP/IP 协议簇应用层几个常用协议及其服务端端口号如下表所示：

协议	使用的端口号
HTTP	80
SMTP	25
POP	110
TELNET	23
FTP	20、21

下图为Web站点的默认网站属性窗口，如果要设置用户对主页文件的读取权限，需要在(29)选项卡中进行配置。



(29)A.网站　　B.主目录　　C.文档　　D.HTTP头

【答案】B

【解析】本题考查Web服务器配置相关知识。

在配置Web站点时，主目录选项卡中可配置主页文件的放置目录及用户对主页文件的读取权限。

DHCP客户端启动时会向网络发出一个Dhcpdiscover包来请求IP地址，其源IP地址为(30)。

(30)A.192.168.0.1　　B.0.0.0.0　　C.255.255.255.0　　D.255.255.255.255

【答案】B

【解析】本题考查DHCP服务器配置相关知识。

DHCP服务器配置完成后，客户端启动时会向网络发出一个Dhcpdiscover包来请求IP地址，由于此时尚未分配IP地址，故其源IP地址与目标IP地址均为0.0.0.0。

当使用时间到达租约期的(31)时，DHCP 客户端和 DHCP 服务器将更新租约。

(31)A.50%　　B.75%　　C.87.5%　　D.100%

【答案】A

【解析】本题考查 DHCP 服务器配置相关知识。

当使用时间到达租约期的 50%时，DHCP 客户端和 DHCP 服务器将更新租约。

在 Linux 中，某文件的访问权限信息为“-rwxr--r--”，以下对该文件的说明中，正确的是(32)。

(32)A.文件所有者有读、写和执行权限，其他用户没有读、写和执行权限

B.文件所有者有读、写和执行权限，其他用户只有读权限

C.文件所有者和其他用户都有读、写和执行权限

D.文件所有者和其他用户都只有读和写权限

【答案】B

【解析】本题考查 Linux 基础知识。

在 Linux 操作系统中，为了保证文件信息的安全，Linux 给文件都设定了一定的访问权限。Linux 中的每一个文件都归某一个特定的用户所有，而且一个用户一般总是与某个用户组相关。Linux 对文件的访问设定了三级权限：文件所有者，与文件所有者同组的用户，其他用户。对文件的访问主要是三种处理操作：读取、写入和执行。三级访问权限和三种处理操作的组合就形成了 9 种情况。可以用它来确定哪个用户可以通过何种方式对文件和目录进行访问和操作。同时，用户可以为自己的文件赋予适当的权限，以保证他人不能修改和访问。当用 Is-l 命令显示文件或目录的详细信息时，每一个文件或目录的列表信息分为四部分，其中最左边的一位是第一部分标示 Linux 操作系统的文件类型，其余三部分是三组访问权限，每组用三位表示，如下图所示。

图　Linux 文件访问权限格式

在 Linux 中，更改用户口令的命令是(33)。

(33)A.pwd　　B.passwd　　C.kouling　　D.password

【答案】B

【解析】本题考查 Linux 基本命令。

pwd 是显示当前工作目录的命令，passwd 是更改用户口令的命令。

在 Linux 中，目录“/proc”主要用于存放(34)。

(34)A.设备文件　　B.命令文件　　C.配置文件　　D.进程和系统信息

【答案】D

【解析】本题考查 Linux 基础知识。

Linux 主要的系统目录及其简单描述如下：

/bin:存放普通用户可以使用的命令文件。目录/usr/bin 也可用来 C 存用户命令。

/sbin： 一般存放非普通用户使用的命令（有时普通用户也可能会用到）。目录/usr/sbin 中也包括了许多系统命令。

/etc：系统的配置文件。

/root：系统管理员（root 或超级用户）的主目录。

/usr：包括与系统用户直接相关的文件和目录，一些主要的应用程序也保存在该目录下。

/home：用户主目录的位置，保存了用户文件（用户自己的配置文件、文档、数据等)。

/dev：设备文件所在目录。在 Linux 中设备以文件形式表现，从而可以按照操作文件的方式简便地对设备进行操作。

/mnt：文件系统挂载点。一般用于安装移动介质，其他文件系统（如 DOS)的分区、网络共享文件系统或任何可安装的文件系统。

/lib：包含许多由/bin 和/sbin 中的_序使用的共享库文件。目录/usr/lib/中含有更多用于用户程序的库文件。

/boot：包括内核和其他系统启动时使用的文件。

/var：包含一些经常改变的文件。例如假脱机（spool)目录、文件日志目录、锁文件、临时文件等等。

/proc：操作系统的内存映像文件系统，是一个虚拟的文件系统（没有占用磁盘空间)。查看时，看到的是内存里的信息，这些文件有助于了解系统内部信息。

/initrd：在计算机启动时挂载 initrd.img 映像文件的目录以及载入所需设备模块的目录。

/opt：存放可选择安装的文件和程序。主要由第三方开发者用于安装他们的软件包。

/tap：用户和程序的临时目录，该目录中的文件被系统定时自动清空。

/lost+found：在系统修复过程中恢复的文件所在目录。

网络用户只能接收但不能发送 Email，不可能的原因是(35)。

(35)A.邮件服务器配置错误

B.路由器端口的访问控制列表设置为 deny pop3

C.路由器端口的访问控制列表设置为 deny smtp

D.客户端代理设置错误

【答案】B

【解析】本题考查邮件服务器配置相关知识。

当邮件服务器配置错误时可能不能发送 Email; 若路由器端口的访问控制列表设置为 deny pop3,会导致网络用户不能接收 Email，与能否发送 Email 无关；若路由器端口的访问控制列表设置为 deny smtp，会导致网络用户不能发送 Email;若客户端代理设置错误，比如发送服务器的域名设置错误，会导致网络用户不能发送 Email。

配置 FTP 服务器的属性窗口如下图所示，默认情况下“本地路径”文本框中的值为(36).

(36)A.c:\inetpub\wwwroot　　B.c:\inetpub\ftproot

C.c:\wmpubi\wwwroot　　D.c:\wmpubi\ftproot

【答案】B

【解析】本题考查 FTP 服务器配置相关知识。

默认情况下，配置 FTP 服务器时“本地路径”文本框中的值为 c:\inetpub\ftproot。

在 Windows 系统中，进行域名解析时，客户端系统会首先从本机的(37)文件中寻找域名对应的 IP 地址。在该文件中，默认情况下必须存在的一条记录是(38).

(37)A.hosts　　B.lmhosts　　C.networks　　D.dnsfile

(38)A.192.168.0.1 gateway　　B.224.0.0.0 multicase

C.0.0.0.0 source　　D.127.0.0.1 localhost

【答案】A　　D

【解析】本题考查域名解析服务相关知识。

在 Windows 系统中，进行域名解析时，客户端系统会首先从本机的 hosts 文件中寻找域名对应的 IP 地址。hosts 文件有用户存放的域名与 IP 地址的对应关系，该文件中通常存在一条 127.0.0.1 localhost,用于设置本地环路。hosts 文件的内容如下图所示。

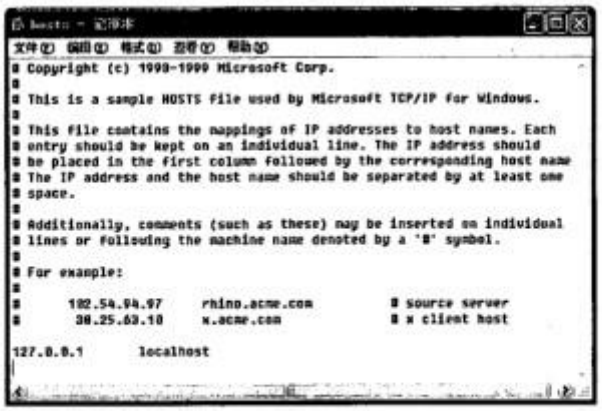
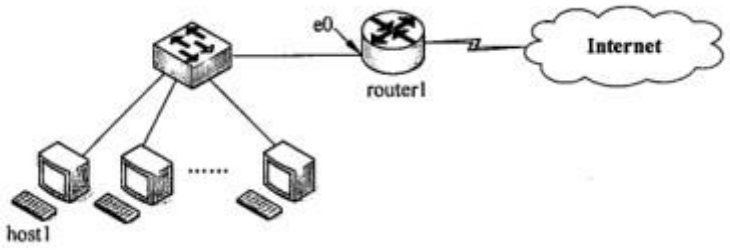


图　hosts 文件示例

某网络拓扑结构如下图所示:



在主机 host1 的命令行窗口输入 tracertwww.abc.com.cn 命令后，得到如下结果:

C:\Documents and Settings\User>tracert www.abc.com.cn

Tracing route to caelum .abc.com.cn [208.30.1.101]

over a maximum of 30 hops:

1 1ms 1ms <1ms 119.215.67.254

2 2ms 1ms 1ms172.116. 11.2

3 71ms 1ms 1ms 119.145. 65.86

4 1ms 1ms 1ms 172.116.141.6

5 1ms 1ms 1ms 192.168.66.14

6 1ms 1ms <1ms 208.30.1.101

Trace complete

则路由器 router1 e0 接口的 IP 地址为(39);www.abc.com.cn 的 IP 地址为（40）。

(39)A.172.116.11.2　　B.119.215.67.254

C.210.120.1.30　　D.208.30.1.101

(40)A.172.116.11.2　　B.119.215.67.254

C.210.120.1.30　　D.208.30.1.101

【答案】B　D

【解析】本题考查网络配置及相关知识。

在输入 tracert 命令后记录的是到达目的主机所经过的所有路由的延迟时间及地址，故第一条记录应为本地网关地址，最后一条为目的主机地址，由此路由器 router1 e0 接口的 IP 地址为 119.215.67.254; www.abc.com.cn 的 IP 地址为 208.30.1.101。

某报文的长度是 1000 字节，利用 MD5 计算出来的报文摘要长度是(41)位，利用 SHA 计算出来的报文摘要长度是(42)位。

(41)A.64　B.128　C.256　D.160

(42)A.64　B.128　C.256　D.160

【答案】B　D

【解析】本题考查网络安全方面关于报文摘要算法的基础知识。

报文摘要算法原理是用不定长的输入数据，通过散列方法转换成定长的输出，主要算法是 MD5 和 SHA, MD5 的输出长度是 128 位，SHA 的输出是 160 位，与报文本身的长度没有关系。

以下安全协议中，用来实现安全电子邮件的协议是(43)。

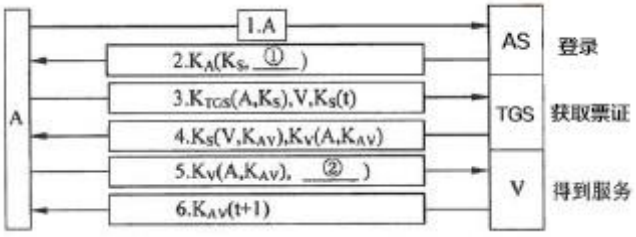
(43)A. IPSec　　B. L2TP　　C. PGP　　D. PPTP

【答案】C

【解析】本题考查网络安全方面关于安全协议的基础知识。

PGP (Pretty Good Privacy)是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。PGP 已经成为使用最广泛的电子邮件加密软件。

Kerberos 由认证服务器(AS)和票证授予服务器(TGS)两部分组成，当用户 A 通过 Kerberos 向服务器 V 请求服务时，认证过程如下图所示，图中①处为(44),②处为(45)。



(44)A. KTGS(A,KS)　　B. KS(V,KAV)　　C. KV(A,KAV)　　D. KS(t)

(45)A. KAV(t+1)　　B. KS(t+1)　　C. KSt　　D. KAVt

【答案】A　D

【解析】本题考查网络安全方面关于安全协议的基础知识。

Kerberos 由认证服务器（AS)和票证授予服务器（TGS)两部分组成，当用户 A 通过 Kerberos 向服务器 V 请求服务时，认证过程如下图所示：

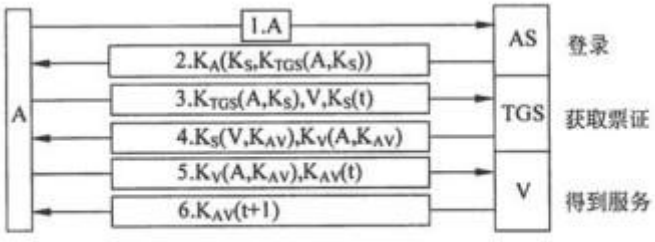


图　Kerberos 认证过程

公钥体系中，用户甲发送给用户乙的数据要用(46)进行加密。

(46)A. 甲的公钥　　B. 甲的私钥　　C. 乙的公钥　　D. 乙的私钥

【答案】C

【解析】本题考查网络安全方面公钥体系的基础知识。

两个用户进行通信时，发送方可以用自身的私钥对数据进行签名，同时也可以用对方的公钥对数据进行加密，接收方收到数据后，用对方的公钥验证签名，用自身的私钥解密数据。

RMON 和 SNMP 的主要区别是(47)。

(47)A.RMON 只能提供单个设备的管理信息，而 SNMP 可以提供整个子网的管理信息

B.RMON 提供了整个子网的管理信息，而 SNMP 管理信息库只包含本地设备的管理信息

C.RMON 定义了远程网络的管理信息库，而 SNMP 只能提供本地网络的管理信息

D.RMON 只能提供本地网络的管理信息，而 SNMP 定义了远程网络的管理信息库

【答案】B

【解析】

SNMP 是应用层协议，它通过 UDP 数据报实现管理站与远程代理之间的通信，如下图所示。每个被管理设备中的代理实现管理信息库 MIB-2,只能收集本地的管理信息。所以最初定义的 SNMP 协议只能提供单个设备的网络管理信息，例如进出某个远程设备的分组数或字节数等。

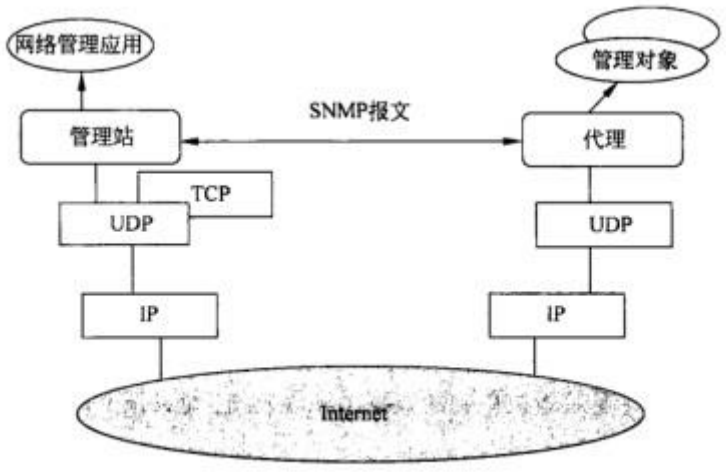


图　简单网络管理协议的体系结构

用于监视整个网络通信情况的设备叫做网络监视器（Monitor)或探测器（Probe)，这种设备观察 LAN 上出现的每个分组，并进行统计和汇总，例如提供出错统计数据（残缺分组数、冲突次数)、性能统计数据（每秒钟提交的分组数、分组大小的分布情况）等，如下图所示。

RMON 探测器（RMONProbe)实现 RMON 管理信息库（RMONMIB)，并且响应管理站的查询请求。所以 RMON 可以提供整个子网的管理信息。

SNMP 采用 UDP 提供的数据报服务传递信息，这是由于(48)。

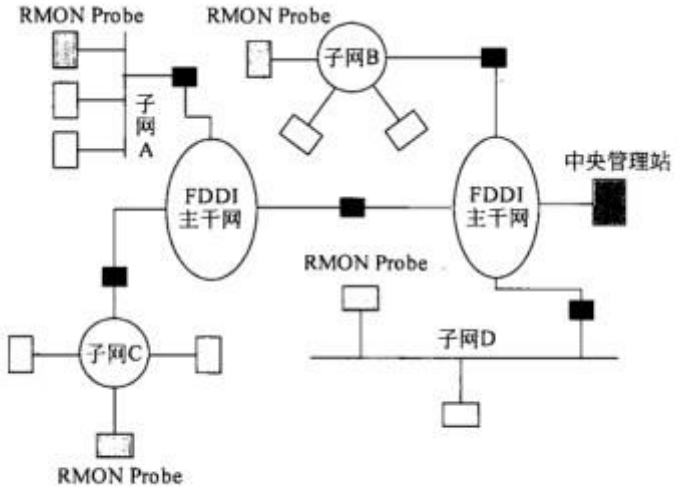


图　远程网络监视的配置

(48)A.UDP 比 TCP 更加可靠　　B.UDP 数据报文可以比 TCP 数据报文大

C.UDP 是面向连接的传输方式　　D.UDP 实现网络管理的效率较高

【答案】D

【解析】

SNMP 是应用层协议，采用 UDP 数据报服务传送网络管理报文。其所以选择 UDP 协议而不是 TCP 协议，这是因为 UDP 效率较高，这样实现网络管理不会太多地增加网络负载。但由于 UDP 不是很可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 实现的建议是对每个管理信息要装配成单独的数据报独立发送，而且报文应短些，不要超过 484 个字节。

在网络管理中要防止各种安全威胁。在 SNMP 中，无法预防的安全威胁是(49)。

(49)A.篡改管理信息：通过改变传输中的 SNMP 报文实施未经授权的管理操作

B.通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息

C.假冒合法用户：未经授权的用户冒充授权用户，企图实施管理操作

D.消息泄露：SNMP 引擎之间交换的信息被第三者偷听

【答案】B

【解析】

SNMPv3 把对网络协议的安全威胁分为主要的和次要的两类。标准规定安全模块必须提供防护的两种主要威胁是：

①修改信息（Modification of Information):就是某些未经授权的实体改变了进来的 SNMP 报文，企图实施未经授权的管理操作，或者提供虚假的管理对象。

②假冒（Masquerade):即未经授权的用户冒充授权用户的标识，企图实施管理操作。

SNMPv3 标准还规定安全模块必须对两种次要威胁提供防护：

①修改报文流（Message Stream Modification)：由于 SNMP 协议通常是基于无连接的传输服务，重新排序报文流、延迟或重放报文的威胁都可能出现。这种威胁的危害性在于通过报文流的修改可能实施非法的管理操作。

②消息泄露（Disclosure): SNMP 引擎之间交换的信息可能被偷听，对这种威胁的防护应采取局部的策略。

有两种威胁是安全体系结构不必防护的,因为它们不是很重要,或者这种防护没有多大作用：

①拒绝服务（Denial of Service):因为在很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全子系统不必采取措施。

②通信分析（Traffic Analysis):即由第三者分析管理实体之间的通信规律，从而获取需要的信息。由于通常都是由少数管理站来管理整个网络的，所以管理系统的通信模式是可预见的，防护通信分析就没有多大作用了。

在 Windows 的 DOS 窗口中键入命令

```
C:\> nslookup
> set type=ptr
>211.151.91.165
```

这个命令序列的作用是(50)。

(50)A.查询 211.151.91.165 的邮件服务器信息

B.查询 211.151.91.165 到域名的映射

C.查询 211.151.91.165 的资源记录类型

D.显示 211.151.91.165 中各种可用的信息

【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。nslookup 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。如果只查询一项信息，可以进入这种工作方式。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。每个命令行选项由一个连字符“-”后跟选项的名字组成，有时还要加一个等号“=”和一个数值。

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 提示符下键入 nslookup 后回车，就进入了交互工作方式，命令提示符变成“>”。

```
> set type=ptr                                              #查询PTR记录
> 211.151.91.165                                           #由地址查域名
服务器:  [61.134.1.4]
Address:  61.134.1.4

非权威应答:
165.91.151.211.in-addr.arpa     name = 165.tsinghua.edu.cn    #查询成功，得到域名
> www.tsinghua.edu.cn                                      #由域名查地址
服务器:  [61.134.1.4]
Address:  61.134.1.4

DNS request timed out.
    timeout was 2 seconds.
非权威应答:
www.tsinghua.edu.cn     canonical name = www.d.tsinghua.edu.cn

d.tsinghua.edu.cn
        primary name server = dns.d.tsinghua.edu.cn          #没有查出地址
        responsible mail addr = szhu.dns.edu.cn               但给出了SOA记录
        serial  = 2007042815
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

图　查询 ptr 记录

在交互方式下，可以用 set type 命令设置查询的资源记录类型。DNS 服务器中主要的资源记录有 A（域名到 IP 地址的映射）、PTR（IP 地址到域名的映射）、MX（邮件服务器及其优先级）、CNAM（别名）和 NS（区域的授权服务器）等类型。通过 A 记录可以由域名查地址，也可以由地址查域名。当查询 PTR 记录时，可以由地址查到域名，参见上图。

32 位的 IP 地址可以划分为网络号和主机号两部分。下面的地址中(51)不能作为目标地址，(52)不能作为源地址。

(51)A. 0.0.0.0　　B. 127.0.0.1　　C. 10.0.0.1　　D. 192.168.0.255/24

(52)A. 0.0.0.0　　B. 127.0.0.1　　C. 10.0.0.1　　D. 192.168.0.255/24

【答案】A　D

【解析】

网络号为 0 是指本地网络，主机号为 0 是指本地主机，所以 0.0.0.0 不能作为目标地址。主机号为全 1 的是广播地址，而地址 192.168.0.255/24 是一个 C 类广播地址，所以不能作为源地址。

假设用户 Q1 有 2000 台主机，则必须给他分配(53)个 C 类网络，如果分配给用户 Q1 的超网号为 200.9.64.0,则指定给 Q1 的地址掩码为(54)；假设给另一用户 Q2 分配的 C 类网络号为 200.9.16.0～200.9.31.0,如果路由器收到一个目标地址为 11001000 00001001 01000011 00100001 的数据报，则该数据报应送给用户(55)。

(53)A.4　　B.8　　C.10　　D.16

(54)A.255.255.255.0　　B.255.255.250.0

C.255.255.248.0　　D.255.255.240.0

(55)A.Q1　　B.Q2　　C.Q1 或 Q2　　D.不可到达

【答案】B　C　A

【解析】

每一个 C 类网络可以分配的主机地址数为 254 个，所以对 Q1 用户必须分配给 8 个 C 类网络，其地址掩码应该为 255.255.248.0。路由器查找路由表时把目标地址与每个表项进行对比，

目标地址为 11001000 0000.1001-41000011 00100001

Q1 的地址 200.9.64.0 11001000 00001001 01000000 00000000/22

Q2 的地址 200.9.16.0 11001000 00001001 00010000 00000000/20

按照最长匹配规则，显然目标地址与 Q1 的地址匹配。

建筑物综合布线系统中工作区子系统是指(56)。

(56)A.由终端到信息插座之间的连线系统　　B.楼层接线间的配线架和线缆系统

C.各楼层设备之间的互连系统　　D.连接各个建筑物的通信系统

【答案】A

【解析】

结构化布线系统分为六个子系统：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。

工作区子系统是指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。

信息插座的类型应根据终端设备的种类而定。信息插座的安装分为嵌入式（新建筑物）和表面安装（老建筑物）两种方式，信息插座通常安装在工作间四周的墙壁下方，距离地面30cm,也有的安装在用户办公桌上。通常一个信息插座需要9平方米的空间。

设有下面4条路由:196.34.129.0/24、196.34.130.0/24、196.34.132.0/24 和196.34.133.0/24,如果进行路由汇聚，能覆盖这4条路由的地址是(57)。

(57)A.196.34.128.0/21　　B.196.34.128.0/22

C.196.34.130.0/22　　D.196.34.132.0/23

【答案】A

【解析】

196.34.129.0/24 的二进制表示是 11000100 00100010 10000001 00000000

196.34.130.0/24 的二进制表示是 11000100 00100010 10110010 00000000

196.34.132.0/24 的二进制表示是 11000100 00100010 10000100 00000000

196.34.133.0/24 的二进制表示是 11000100 00100010 10000101 00000000

从中可以看出，经过路由会聚的地址应该是196.34.128.0/21。

IPv6 地址33AB:0000:0000:CD30:0000:0000:0000:0000/60 可以表示成各种简写形式，以下写法中，正确的是(58).

(58)A.33AB:0:0:CD30::/60　　B.33AB:0:0:CD3/60

C.33AB::CD30/60　　D.33AB::CD3/60

【答案】A

【解析】

IPv6地址扩展到128位。2128足够大，这个地址空间可能永远用不完。事实上，这个数足够为地球上每个分子分配一个IP地址。

IPv6 地址采用冒号分隔的十六进制数表示，例如下面是一个 IPv6 地址

8000:0000:0000:0000:0123:4567:89AB:CDEF

为了便于书写，规定了一些简化写法。首先，每个字段前面的 0 可以省去，例如 0123 可以简写为 123;其次一个或多个全 0 字段 0000 可以用一对冒号代替。例如以上地址可简写为

8000::123:4567:89AB:CDEF

因此,答案 B 的错误在于 CD30 不能省略成 CD3,答案 C 的错误在于::之间 0 的个数无法确定，答案 D 的错误综合了 B 和 C 的错误。

配置路由器时，PC 的串行口与路由器的(59) 口相连，路由器与 PC 串行口通信的默认数据速率为(60)。

(59)A.以太接口　　B.串行接口　　C.RJ-45 端口　　D.console 接口

(60) A.2400b/s　　B.4800b/s　　C.9600b/s　　D.10Mb/s

【答案】D　C

【解析】

第一次配置路由器必须通过控制台端口来访问，这也是最常用、最有效的配置方法。控制台端口是路由器的基本端口，连接控制台端口的线缆称为控制台电缆(Console Cable)。控制台电缆一端插入路由器的控制台端口，另一端插入 PC 的串行口，参见下图。

图　通过控制台端口访问路由器

计算机与路由器连接好以后，进入系统桌面，点击“开始一所有程序一附件一通讯一超级终端”，然后配置连接的默认参数。路由器与 PC 串行口通信的默认数据速率为 9600b/s，参见下图。

图 连接属性

交换机命令 SwitchA(VLAN) #vtp pruning 的作用是(61)。

(61)A.退出 VLAN 配置模式　　B.进入配置子模式

C.删除一个 VLAN　　D.启动 VLAN 修剪功能

【答案】D

【解析】

VLAN 中继协议（VLAN Trunking Protocol, VTP)用于简化 VLAN 的管理。VTP 协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为服务器模式（Server)、客户机模式（Client）和透明模式（Transparent)。只有在服务器模式下，交换机才能创建和修改 VLAN 配置。在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包、或者一个未知的单播数据包，交换机都会将其洪泛（flood)到所有与源 VLAN 端口相关的各个输出端口上（包括中继端口）。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

例如，在图 2-5 中，PC-A、PC-B、PC-E 和 PC-F 同属于 VLAN1（用粗虚线表示）。如果 PC-A 产生了一个广播包，则交换机 A 将把它转发给连接 PC-B 的接入链路，也转发到连接交换机 B 的中继链路，因为中继链路是任何 VLAN 的成员。这种转发是有意义的，因为 PC-E 和 PC-F 连接在交换机 B 上，而它们与 PC-A 同属于 VLAN 1。

在下图中，PC-C 和 PC-D 是 VLAN2（用细虚线表示）的成员。如果 PC-C 产生了一个本地广播包，显然交换机 A 会将其发送给 PC-D 的接入端口，然而若交换机 A 将这个广播包通过中继链路洪泛到交换机 B 则是无意义的，因为那里没有属于 VLAN 2 的设备。

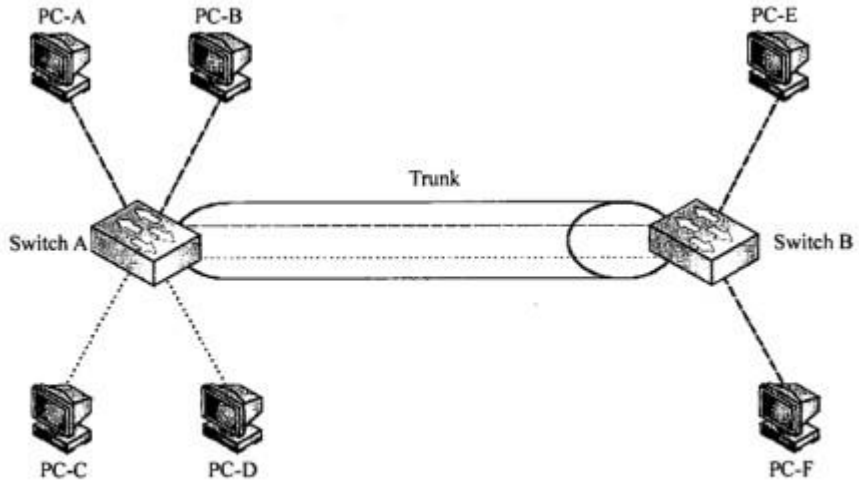


图　VLAN 之间的洪泛发送

为了解决这个问题，可以使用静态或动态的修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN，在下图中，两个交换机之间的一条中继链路已经被剪掉了。

但是，手工修剪会遇到一些问题，如果后来在交换机 B 上添加了 VLAN 2 的成员，则必须重新改变两个交换机的配置，并在中继链路上添加 VLAN 2 的中继连接。在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错。在这种情况下，并不是每一个 VLAN 都在每一个交换机上处于活动状态，并且很可能会在某条中继链路上剪掉不应该修剪的 VLAN，从而出现连接问题。

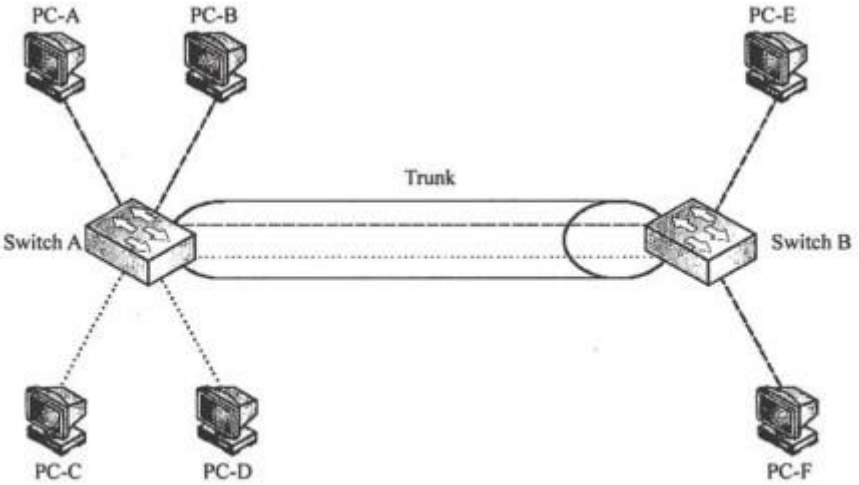


图　经过手工修剪的中继链路

VTP 动态修剪允许交换机之间共享 VLAN 信息,也允许交换机从中继连接上动态地剪掉不活动的 VLAN,使得所有共享的 VLAN 都是活动的。例如，交换机 A 可以舍诉交换机 B，它有两个活动的 VLAN1 和 VLAN2,而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。

VTP 动态修剪的缺点是它要求在 VTP 域中的所有交换机都必须配置成服务器。由于交换机在服务器模式下工作时可以改变 VLAN 配置，也可以接受 VLAN 配置的改变，所以当多个管理员在多个服务器上同时配置 VLAN 时将会出现难以预见的后果。

以太网介质访问控制策略可以采用不同的监听算法，其中一种是：“一旦介质空闲就发送数据，假如介质忙，继续监听，直到介质空闲后立即发送数据”，这种算法称为(62)监听算法。这种算法的主要特点是(63)。

(62)A.1-坚持型　　B.非坚持型　　C.P-坚持型　　D.0-坚持型

(63)A.介质利用率低，且冲突概率低　　B.介质利用率高，但冲突概率也高

C.介质利用率低，且无法避免冲突　　D.介质利用率高，且可以有效避免冲突

【答案】A　B

【解析】

在以太网上采用 CSMA 协议，其基本原理是，站在发送数据之前，先监听信道上是否有别的站发送的载波信号。若有，说明信道正忙；否则信道是空闲的。然后根据预定的策略决定，是否立即发送，还是继续监听。

监听算法有三种：

第一种是非坚持型监听算法，其处理思路是：当一个站准备好帧，发送之前先监听信道，若信道空闲，立即发送，若信道忙，则后退一个随机时间，再监听信道并重复上述过程。由于随机时延后退，从而减少了冲突的概率；然而，可能因后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

第二种是 1-坚持型监听算法，其处理思路是：当一个站准备好帧，发送之前先监听信道，若信道空闲，立即发送，否则继续监听，直到信道空闲后立即发送。这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

第三种是 P-坚持型监听算法，其处理思路是：

①若信道空闲，以概率 P 发送，以概率（1-P)延迟一个时间单位τ（网络传输时延）。

②若信道忙，继续监听直到信道空闲，转①。

③如果发送延迟一个时间单位τ，则重复①。

这种算法汲取了以上两种算法的优点，但较为复杂。

采用 CSMA/CD 协议的基带总线，其段长为 1000m，中间没有中继器，数据速率为 10Mb/s，信号传播速度为 200m/μs,为了保证在发送期间能够检测到冲突，则该网络上的最小帧长应为(64)比特。

(64)A.50　　B.100　　C.150　　D.200

【答案】B

【解析】

带冲突检测的监听算法把浪费带宽的时间减少到检测冲突的时间。对局域网来说这个时间是很短的。通过分析确定，在基带系统中检测冲突需要的最长时间为 2t，即网络传播延迟时间的两倍。

与冲突窗口相关的参数是最小帧长。如果在时间内帧已经发送完毕，这样发送站站在整个发送期间将检测不到冲突。为了避免这种情况，网络标准中根据设计的数据速率和最大网段长度规定了最小帧长 Lmin：

Lmin=2R×d/v

这里是网络数据速率，d 为最大段长，v 是信号传播速度。有了最小帧长的限制，发送站必须对较短的帧增加填充位，使其等于最小帧长。接收站对收到的帧要检查长度，小于最小帧长的帧被认为是冲突碎片而丢弃。

根据题中给出的条件，可以计算如下：

Lmin =2R×d/v=2×10Mb/s X 1000m/200m/μs = 100bit

以下属于万兆以太网物理层标准的是(65)。

(65)A.IEEE 802.3u　　B.IEEE 802.3a　　C.IEEE 802.3e　　D.IEEE 802.3ae

【答案】D

【解析】

2002 年 6 月，IEEE 发布了万兆以太网标准 802.3ae，其规定的几种传输介质如下表所示。传统以太网采用 CSMA/CD 协议，而万兆以太网基本应用于点到点线路，不再共享带宽，

也没有冲突检测，所以，载波监听和多路访问技术不再重要。千兆以太网和万兆以太网采用与传统以太网同样的帧结构。

名　称	电　缆	最大段长	特　点
10GBase-S(Short)	50μm 的多模光纤	300m	850nm 串行
	62.5μm 的多模光纤	65m	
10GBase-L(Long)	单模光纤	10km	1310nm 串行
10GBase-E(Extended)	单模光纤	40km	1550nm 串行
10GBase-LX4	单模光纤	10km	1310nm 4×2.5Gb/s 波分多路复用（WDM）
	50μm 的多模光纤	300m	
	62.5μm 的多模光纤	300m	

IEEE802.11 采用了类似于 802.3 CSMA/CD 协议的 CSMA/CA 协议，之所以不采用 CSMA/CD 协议的原因是(66)。

(66)A.CSMA/CA 协议的效率更高　　B.为了解决隐蔽终端问题

C.CSMA/CD 协议的开销更大　　D.为了引进其他业务

【答案】B

【解析】

CSMA/CA 叫做载波监听多路访问/冲突避免协议，与 CSMA/CD 协议的区别是不再使用冲突检测技术。在无线网中进行冲突检测是困难的。例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个巾贞间隔(Inter Frame Spacing, IFS)时间。另外还有一个后退计数器，它的初始值是随机设置的，递减计数直到 0。基本的操作过程是：

①如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后退计数器并坚持监听。

②听到信道空闲后等待 IFS 时间，然后开始计数。最先计数完的站可以开始发送。

其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个 IFS 时间继续计数，直到计数完成开始发送。

分析这个算法发现，两次 IFS 之间的间隔是各个站竞争发送到时间。这个算法对参与竞争的站是公平的，基本上是按先来先服务的顺序获得发送的机会。

无线局域网(WLAN)标准 IEEE802.11g 规定的最大数据速率是(67).

(67)A.1Mb/s　　B.11Mb/s　　C.5Mb/s　　D.54Mb/s

【答案】D

【解析】

IEEE 802.11 标准的制定始于 1987 年。1997 年颁布的 IEEE 802.11 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《随后又出现了两个新的标准,1998 年推出的 IEEE 802.11b 标准也是运行在 ISM 频段，采用 CCK (Complementary Code Keying)技术，支持 11Mb/s 的数据速率.1999 年推出的 IEEE 802.11a 标准运行在 U-NII (UnlicensedNational Information Infrastructure) 频段，采用 OFDM 调制技术，支持最高达 54Mb/s 的数据速率。2003 年推出的 IEEE 802.11g 标准运行在 ISM 频段，与 IEEE 802.11b 兼容，数据速率提高到 54Mb/s。下表列出了目前广泛使用的 4 种 WLAN 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

大型局域网通常组织成分层结构（核心层、汇聚层和接入层），以下关于网络核心层的叙述中，正确的是(68)

(68)A.为了保障安全性，应该对分组进行尽可能多的处理

B.将数据分组从一个区域高速地转发到另一个区域

C.由多台二、三层交换机组成

D.提供用户的访问控制

【答案】B

【解析】

大型园区网是一种具有复杂互连结构的局域网，通常被划分成不同的功能层次，典型的层次结构如下图所示。这种层次结构有利发挥联网设备的最大效率，使得故障定位可分级进行，便于维护和管理，也便于网络拓扑的后续扩展。

在三层模型中，核心层提供不同区域之间的高速连接和最优传输路径，汇聚层提供网络业务接入，并实现与安全、流量和路由相关的控制策略，接入层为终端用户提供接入服务。

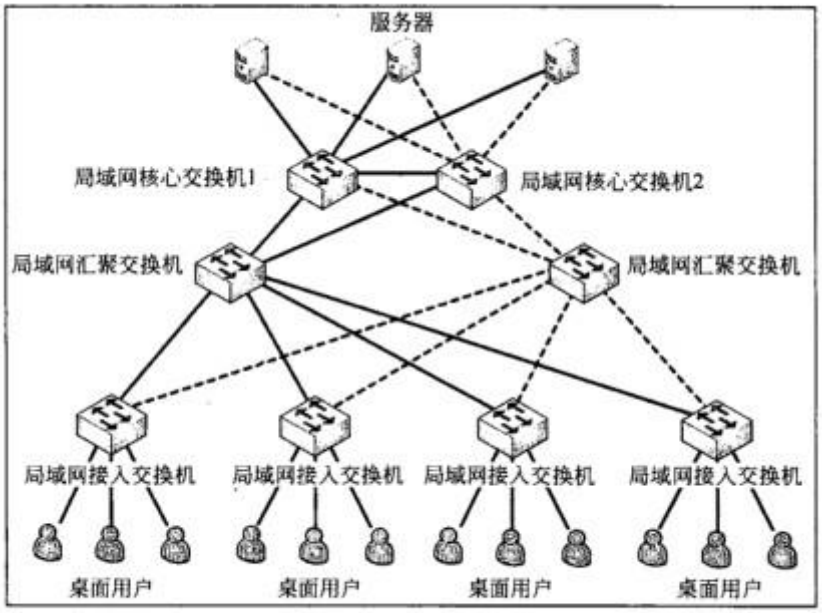


图　分层次的局域网结构

核心层是互连网络的高速主干网，在设计中应增加冗余组件，使其具备高可靠性，能快速适应通信流量的变化。在设计核心层设备的功能时应避免使用数据包过滤、策略路由等降低转发速率的功能特性，使得核心层具有高速率、低延迟和良好的可管理性。核心层设备覆盖的地理范围不宜过大，连接的设备不宜过多，否则会使得网络的复杂度增大，导致网络性能降低。核心层应包括一条或多条连接外部网络的专用链路，使得可以高效地访问互联网。’汇聚层是核心层与接入层之间的分界点，应实现资源访问控制和流量控制等功能。汇聚层应该对核心层隐藏接入层的详细信息，不管划分了多少个子网，汇聚层向核心路由器发布路由通告时，只通告各个子网汇聚后的超网地址。如果局域网中运行了以太网和弹性分组环等不同类型的子网，或者运行了不同路由算法的区域网络，可以通过汇聚层设备完成路由汇总和协议转换功能。

接入层提供网络接入服务，并解决本地网段内用户之间互相访问的需求，要提供足够的带宽，使得本地用户之间可以高速访问；接入层还应提供一部分管理功能，例如 MAC 地址认证、用户认证、计费管理等；接入层要负责收集用户信息（例如用户 IP 地址、MAC 地址、访问日志等），作为计费和排错的依据

网络设计过程包括逻辑网络设计和物理网络设计两个阶段，各个阶段都要产生相应的文档，以下选项中，(69)应该属于逻辑网络设计文档，(70)属于物理网络设计文档。

(69)A.网络 IP 地址分配方案　　B.设备列表清单

C.集中访谈的信息资料　　D.网络内部的通信流量分布

(70)A.网络 IP 地址分配方案　　B.设备列表清单

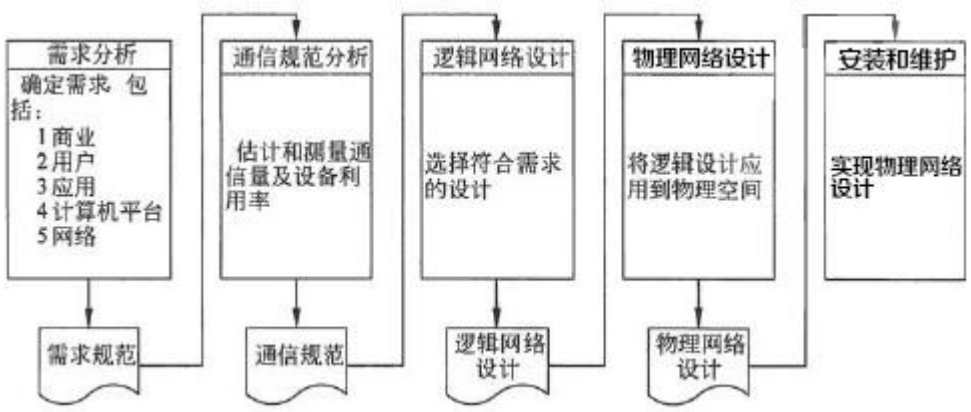
C.集中访谈的信息资料　　D.网络内部的通信流量分布

【答案】A　B

【解析】

一个网络系统从构思开始，到最后被淘汰的过程称为网络生命周期。一般来说，网络生命周期应包括系统的构思和计划、分析和设计，以及运行和维护的全过程。网络系统的生命周期是一个循环迭代的过程，每次迭代的动力都来自于网络应用需求的变更。每一个迭代周期都是网络重构的过程。常见的迭代周期构成可分为以下阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。

根据五阶段迭代周期的模型，每个阶段都必须依据上一阶段的成果，完成本阶段的工作，并形成本阶段的工作成果，作为下一阶段的工作依据。这些阶段成果分别为需求规范、通信规范、逻辑网络设计和物理网络设计文档。网络开发过程可以用下图来描述。



本题中的 4 个选项分别属于不同阶段的文档，其中：

A：网络 IP 地址分配方案：逻辑网络设计文档

B：设备列表清单：物理网络设计文档

C：集中访谈的信息资料：需求规范文档

D：网络内部的通信流量分布：通信规范文档

A transport layer protocol usually has several responsibilities. One is to create a process-to-process communication; UDP uses (71) numbers to accomplish this. Another responsibility is to provide control mechanisms at the transport level. UDP

does this task at a very minimal level. There is no flow control mechanism and there is no (72) for received packet. UDP, however, does provide error control to some extent. If UDP detects an error in the received packet, it silently drop it.

The transport layer also provides a connection mechanism for the processes. The (73) must be able to send streams of data to the transport layer. It is the responsibility of the transport layer at (74) station to make the connection with the receiver, chop the stream into transportable units, number them, and send them one by one. It is the responsibility of the transport layer at the receiving end to wait until all the different units belonging to the same process have arrived, check and pass those that are (75) free, and deliver them to the receiving process as a stream.

(71)A.hop	B.port	C.route	D.packet
(72)A.connection	B.window	C.acknowledgement	D.destination
(73)A.jobs	B.proces	C.programs	D.users
(74)A.sending	B.routing	C.switching	D.receiving
(75)A.call	B.state	C.cost	D.error

【答案】B　C　B　A　D

【解析】

传输层协议通常有几个功能，其中之一就是生成进程与进程之间的通信。UDP 使用端口号来实现这个功能。另外一个责任是在传输级实现控制机制。UDP 对于这个任务只做很少的工作。没有流量控制，对于接收到的报文也没有应答。然而，UDP 在一定程度上还是做了差错控制工作。如果 UDP 在收到的报文中检测到了错误，就直接丢弃之。

传输层也提供进程之间的连接机制。进程应该能够向传输层发送数据流。与接收站建立连接是发送方传输层的责任，同时把数据流划分成可传输的单元，对其进行编号，然后一个接一个地发送它们。接收方传输层的责任就是等待属于同一进程的各个传输单元到达，检查其正确性，让没有错误的通过，并将其组织成数据流提交给接收进程。

试题一

某学校计划部署校园网络，其建筑物分布如图 1-1 所示。

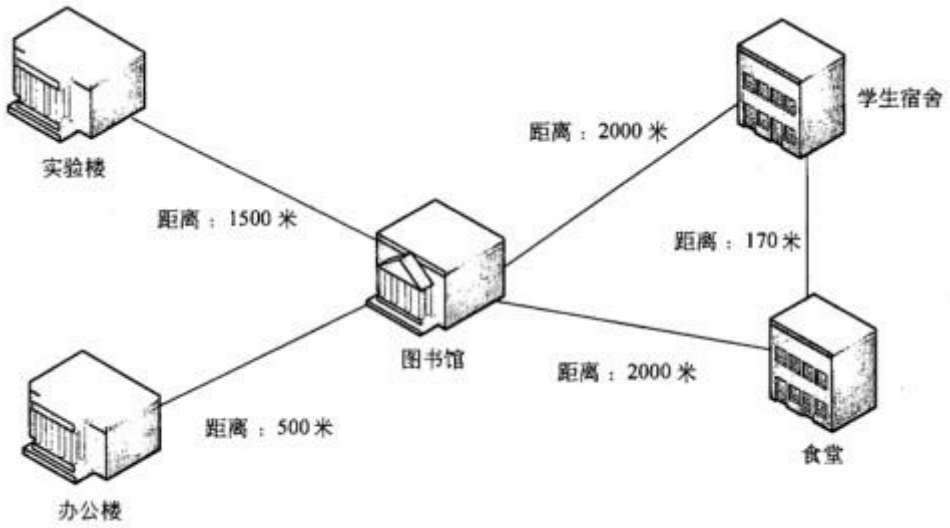


图 1-1

根据需求分析结果，校园网规划要求如下：

1.信息中心部署在图书馆。

2.实验楼部署 237 个点，办公楼部署 87 个点，学生宿舍部署 422 个点，食堂部署 17 个点。

3.为满足以后应用的需求，要求核心交换机到汇聚交换机以千兆链路聚合，同时千兆到桌面。

4.学校信息中心部署服务器，根据需求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务。

5.部署流控网关对 P2P 流量进行限制，以保证正常上网需求。

【问题 1】

根据网络需求，设计人员设计的网络拓扑结构如图 1-2 所示。

请根据网络需求描述和网络拓扑结构回答以下问题。

1.图 1-2 中设备①应为(1)，设备②应为（2），设备③应为(3)，设备④应为(4)

(1)～（4)备选答案：（每设备限选 1 次）

A.路由器 B.核心交换机 C.流控服务器 D.防火墙

2.设备④应该接在设备(5)上。

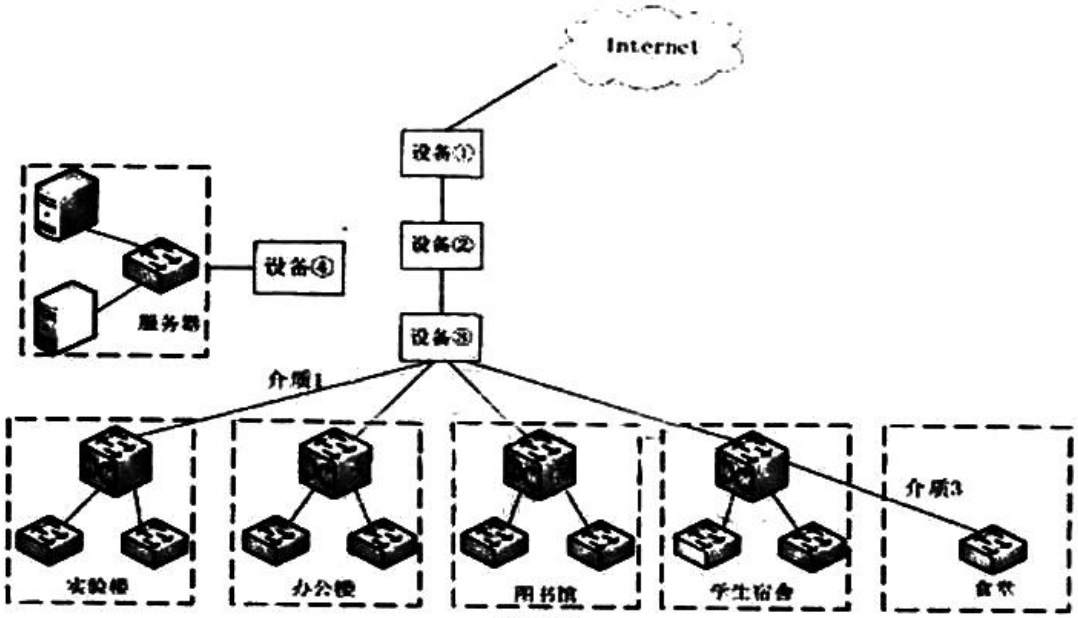


图 1-2

1.A 路由器（2）C 流控服务器 （3）B 核心交换机 （4）D 防火墙

2.(5)核心交换机（或 B 或设备③）

本题考查园区网络部署的基本知识。要求考生结合自己掌握的传输介质、网络设备、服务器等知识，根据实际项目需求，完成网络部署方案的设计。

本问题考查网络设备选型及部署的能力。

由题目给出的需求分析结果及校园网规划要求可知，该网络采用了三层架构部署。由拓扑图 1-2 可知，设备①直接连接 Internet,在可选的四个设备中，在此位置可选择的设备可以是路由器或防火墙，但是由于每个设备只能选择一次，而需求说明中提到“学校信息中心部署服务器，根据需求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务”，所以可以判断设备④应为防火墙，所以设备①应为路由器。由于该网络采用三层架构，所以设备③直接连接多台汇聚交换机，该设备应为核心交换机，剩下的设备②直连在路由器与核心交换机之间，按照需求分析和设备选项，这里应该部署流控服务器。

根据以上分析可知，设备④应为防火墙，由于服务器要对内外网分别提供不同的服务，根据网络拓扑结构，防火墙设备连接在核心交换机上最适合。

【问题 2】

1.根据题目说明和网络拓扑图，在图 1-2 中，介质 1 应选用(6)，介质 2 应选用(7),介质 3 应选用(8).

(6)～(8)备选答案：(注：每项只能选择一次)

A.单模光纤 B.多模光纤

C.6 类双绞线 D. 5 类双绞线

2.根据网络需求分析和网络拓扑结构图，所有接入交换机都直接连接汇聚交换机，本校园网中至少需要(9)台 24 口的接入交换机(不包括服务器使用的交换机)。

1.(6) A 单模光纤(7) C 6 类双绞线(8) B 多模光纤

2.(9) 35

本问题主要考查网络传输介质的选择能力。

由需求分析可知，信息中心部署在图书馆，核心交换机到汇聚交换机以千兆链路聚合，接入交换机千兆到桌面。同时由图 1-1 可知，图书馆到实验楼的距离为 1500 米，所以介质 1 应选择单模光纤；由图 1-2 可知，食堂的接入交换机上联到学生宿舍的汇聚交换机，距离为 170 米，所以介质 3 应选择光纤，而介质 1 必须选择单模光纤，题目要求每项只能选择一次，所以介质 3 应选择多模光纤。介质 2 只剩下 6 类双绞线和 5 类双绞线两个选项，由于需求要求千兆到桌面，所以此处合适的介质只能选择 6 类双绞线

由需求可知，实验楼部署 237 个点，办公楼部署 87 个点，学生宿舍部署 422 个点，食堂部署 17 个点，如果采用 24 口的接入交换机，所有接入交换机都直接连接汇聚交换机，则每个交换机可用 23 个端口，这样实验楼需部署 11 个；办公楼部署 4 个；学生宿舍部署 19 个；食堂部署 1 个；合计 35 个。

【问题 3】

交换机的选型是网络设计的重要工作。而交换机的背板带宽、包转发率、交换容量是其重要技术指标。其中，交换机进行数据包转发的能力称为(10)，交换机端口处理器和数据总线之间单位时间内所能传输的最大数据景称为(11) 。某交换机有 24 个固定的千兆端口，其端口总带宽为(12) Mbps。

(10)包转发率 (11)背板带宽 (12)48000

本问题考查交换机基本参数的知识。,

交换机的选型是网络设计的重要工作。而交换机的背板带宽、包转发率、交换容量是其重要技术指标。

其中，交换机进行数据包转发的能力称为包转发率，也称端口吞吐率，指交换机进行数据包转发的能力，单位为 pps（package per second）。

交换机的背板带宽是指交换机端口处理器和数据总线之间单位时间内所能传输的最大数据量。背板带宽标志了交换机总的交换能力，单位为 Gb/s。一般交换机的背板带宽从几个 Gb/s 到上百个 Gb/s。

交换机所有端口能提供的总带宽的计算公式为：

总带宽=端口数×端口速率×2（全双工模式）

如果某交换机有 24 个固定的千兆端口，其端口总带宽=24×1000×2=48000Mbps

【问题 4】

根据需求分析，图书馆需要支持无线网络接入，其部分交换机需要提供 POE 功能，POE 的标准供电电压值为(13)。

(13)备选答案：

A.5V B.12V C.48V D.110V

(13)C 48V

本问题考查 POE 的基础知识。

POE（Power over Ethernet)称为以太网供电，其可以通过双绞线为以太网提供 48V 的交流电源。

试题二

如图 2-1 所示,某公司办公网络划分为研发部和销售部两个子网,利用一台双网卡 Linux 服务器作为网关，同时在该 Linux 服务器上配置 Apache 提供 Web 服务。

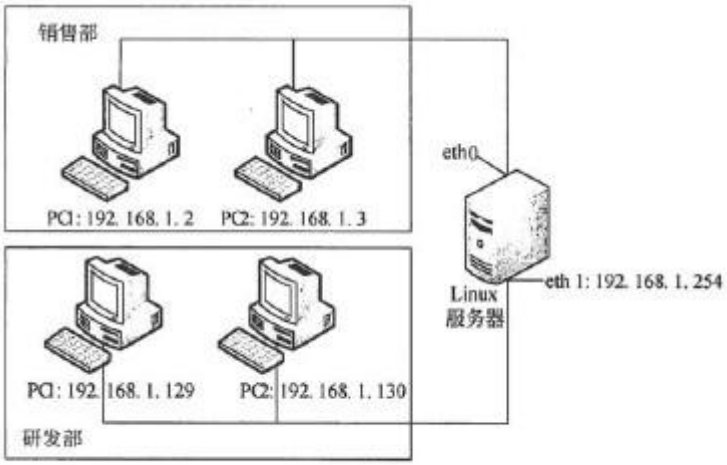


图 2-1

【问题 1】

图 2-2 是 Linux 服务器中网卡 eth0 的配置信息，从图中可以得知：①处输入的命令是(1)，eth0 的 IP 地址是(2),子网掩码是(3),销售部子网最多可以容纳的主机数量是(4)。

```
[root@localhost conf]#____①
eth0      Link encap:Ethernet  HWaddr 00:0C:29:C8:0D:10
          inet addr:192.168.1.126  Bcast:192.168.1.255  Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1667 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:291745 (284.9 Kb)  TX bytes:924 (924.0 b)
          Interrupt:10 Base address:0x10a4
```

图 2-2

(1) ifconfig eth0 或 ifconfig (2) 192.168.1.126

(3)255.255.255.128 (4) 125（答 126 也正确）

本题考查 Linux 服务器相关的配置。

Linux 系统中，采用 ifconfig 命令可以查看网卡的配置信息，ifconfig 命令加上网卡的名称，可以指定需要查看的网卡。

从 eth0 网卡配置信息中可以知道网卡的 IP 地址为 192.168.1.126，子网掩码为 255.255.255.128 从子网掩码可以看出该网段可以容纳的主机数量为126台,如果除去Linux服务器占用的一个地址，则答案为 125 台。

【问题 2】

Linux 服务器配置 Web 服务之前，执行命令[root@root] rpm -qa | grep httpd 的目的是(5). Web 服务器配置完成后，可以用命令(6)来启动 Web 服务。

(5)确认 Apache 软件包是否已经成功安装

(6)service httpd start

Linux 命令 rpm-qa 用于查看系统安全的软件包，如果系统安装了 Apache，就包含 httpd 文件。所以该命令可用来检查 Apache 是否安装成功。

Linux 中启动某服务的命令是 service xxx start。所以用 service httpd start 来启动 Web 服务。

【问题 3】

缺省安装时，Apache 的主配置文件名是(7)，该文件所在目录为(8)。

配置文件中下列配置信息的含义是(9) 。

```
<Directory"/var/www/html/secure">
Allowoverride AuthConfig
Order deny, allow
allow from 192.168.1.2
Deny from all
</Directory>
```

(7)httpd.xonf

(8)/etc/httpd/conf

(9)目录“/var/www/html/secure” 只允许主机 192.168.1.2 访问。

Apache 缺省的主配置文件名是 httpdxonf,该文件所在目录为/etc/httpd/conf。

目录“/var/www/html/secure”的配置信息表明该目录只允许主机 192.168.1.2 访问。

【问题 4】

Apache 的主配置文件中有一行：Listen 192.168.1.126:80，其含义是(10)。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务。在 Linux 服务器中应如何配置，方能使研发部的主机也可以访问 Web 服务。

(10)提供 Web 服务的地址是 192.168.1.126，端口是 80

将 Apache 的主配置文件中配置“Listen 192.168.1.126:80”修改为“Listen 80”，或者增加从研发部网络到销售部网络的路由。

Apache 的主配置文件中有配置项 Listen ip:port 的含义是指定服务在某个 IP 地址和端口上提供。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务，表明研发部无法访问 192.168.1.126 这个 IP 地址，解决方法是增加从研发部网络到销售部网络的路由配置或者更改配置项 Listen ip:port 为不指定 IP 地址，则研发部网络可以通过 192.168.1.254 访问 Web 服务。

试题三

在 Windows Server 2003 中可以采用筛选器来保护 DNS 通信。某网络拓扑结构如图 3-1 所示。WWW 服务器的域名是 www.abc.edu。DNS 服务器上安装 Windows Server 2003 操作系统。

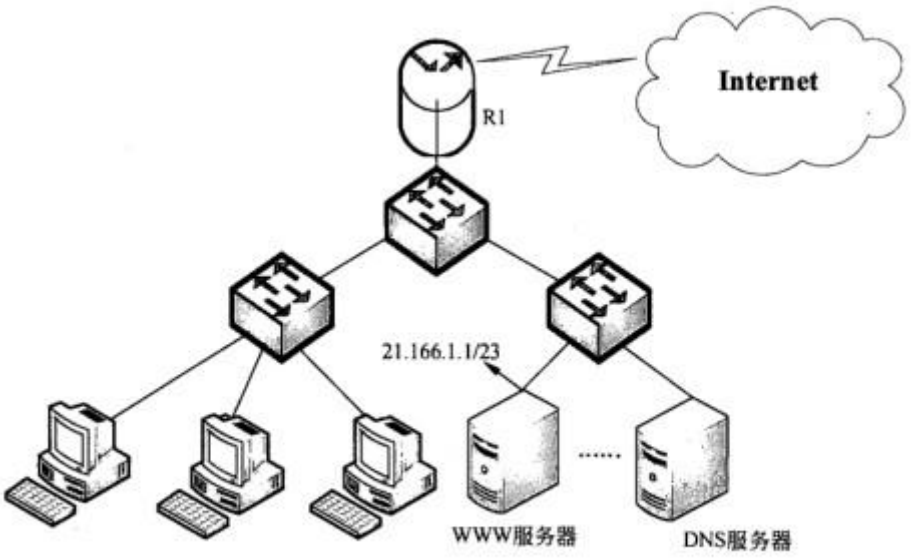


图 3-1

【问题 1】

配置 DNS 服务器时，在图 3-2 所示的对话框中，为 Web Server 配置记录时新建区域的名称是(1);在图 3-3 所示的对话框中，添加的新建主机“名称”为(2)，IP 地址栏应填入(3)。

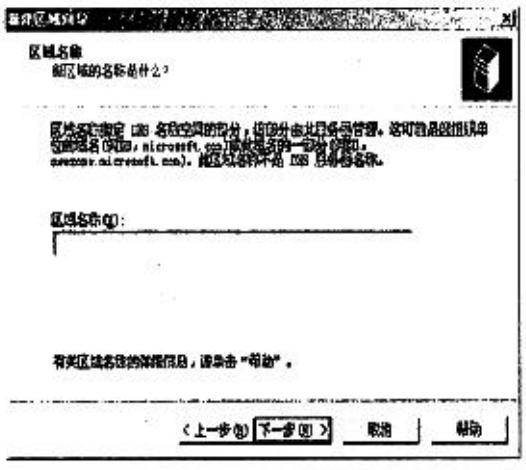


图 3-2

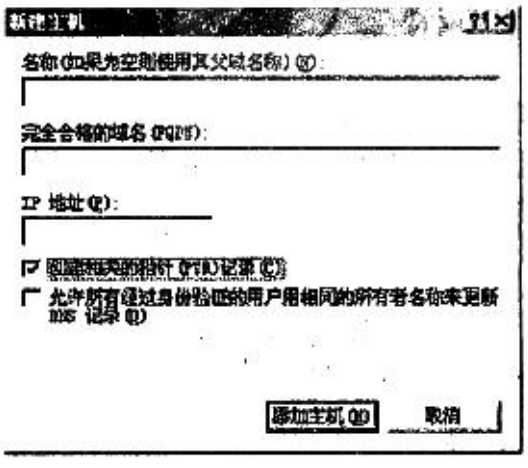


图 3-3

(1) abc.edu (2) www (3) 221.166.1.1

配置 DNS 服务器解析记录时，新建区域即记录主机所在域的名称，主机名称是该域中主机的标识，IP 地址为记录主机的 IP 地址，故(1)～(3)依次应填入 abc.edu.www 和 221.166.1.1。

【问题 2】

在 DNS 服务器的“管理工具”中运行“管理 IP 筛选器列表”，创建一个名为“DNS 输入”的筛选器，用以对客户端发来的 DNS 请求消息进行筛选。在如图 3-4 所示的“IP 筛选器向导”中指定 IP 通信的源地址，下拉框中应选择（4）：在如图 3-5 中指定 IP 通信的目标地址，下拉框中应选择(5).

图 3-4

图 3-5

在图 3-6 中源端口项的设置方式为(6)，目的端口项的设置方式为(7)。在筛选器列表配置完成后，设置“筛选器操作”为“允许”。

图 3-6

（4）任何 IP 地址

（5）我的 IP 地址

（6）点击“从任意端口”

（7）点击“到此端口 ”，文本框中填入“53”

在创建客户端发来的 DNS 请求消息筛选器时，源地址为客户端的 IP 地址，故(4) 处应选“任何 IP 地址”；目标地址处为 DNS 服务器的 IP 地址，故(5)处应选“我的 IP 地址”。源端口项为客户端的端口号，应为任意高端，故(6)处应点击“从任意端口 ”，目的端口项是 DNS 服务的端口号，故设置方式为点击“到此端口”，文本框中填入“53”。

【问题 3】

在图 3-7 中双击“新 IP 安全策略”即可查看“DNS 输入”安全规则，要使规则生效，在图 3-7 中如何配置？

图 3-7

右键单击“新 IP 安全策略”，点击“指派”

要使规则生效，需要对指派规则，故右键单击“新 IP 安全策略”，点击“指派”。

【问题 4】

在本机 Windows 命令行中输入(8)命令可显示当前 DNS 缓存，如图 3-8 所示。“Record Type”字段中的值为 4 时存储的记录是 MX，若“Record Type”字段中的值为 2 时存储的记录是(9)客户端在排除 DNS 域名解析故障时需要刷新 DNS 解析器缓存，使用的命令是(10)。

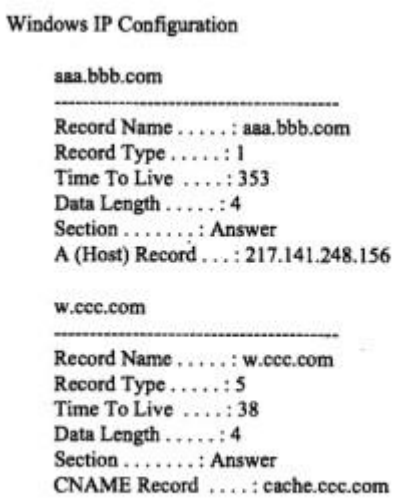


图 3-8

(8)ipconfig/displaydns

(9)IP 地址对应的域名（反向解析）

(10)ipconfig/flushdns

要显示当前 DNS 缓存，可在本机 Windows 命令行中输入 ipconfig/displaydns;若“RecordType”字段中的值为 2 时存储的记录是 IP 地址对应的域名，即反向解析。客户端在排除 DNS 域名解析故障时需要刷新 DNS 解析器缓存，使用的命令是 ipconfig/flushdns。

试题四

某公司网络结构如图 4-1 所示，通过在路由器上配置访问控制列表 ACL 来提高内部网络和 Web 服务器的安全。

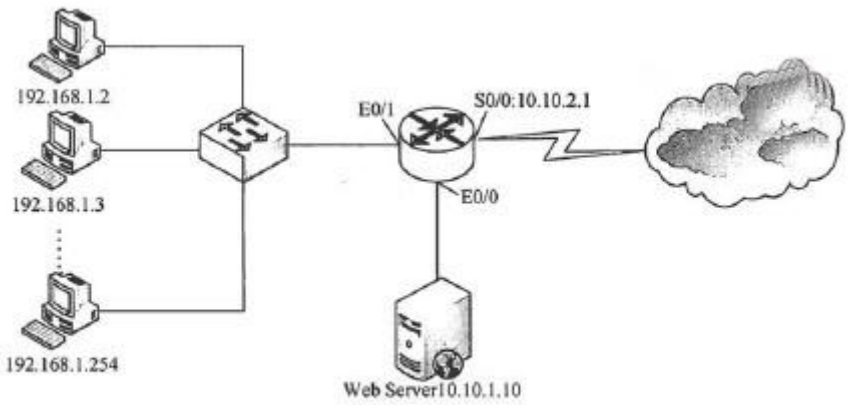


图 4-1

【问题 1】

访问控制列表（ACL)对流入/流出路由器各端口的数据包进行过滤。ACL 按照其功能分为两类，(1)只能根据数据包的源地址进行过滤，(2)可以根据源地址、目的地址以及端口号进行过滤。

(1)标准 ACL (2)扩展 ACL

访问控制列表（ACL)对流入/流出路由器各端口的数据包进行过滤。ACL 按照其功能分为两类，标准 ACL 只能根据数据包的源地址进行过滤，扩展 ACL 可以根据源地址、目的地址以及端口号进行过滤。

【问题 2】

根据图 4-1 的配置，补充完成下面路由器的配置命令：

```
    Router(config)# interface __(3)__
    Router(config-if)#ip address 10.10.1.1  255.255.255.0
    Router(config-if)#no shutdown
    Router(config-if)#exit
    Router(config)# interface __(4)__
    Router(config-if)# ip address 192.168.1.1  255.255.255.0
…
Router(config)# interface __(5)__
    Router(config-if)# ip address 10.10.2.1  255.255.255.0
…
```

(3) ethernet 0/0 (e 0/0) (4) ethernet 0/1 (e0/1) (5) serial 0/0 (s0/0)

根据图 4-1 的配置可知,E0/1 接口对应 192.168.1.1/24 网段,该网段只有地址 192.168.1.1 可用，S0/0 对应的 IP 地址是 10.10.2.1，E0/0 对应 10.10.1.1/24 网段。所以(3)~(5)处应分别填入 e0/0、e0/1、s0/0。

【问题 3】

补充完成下面的 ACL 语句，禁止内网用户 192.168.1.254 访问公司 Web 服务器和外网。

```
Router(config)#access-list 1 deny   (6)
Router(config)#access-list 1 permit  any
Router(config)#interface ethernet 0/1

Router(config-if)#ip access-group 1  (7)
```

(6)192.168.1.254 (7) in

禁止内网用户 192.168.1.254 访问公司 Web 服务器和外网，可以采用标准 ACL 在 E0/1 接口禁止源地址为 192.168.1.254 的包进入路由器接口。所以（6)处应为 192.168.1.254,(7)处应为 in。

【问题 4】

请说明下面这组 ACL 语句的功能。

```
Router(config)#access-list 101 permit tcp any host 10.10.1.10 eq www
Router(config)#interface ethernet 0/0
Router(config-if)#ip access-group 101 out
```

允许任何主机访问公司内部的 Web 服务。

“permit tcp any host 10.10.1.10 eq www”” 为允许任何主机访问 10.10.1.10 的 WWW 服务。

【问题 5】

请在问题 4 的 ACL 前面添加一条语句，使得内网主机 192.168.1.2 可以使用 telnet 对 Web 服务器进行维护。

```
Router(config)#access-list 101  (8)
```

permit tcp host 192.168.1.2 host 10.10.1.10 eq telnet

(host x.x.x.x 可以写成 x.x.x.x 0.0.0.0，telnet 可以写成 23)

扩展 ACL 的语法如下：

```
    access-list 100-199|2000-2699 permit|deny protocol
source_address source_wildcard_mask [protocol_information]
destination_address destination_wildcard_mask [protocol_information] [log]
```

所以内网主机 192.168.1.2 使用 telnet 对 Web 服务器进行维护的 ACL 语句应该为“permit tcp host 192.168.1.2 host 10.10.1.10 eq telnet”。

试题五

某单位在实验室部署了 IPv6 主机，在对现有网络不升级的情况下，计划采用 NAT-PT 方式进行过渡，实现 IPv4 主机与 IPv6 主机之间的通信，其网络结构如图 5-1 所示。其中，IPv6 网络使用的 NAT-PT 前缀是 2001:aaaa:0:0:0:1::/96，IPv6 网络中的任意结点动态映射到地址池 16.23.31.10～16.23.31.20 中的 IPv4 地址。

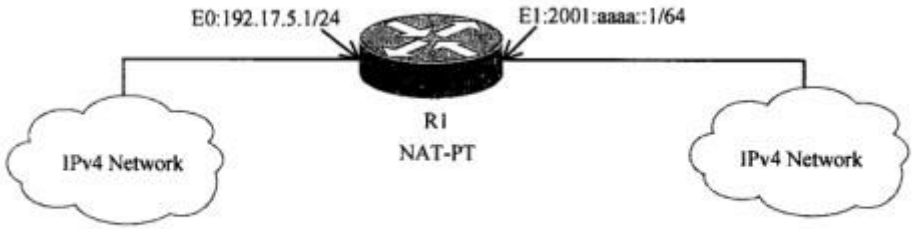


图 5-1

【问题 1】

使用 NAT-PT 方式完成 IPv4 主机与 IPv6 主机通信，需要路由器支持，在路由器上需要配置 DNS-ALG 和 FTP-ALG 这两种常用的应用网关。

没有 DNS-ALG 和 FTP-ALG 的支持，无法实现(1)结点发起的与(2)结点之间的通信。

(1)IPv4 (2) IPv6

本问题考查考生掌握 NAT-PT 的基本知识的能力。

NAT-PT (Network Address Translation-Protocol)网络地址转换协议转换是一种纯 IPv6 结点和 IPv4 结点间的互通方式，所有包括地址、协议在内的转换工作都由网络设备来完成。支持 NAT-PT 的网关路由器应具有 IPv4 地址池，在从 IPv6 向 IPv4 域中转发包时使用，地址池中的地址是用来转换 IPv6 报文中的源地址的。此外网关路由器需要 DNS-ALG 和 FTP-ALG 这两种常用的应用层网关的支持，在 IPv6 结点访问 IPv4 结点时发挥作用。如果没有 DNS-ALG 的支持，只能实现由 IPv6 结点发起的与 IPv4 结点之间的通信，反之则不行。如果没有 FTP-ALG 的支持，IPv4 网络中的主机将不能用 FTP 软件从 IPv6 网络中的服务器上下载文件或者上传文件，反之亦然。

【问题 2】

根据网络拓扑和需求说明，完成（或解释）路由器 R1 的配置

```
R1 # configure terminal                                    ;进入全局配置模式
R1(config) # interface ethernet0                           ;进入端口配置模式
R1(config-if) # ip address  (3)  (4)                       ; 配置端口 IP 地址
R1(config-if) # ipv6 nat                                   ;  (5)
…
R1(config-if) # interface ethernet1
R1(config-if) # ipv6 address  (6) /64
R1(config-if) # ipv6 nat
…
R1(config) #ipv6 access-list ipv6 permit 2001:aaaa::1/64 any    ;  (7)
R1(config) #ipv6 nat prefix  (8)
R1(config) #ipv6 nat v6v4 pool ipv4-pool  (9)  (10)  prefix-length 24
R1(config) #ipv6 nat v6v4 source list ipv6 pool ipv4-pool
R1(config) #exit
```

(3)192.17.5.1　　(4) 255.255.255.0 (5)在接口上启用 NAT-PT

(6)2001:aaaa::1　(7)指定 IPv6 网络中允许被转换的 IPv6 地址范围

(8)2001:aaaa:0:0:0:1::/96 (9) 16.23.31.10 (10) 16.23.31.20

本问题主要考查考生配置 NAT-PT 的能力。

根据题目的描述可知，在该配置中，IPv6 网络使用的 NAT-PT 前缀是 2001:aaaa:0:0:0:1::/96，IPv6 网络中的任意结点动态映射到地址池 16.23.31.10～16.23.31.20 中的 IPv4 地址。具体的端口地址见图 5-1。所以，其配置应为:

```
R1 # configure terminal                                    ; 进入全局配置模式
R1(config) # interface ethernet0                           ; 进入端口配置模式
R1(config-if) # ip address  192.17.5.1  255.255.255.0     ; 配置端口 IP 地址
R1(config-if) # ipv6 nat                                   ; 在接口上启用 NAT-PT
…
R1(config-if) # interface ethernet1
R1(config-if) # ipv6 address 2001:aaaa::1/64
R1(config-if) # ipv6 nat
…
R1(config) #ipv6 access-list ipv6 permit 2001:aaaa::1/64 any;
指定 IPv6 网络中允许被转换的 IPv6 地址范围
R1(config) #ipv6 nat prefix  2001:aaaa:0:0:0:1::/96
R1(config) #ipv6 nat v6v4 pool ipv4-pool  16.23.31.10  16.23.31.20  pref-
ix-length 24
R1(config) #ipv6 nat v6v4 source list ipv6 pool ipv4-pool
R1(config) #exit
```

【问题 3】

NAT-PT 机制定义了三种不同类型的操作，其中，(11)提供一对一的 IPv6 地址和 IPv4 地址的映射：(12)也提供一对一的映射，但是使用一个 IPv4 地址池：(13)提供多个有 NAT-PT 前缀的 IPv6 地址和一个源 IPv4 地址间的多对一动态映射。

(11)静态模式 （12)动态模式

(13)NAPT-PT(网络地址端口转换协议转换)

本问题考查 NAT-PT 机制定义了三种不同类型的操作。

NAT-PT 机制定义的以下不同类型的操作：

静态 NAT-PT:静态模式提供一对一的 IPv6 地址和 IPv4 地址的映射。IPv6 单协议网络内的结点要访问的 IPv4 单协议网络内的每一个 IPv4 地址都必须在 NAT-PT 设备中设置。每一个目的 IPv4 地址在 NAT-PT 设备中被映射为一个具有预定义 NAT-PT 前缀的 IPv6 地址。这种模式中，每一个 IPv6 到 IPv4 映射需要一个源 IPv4 地址。静态 NAT-PT 模式跟 IPv4 中的静态 NAT 类似。

动态 NAT-PT:动态模式也提供一对一的映射，但是使用一个 IPv4 地址池。池中的源 IPv4 地址数量决定了并发的 IPv6 到 IPv4 转换的最大数目》在 IPv6 网络中 IPv6 单协议网络结点动态地把预定义的 NAT-PT 前缀增加到目的 IPv4 地址。这种模式需要一个 IPv4 地址池来执行动态的地址转换，动态 NAT-PT 模式和 IPv4 中的动态 NAT 类似。

NAPT-PT：网络地址端口转换协议转换，NAPT-PT 提供多个有 NAT-PT 前缀的 IPv6 地址和一个源 IPv4 地址间的多对一动态映射。这种转换同时在第 3 层（IPv4/IPv6)和上层（TCP/UDP)进行。NAPT-PT 和 IPv4 中的 PAT 转换类似。