属于 CPU 中算术逻辑单元的部件是(1)。

(1)A.程序计数器　　B.加法器　　C.指令寄存器　　D.指令译码器

【答案】B

【解析】本题考查计算机系统基础知识。

程序计数器、指令寄存器和指令译码器都是 CPU 中控制单元的部件，加法器是算术逻辑运算单元的部件。

内存按字节编址从 A5000H 到 DCFFFH 的区域其存储容量为(2)。

(2)A.123KB　　B.180KB　　C.223KB　　D.224KB

【答案】D

【解析】本题考查计算机系统基础知识。

从地址 A5000H 到 DCFFFH 的存储单元数目为 37FFFH (即 224*1024)个，由于是字节编址，从而得到存储容量为 224KB。

计算机采用分级存储体系的主要目的是为了解决(3)的问题。

(3)A.主存容量不足　　B.存储器读写可靠性

C.外设访问效率　　D.存储容量、成本和速度之间的矛盾

【答案】D

【解析】本题考查计算机系统基础知识。

计算机系统中，高速缓存一般用 SRAM,内存一般用 DRAM,外存一般采用磁存储器。SRAM 的集成度低、速度快、成本高，DRAM 的集成度高，但是需要动态刷新。磁存储器速度慢、容量大，价格便宜。因此，组成分级存储体系来解决存储容量、成本和速度之间的矛盾。

Flynn 分类法基于信息流特征将计算机分成 4 类，其中(4)只有理论意义而无实例。

(4)A.SISD　　B.MISD　　C.SIMD　　D.MIMD

【答案】B

【解析】本题考查计算机系统基础知识。

Flynn 于 1972 年提出计算平台分类法主要根据指令流和数据流来分类，分为四类：

①单指令流单数据流机器（S1SD)

SISD 机器是一种传统的串行计算机，它的硬件不支持任何形式的并行计算，所有的指令都

是串行执行。并且在某个时钟周期内，CPU 只能处理一个数据流。因此这种机器被称作单指令流单数据流机器。早期的计算机都是 SISD 机器。

②单指令流多数据流机器（SIMD)

SIMD 是采用一个指令流处理多个数据流。这类机器在数字信号处理、图像处理，以及多媒体信息处理等领域非常有效。

Intel 处理器实现的 MMXTM、SSE (Streaming SIMD Extensions)、SSE2 及 SSE3 扩展指令集，都能在单个时钟周期内处理多个数据单元。也就是说人们现在用的单核计算机基本上都属于 SIMD 机器。

③多指令流单数据流机器（MISD)

MISD 是采用多个指令流来处理单个数据流。在实际情况中，采用多指令流处理多数据流才是更有效的方法，因此 MISD 只是作为理论模型出现，没有投入实际应用。

④多指令流多数据流机器（MIMD)

MIMD 机器可以同时执行多个指令流，这些指令流分别对不同数据流进行操作。最新的多核计算平台就属于 MIMD 的范畴，例如 Intel 和 AMD 的双核处理器。

以下关于结构化开发方法的叙述中，不正确的是(5)。

(5)A.总的指导思想是自顶向下，逐层分解

B.基本原则是功能的分解与抽象

C.与面向对象开发方法相比，更合适大规模、特别复杂的项目

D.特别适合于数据处理领域的项目

【答案】C

【解析】本题考查结构化开发方法的基础知识。

结构化开发方法由结构化分析、结构化设计和结构化程序设计构成，是一种面向数据流的开发方法。结构化方法总的指导思想是自顶向下、逐层分解，基本原则是功能的分解与抽象。它是软件工程中最早出现的开发方法，特别适合于数据处理领域的问题，但是不适合解决大规模的、特别复杂的项目，而且难以适应需求的变化。

模块 A、B 和 C 都包含相同的 5 个语句，这些语句之间没有联系。为了避免重复，把这 5 个语句抽取出来组成一个模块 D，则模块 D 的内聚类型为(6)内聚。

(6)A.功能　　B.通信　　C.逻辑　　D.巧合

【答案】D

【解析】本题考查软件设计的相关知识。

模块独立性是创建良好设计的一个重要原则，一般采用模块间的耦合和模块的内聚两个准则来进行度量。内聚是指模块内部各元素之间联系的紧密程度，内聚度越高，则模块的独立性越好。内聚性一般有以下几种：

①巧合内聚，指一个模块内的各个处理元素之间没有任何联系。

②逻辑内聚，指模块内执行几个逻辑上相似的功能，通过参数确定该模块完成哪一个功能。

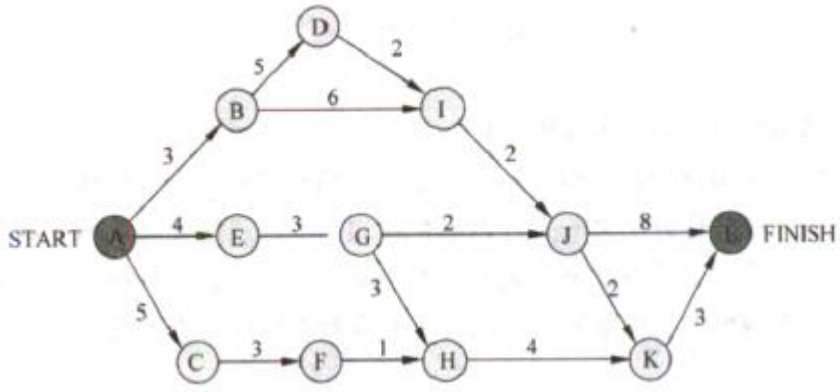
③时间内聚，把需要同时执行的动作组合在一起形成的模块。

④通信内聚，指模块内所有处理元素都在同一个数据结构上操作，或者指各处理使用相同的输入数据或者产生相同的输出数据。

⑤顺序内聚，指一个模块中各个处理元素都密切相关于同一功能且必须顺序执行，前一个功能元素的输出就是下一个功能元素的输入。

⑥功能内聚，是最强的内聚，指模块内所有元素共同完成一个功能，缺一不可。

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示活动，边的权重表示活动的持续时间，则里程碑(7)在关键路径上。活动 GH 的松弛时间是(8)。



(7)A.B　　B.E　　C.C　　D.K

(8)A.0　　B.1　　C.2　　D.3

【答案】A　D

【解析】本题考查活动图的基础知识。

根据关键路径法，计算出关键路径为 A—B—D—I—J—L，其长度为 20。因此里程碑 B 在关键路径上，而里程碑 E、C 和 K 不在关键路径上。包含活动 GH 的最长路径是 A—E—G—H—K—L,长度为 17，因此该活动的松弛时间为 20-17=3。

将高级语言源程序翻译成机器语言程序的过程中，常引入中间代码。以下关于中间代码的叙述中，不正确的是(9)。

(9)A.中间代码不依赖于具体的机器　　B.使用中间代码可提高编译程序的可移植性

C.中间代码可以用树或图表示　　D.中间代码可以用栈或队列表示

【答案】D

【解析】本题考查程序语言基础知识。

从原理上讲，对源程序进行语义分析之后就可以直接生成目标代码，但由于源程序与目标代码的逻辑结构往往差别很大，特别是考虑到具体机器指令系统的特点，要使翻译一次到位很困难，而且用语法制导方式机械生成的目标代码往往是烦琐和低效的，因此有必要设计一种中间代码，将源程序首先翻译成中间代码表示形式，以利于进行与机器无关的优化处理。由于中间代码实际上也起着编译器前端和后端分水岭的作用，所以使用中间代码也有助于提高编译程序的可移植性。常用的中间代码有后缀式、三元式、 四元式和树（图）等形式。

甲公司接受乙公司委托开发了一项应用软件，双方没有订立任何书面合同。在此情形下，(10)享有该软件的著作权。

(10)A.甲公司　　B.甲、乙公司共同　　C.乙公司　　D.甲、乙公司均不

【答案】A

【解析】

委托开发软件著作权关系的建立，通常由委托方与受委托方订立合同而成立。委托开发软件关系中，委托方的责任主要是提供资金、设备等物质条件，并不直接参与开发软件的创作开发活动。受托方的主要责任是根据委托合同规定的目标开发出符合条件的软件。关于委托开发软件著作权的归属，《计算机软件保护条例》第十二条规定：“受他人委托开发的软件，其著作权的归属由委托者与受委托者签定书面协议约定，如无书面协议或者在协议中未作明确约定，其著作权属于受委托者。”根据该条的规定，确定委托开发的软件著作权的归属应当掌握两条标准：

①委托开发软件系根据委托方的要求，由委托方与受托方以合同确定的权利和义务的关系而进行开发的软件，因此软件著作权归属应当作为合同的重要条款予以明确约定。对于当事人已经在合同中约定软件著作权归属关系的，如事后发生纠纷，软件著作权的归属仍应当根据委托开发软件的合同来确定。

②对于在委托开发软件活动中，委托者与受委托者没有签定书面协议，或者在协议中未对软件著作权归属作出明确的约定,其软件著作权属于受委托者,即属于实际完成软件的开发者。

思科路由器的内存体系由多种存储设备组成，其中用来存放 IOS 引导程序的是(11)，运行时活动配置文件存放在(12)中。

(11)A.FLASH　　B.ROM　　C.NVRAM　　D.DRAM

(12)A.FLASH　　B.ROM　　C.NVRAM　　D.DRAM

【答案】B　D

【解析】

路由器采用了不同类型的内存，各种内存以不同方式支持路由器运行。闪存（Flash）是可读可写的存储器，在系统重新启动或关机之后仍能保存数据。Flash 中存放着当前使用的 IOS。如果 Flash 容量足够大，甚至可以存放多个操作系统，这在 IOS 升级时十分有用。当不知道新版 IOS 是否稳定时，可在升级后仍保留旧版 IOS，当出现问题时可退回到旧版操作系统，从而避免长时间的网路故障。

只读存储器 ROM 在路由器中与在计算机中的功能相似，用于系统初始化等。ROM 中包含：系统加电自检代码 POST,用于检测路由器中各种硬件是否完好；系统引导代码（Bootstrap）用于启动路由器并载入 IOS 操作系统；备份的 IOS 操作系统，以便在原有 IOS 操作系统被删除或破坏时使用,通常这个 IOS 比现运行 IOS 的版本低一些,但却足以使路由器启动和工作。

非易失性 RAM (Nonvolatile RAM)是可读可写的存储器，在系统重启或关机之后仍能保存数据。NVRAM 速度较快，成本也较高。NVRAM 仅用于保存启动配置文件 (Startup-Config)，故其容量较小，通常在路由器中只配置 32KB～128KB 的 NVRAM。

动态随机存储器 DRAM 也是可读可写的存储器，但是存储的内容在系统重启或关机后会被清除。RAM 的存取速度比上面 3 种存储器都快。路由器运行时，RAM 中存储路由表、ARP 缓冲区、运行日志和排队等待发送的分组，还包括运行配置文件 (Running-config),正在执行的代码、IOS 操作系统程序和一些临时数据等信息。

下面的广域网络中属于电路交换网络的是(13)。

(13)A.ADSL　　B.X.25　　C.FRN　　D.ATM

【答案】A

【解析】

ADSL 用于连接公共交换电话网 PSTN。PSTN 属于电路交换网，所以 ADSL 是电路交换网的一部分。X.25、FRN 和 ATM 都是分组交换网。

PCM 编码是把模拟信号数字化的过程，通常模拟话音信道的带宽是 4000Hz，则在数字化时采样频率至少为(14)次/秒。

(14)A.2000　　B.4000　　C.8000　　D.16000

【答案】C

【解析】

将模拟信号（例如声音、图像等）变换成数字信号，经传输到达接收端再还原为模拟信号，这种技术叫做脉冲编码调制（Pulse Code Modulation, PCM)技术。PCM 主要经过 3 个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续、幅度连续的模拟信号变换为时间离散、幅度连续的采样信号；量化过程将采样信号变为时间离散、幅度离散的数字信号；编码过程将最化后的离散信号编码为二进制码组。采样频率决定了可恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即

$$f=\frac{1}{T}>2f_{max}$$

其中 f 为采样频率，T 为采样周期，fmax 为信号的最高频率。通常模拟话音信道的带宽（即最高频率）是 4000Hz，所以在数字化时采样频率至少为 8000 次/秒。

设信道带宽为 4000Hz，信噪比为 30dB，按照香农定理，信道容量为(15)。

(15)A.4kb/s　　B.1.6kb/s　　C.40kb/s　　D.120kb/s

【答案】C

【解析】

尼奎斯特定理指出：若信道带宽为 W,则最大码元速率为

B=2W (Baud)

这是由信道的物理特性决定的，是在无噪声的理想情况下的极限值。实际信道会受到各种噪声的干扰，因而达不到按尼奎斯特定理计算出的数据传送速率。香农（Shannon）的研究表明，有噪声信道的极限数据速率可由下面的公式计算：

$$C = W\log_2(1+\frac{S}{N})$$

这个公式叫做香农定理。其中，w 为信道带宽，S 为信号的平均功率，N 为噪声的平均功率，S/N 叫做信噪比。由于在实际使用中 S 与 N 的比值太大，故常取其分贝数(dB)。分贝与信噪比的关系为 SNRDB=10log10(S/N)，例如当 S/N=1000 时，信噪比为 30dB。这个公式表明，无论用什么方式调制，只要给定了信噪比，则单位时间内可传输的最大信息量就确定了，所以称为信道容景。本题中信道带宽为 4 000Hz，信噪比为 30dB，则最大数据速率为

$$C=4\,000\log_2(1+1\,000)\leqq 4\,000\times 9.97\leqq 40\,000\ b/s=40Kb/s$$

这是极限值，只有理论上的意义。

所谓正交幅度调制是把两个(16)的模拟信号合为一个载波信号。

(16)A.幅度相同相位相差 90°　　B.幅度相同相位相差 180°

C.频率相同相位相差 90°　　D.频率相同相位相差 180°

【答案】A

【解析】

正交幅度调制（Quadrature Amplitude Modulation，QAM)是把两个幅度相同但相位相差 90 的模拟信号合成为一个载波信号，经过信道编码后把数据组合映射到星座图上。如下图所示。

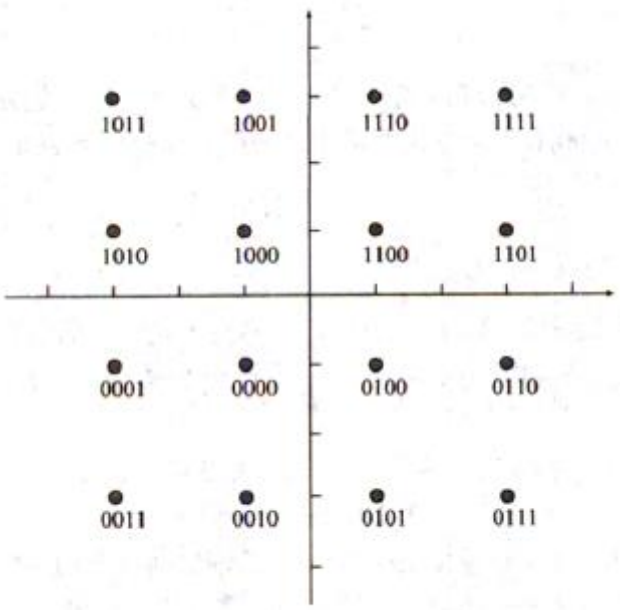


图　QAM 调制

QAM 调制实际上是幅度调制和相位调制的组合，同时利用了载波的幅度和相位来传递数

据信息。与单纯的PSK调制相比，在最小距离相同的条件下，QAM星座图中可以容纳更多的载波码点，可以实现更高的频带利用率。

电信运营商提供的ISDN服务有两种不同的接口，其中供小型企业和家庭使用的基本速率接口(BRI)可提供的最大数据速率为(17)，供大型企业使用的主速率接口(PRJ)可提供的最大数据速率为(18)。

(17)A.128kb/s　　B.144kb/s　　C.1024kb/s　　D.2048kb/s

(18)A.128kb/s　　B.144kb/s　　C.1024kb/s　　D.2048kb/s

【答案】B　D

【解析】

ISDN 分为窄带 ISDN (Narrowband ISDN, N-ISDN)和宽带 ISDN (Broadband ISDN, B-ISDN)。 N-ISDN的目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一个网络上统一传输。ISDN系统提供两种用户接口：即基本速率2B+D和基群速率30B+D。所谓B信道是64kb/s的话音或数据信道，而D信道是16kb/s或64kb/s的信令信道。对于家庭用户，通信公司在用户住所安装一个第一类网络终接设备NT1。用户可以在连接NT1的总线上最多挂接8台设备，共享2B+D的144kb/s信道。大型商业用户则要通过第二类网络终接设备NT2连接ISDN,这种接入方式可以提供30B+D (2.048Mb/s)的接口速率。

PPP是连接广域网的一种封装协议，下面关于PPP的描述中错误的是(19)。

(19)A.能够控制数据链路的建立　　B.能够分配和管理广域网的IP地址

C.只能采用IP作为网络层协议　　D.能够有效地进行错误检测

【答案】C

【解析】

点对点协议应用在许多场合，例如家庭用户拨号上网，或者局域网通过租用公网专线远程联网等。常用的点对点协议是PPP协议（Point-to-Point Protocol)。事实上，PPP是一组协议，其中包括：

链路控制协议LCP (Link Control Protocol),用于建立、释放和测试数据链路，以及协商数据链路参数；

网络控制协议NCP (Network Control Protocol)，用于协商网络层参数，例如动态分配IP地址等；

身份认证协议，用于通信双方确认对方的链路标识。

PPP 帧的封装格式（如下图所示）类似于 HDLC。

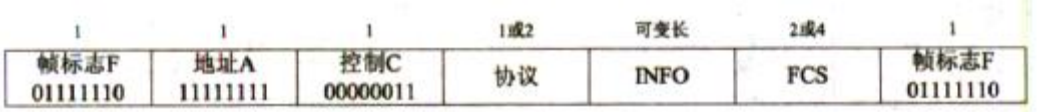


图　PPP 的帧结构

PPP 的地址字段为全 1，表示广播地址。控制字段取值 0x03,表示无编号帧。PPP 的协议字段用于标识信息字段(INFO)中封装的数据报。PPP 可以支持任何网络层协议，例如 IP、IPX, AppleTalk、OSI CLNP、XNS 等。PPP 的负载（INFO)长度默认为 1500 个字节。校验和（FCS)长度是可协商的，可以使用 16 位或 32 位的校验码。

下面关于帧中继的描述中错误的是(20)，思科路由器支持的帧中继本地管理接口类型(Lmi-type)不包括(21)。

(20)A.在第三层建立虚电路

B.提供面向连接的服务

C.是一种高效率的数据链路技术

D.充分利用了光纤通信和数字网络技术的优势

(21)A.Cisco　　B.DCE　　C.ANSI　　D.Q933A

【答案】A　B

【解析】

帧中继（Frame Relay, FR)网络运行在 OSI 参考模型的物理层和数据链路层。FR 用第二层的帧承载数据业务，因而第三层被省掉了。帧中继提供面向连接的服务，在互相通信的每对设备之间都存在一条定义好的虚电路，并且指定了一个链路识别码 DLCI。 帧中继利用了光纤通信和数字网络技术的优势，FR 帧层操作比 HDLC 简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。所以，帧中继比 X.25 具有更高的传输效率。

普通路由器就可以配置成帧中继交换机。在路由器串行接口配置 FR 封装的命令如下表所示，可设置的本地管理接口类型有 3 种{ansi | cisco | q933a}

命　令	功　能
encapsulation frame-relay[ietf]	设置 Frame Relay 封装
frame-relay lmi-type {ansi | cisco | q933a}	设置 Frame Relay LMI 类型
interface interface-type interface-number subinterface-number [multipoint|point-to-point]	设置子接口
frame-relay map protocol protocol-address dlci [broadcast]	映射协议地址与 DLCI
frame-relay interface-dlci dlci [broadcast]	设置 FR DLCI 编号

边界网关协议 BGP4 被称为路径矢量协议，它传送的路由信息是由一个地址前缀后跟(22)组成。这种协议的优点是(23)。

(22)A.一串 IP 地址　　B.一串自治系统编号　C.一串路由器编号　　D.一串子网地址

(23)A.防止域间路由循环　　B.可以及时更新路由

C.便于发现最短通路　　D.考虑了多种路由度量因素

【答案】B　A

【解析】

边界网管协议 BGP 是应用于自治系统（AS)之间的外部网关协议。BGP4 基本上是一个距离矢童路由协议，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域小通信费用，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域短路径（由 AS 编号的列表组成)。所以 BGP4 被称为路径矢量协议。

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路径列表中。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。

BGP4 支持无类别的域间路由（CIDR)，BGP 邻居之间通过 TCP 连接端口 179 交换路由信息。这意味着 BGP4 可以利用 TCP 连接的差错和流量控制功能。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。

与 RIPv2 相比，IGRP 协议增加了一些新的特性，下面的描述中错误的是(24)。

(24)A.路由度量不再把跳步数作为唯一因素，还包含了带宽、延迟等参数

B.增加触发更新来加快路由收敛，不必等待更新周期结束再发送更新报文

C.不但支持相等费用负载均衡，而且支持不等费用的负载均衡

D.最大跳步数由 15 跳扩大到 255 跳，可以支持更大的网络

【答案】B

【解析】

内部网关路由协议（Interior Gateway Routing Protocol, IGRP)是 Cisco 公司 1980 年代设计的一种动态距离矢量路由协议。它组合了网络配置的各种因素，包括带宽、延迟、可靠性和负载等作为路由度量。它支持相等费用通路负载均衡和不等费用通路负载均衡。IGRP 的最大跳步数由 15 跳扩大到 255 跳，可以支持比 RIPv2 更大的网络。

默认情况下，IGRP 每 90s 发送一次路由更新广播，在 3 个更新周期内（即 270s）没有从某个路由器接收到更新报文，则宣布该路由不可访问。在 7 个更新周期即 630s 后，IOS 从路由表中清除该路由表项。

用触发更新来加快路由收敛，这是 RIPv2 和 IGRP 都有的功能。

为了解决 RIP 协议形成路由环路的问题可以采用多种方法，下面列出的方法中效果最好的是(25)。

(25)A.不要把从一个邻居学习到的路由发送给那个邻居

B.经常检查邻居路由器的状态，以便及时发现断开的链路

C.把从邻居学习到的路由设置为无限大，然后发送给那个邻居

D.缩短路由更新周期，以便出现链路失效时尽快达到路由无限大

【答案】C

【解析】

距离矢量法算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路（RoutingLoops),使得各个路由器无法就网络的可到达性取得一致。

解决路由环路问题可以采用水平分割法（Split Horizon)。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。如果每一条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。

简单的水平分割方案是:“不能把从邻居学习到的路由发送给那个邻居”，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse)是:“把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居”。采用反向毒化的方案更安全一些，可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

另外，触发更新技术也能加快路由收敛，如果触发更新足够及时，则也可以防止环路的形成。

城域以太网在各个用户以太网之间建立多点第二层连接，IEEE 802.1ah 定义的运营商主干网桥协议提供的基本技术是在用户以太帧中再封装一层(26)，这种技术被称为(27)技术。

(26)A.运营商的 MAC 帧头　　B.运营商的 VLAN 标记

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　D

【解析】

城域以太网论坛（MEF)定义的 IEEE802.1ad 标准提出了运营商主干网桥（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-V1D)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。

按照 802.1ah 协议，主干网与用户网具有不同的地址空间。主干网的核心交换机只处理通常的以太网帧头，仅主干网边界交换机才具有 PBB 功能。这样，用户网和主干网被 PBB 隔离，使得扁平式的以太网变成了层次化结构，简化了网络管理，保证了网络安全。802.1ah 协议规定的服务标识（I-SID)字段为 24 位，可以区分 1600 万种不同的服务，使得网络的扩展性得以提升。由于采用了二层技术，没有复杂的信令机制，因此设备成本和维护成本较低，被认为是城域以太网的最终解决方案。IEEE 802.1ah 与其他局域网协议的关系参见下阁。

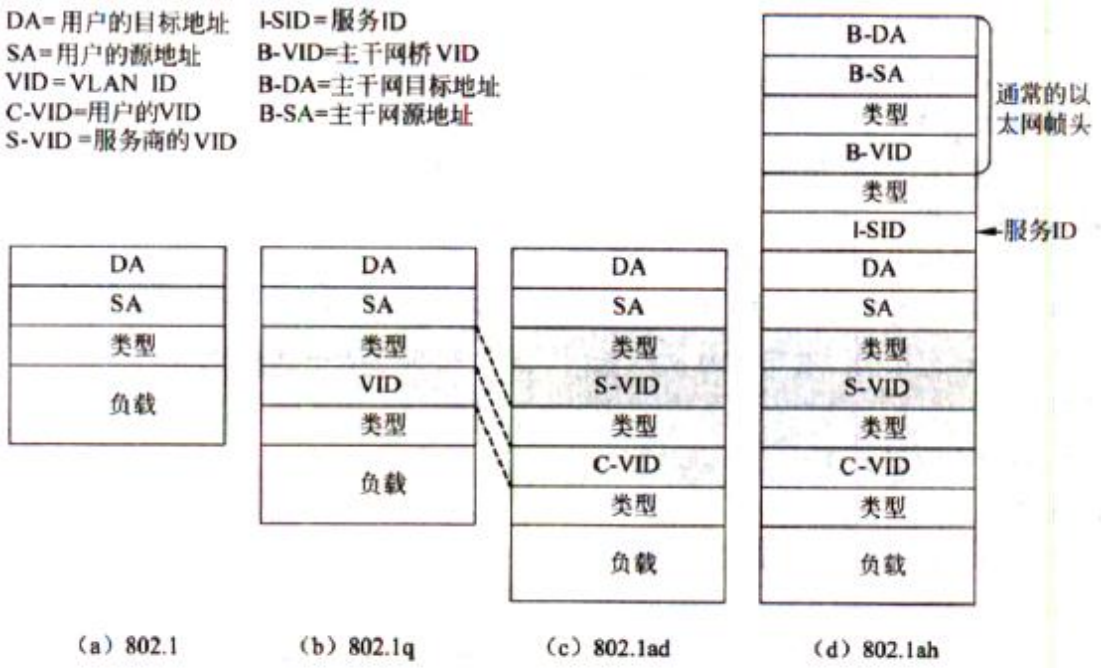
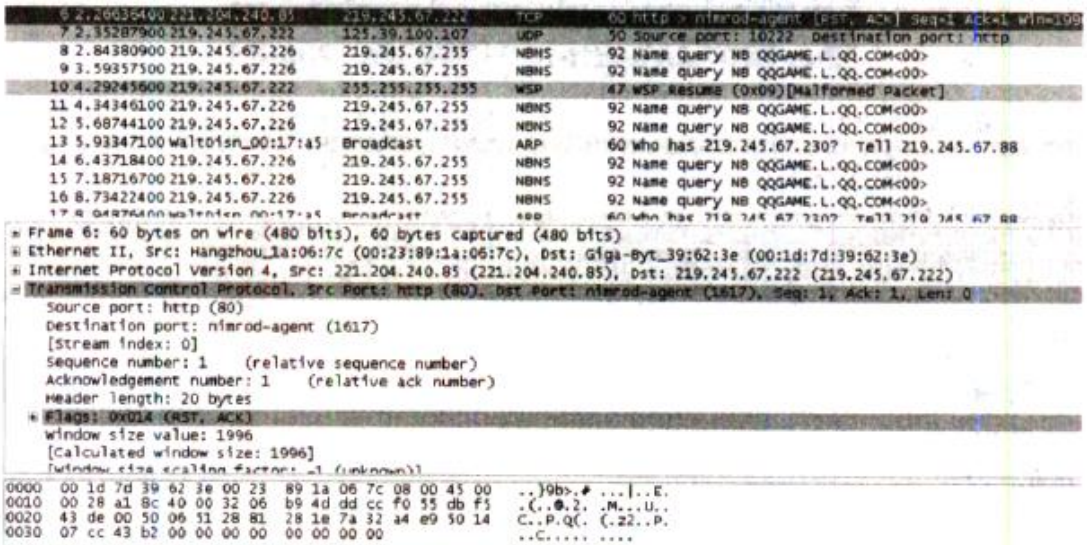


图 城域以太网的帧格式

采用抓包工具截获的结果如下图所示。图中数据包标号(No.)为“6”的条目记录显示的是(28)。该报文由(29)发出。



(28)A.TCP 错误连接响应报文　　B.TCP 连接建立请求报文

C.TCP 连接建立响应报文　　D.Urgent 紧急报文

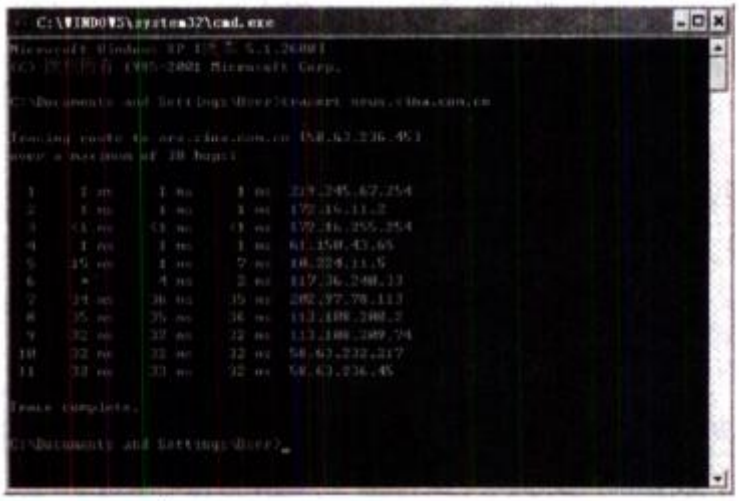
(29)A.Web 客户端　　B.Web 服务器　　C.DNS 服务器　　D.DNS 客户端

【答案】A　B

【解析】本题考查网络管理工具的应用及 TCP 协议原理。

从图中的标志字段为 RST 和 ACK 可以看出，该报文为 TCP 连接出现错误，并进行捎带应答。该记录的源端口号为 80,表明发出报文的是 Web 服务器端。

在 Windows 命令行窗口中键入 tracert 命令，得到如下图所示的窗口，则该 PC 的 IP 地址可能为(30)。



(30)A.172.16.11.13　　B.113.108.208.1　　C.219.245.67.5　　D.58.63.236.45

【答案】C

【解析】本题考查网络管理命令及其含义。

tracert 命令查看的是从本机出发到目的主机时经过的所有路由器及三个延迟时间。第 1 条记录是本机的网关，主机应与网关在一个网段。

管理员为某台 Linux 系统中的/etc/hosts 文件添加了如下记录，下列说法中正确的是(31)。

127.0.0.1 localhost.localdomain localhost

192.168.1.100 linumu100.com web80

192.168.1.120 emailserver

(31)A.linumu100.com 是主机 192.168.1.100 的主机名

B.web80 是主机 192.168.1.100 的主机名

C.emailserver 是主机 192.165.1.120 的别名

D.192.168.1.120 行记录的格式是错误的

【答案】A

【解析】本题考查 Linux 文件系统的基础知识。

Linux 文件系统中的/etc/hosts 文件包含了 IP 地址和主机名之间的映射关系，包括系统的别名（可以没有），记录的顺序为：

IP 地址 主机名 别名

下列关于 Linux 文件组织方式的说法中，(32)是错误的。

(32)A.Linux 文件系统使用索引节点来记录文件信息

B.文件索引节点号由管理员手工分配

C.每个文件与唯一的索引节点号对应

D.一个索引节点号可对应多个文件

【答案】B

【解析】本题考查 Linux 文件系统的基础知识。

Linux 文件系统使用索引节点来记录文件信息，作用与 Windows 的文件分配表类似。索引节点是一个数据结构，它包含了一个文件的文件名、位置、大小、建立或修改时间、访问权限、所属关系等文件控制信息。一个文件系统维护了一个索引节点的数组，每个文件或目录都与索引节点数组中的唯一一个元素对应。系统为每个索引节点分配了一个号码，也就是该节点在数组中的索引号，称为索引节点号。

Linux 文件系统将文件索引节点号和文件名同时保存在目录中。所以，目录只是将文件的名称和它的索引节点号结合在一起的一张表，目录中每一对文件名称和索引节点号称为一个连接。对于每个文件都有一个唯一的索引节点号与之对应，而对于一个索引节点号，却可以有多个文件名与之对应。因此，在磁盘上的同一个文件可以通过不同的路径去访问它。

netstat-r 命令的功能是(33)。

(33)A.显示路由记录　　B.查看连通性　C.追踪 DNS 服务器　　D.捕获网络配置信息

【答案】A

【解析】本试题考查网络管理命令及其含义。

netstat -r 命令的功能是显示路由记录。

搭建试验平台、进行网络仿真是网络生命周期中(34)阶段的任务。

(34)A.需求规范　　B.逻辑网络设计　　C.物理网络设计　　D.实施

【答案】B

【解析】本题考查网络生命周期。

逻辑网络设计的任务包括搭建试验平台、进行网络仿真。

在 Windows 系统中可通过停止(35)服务器来阻止对域名解析 Cache 的访问。

(35)A.DNS Server　　B.Remote Procedure Call (RPC.

C.Ns lookup　　D.DNS Client

【答案】D

【解析】本题考查网络操作系统及服务器配置。

DNS Client 是一个访问本地域名解析 Cache 的组件。

某公司域名为 pq.com，其 POP 服务器的域名为 pop.pq.com，SMTP 服务器的域名为要 smtp.pq.com，配置 Foxmail 邮件客户端时，在发送邮件服务器栏应该填写(36)，在接收邮件服务器栏应该填写(37)。

(36)A.pop.pq.com　　B.smtp.pq.com　　C.pq.com　　D.pop3.pq.com

(37)A.pop.pq.com　　B.smtp.pq.com　　C.pq.com　　D.pop3.pq.com

【答案】B　A

【解析】本题考查邮件服务器的基础知识。

SMTP 协议和 POP 协议是邮件服务器的两个重要协议。SMTP 协议用于邮件的发送，POP 协议用于邮件的接收。Foxmail 是一种常用的桌面邮件客户端，使用该软件时，需设置相应的发送邮件服务器和接收邮件服务器地址,根据题目所给出的发送邮件服务器和接收邮件服务器地址，试题（36)空白处应填写 smtp.pq.com，试题（37)空白处应填写 pop.pq.com。

在 Linux 操作系统中，采用(38)来搭建 DNS 服务器。

(38)A.Samble　　B.Tomcat　　C.Bind　　D.Apache

【答案】C

【解析】本题考查 Linux 系统下应用服务器的基础知识.

Tomcat 是 Apache 软件基金会（Apache Software Foundation)的 Jakarta 项目中的一个核心项目，由 Apache、Sun 和其他一些公司及个人共同开发而成，成为目前比较流行的 Web 应用服务器。目前最新版本是 8.0。

Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，属于轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用。当在一台机器上配置好 Apache 服务器，可利用它响应 HTML（标准通用标记语言下的一个应用）页面的访问请求。Tomcat 部分是 Apache 服务器的扩展，它独立运行，因此当运行 tomcat 时，它实际上是作为一个与 Apache 独立的进程单独运行的。

BIND (Berkeley Internet Name Daemon)是现今互联网上最常使用的 DNS 服务器软件，使用 BIND 作为服务器软件的 DNS 服务器约占所有 DNS 服务器的九成。BIND 现在由互联网系统协会（Internet Systems Consortium)负责开发与维护。

Apache 是一种广为使用的 Web 服务器软件。它可以运行在几乎所有的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的 Web 服务器端软件。

DNS 服务器的默认端口号是(39)端口。

(39)A.50　　B.51　　C.52　　D.53

【答案】D

【解析】本题考查应用服务器的基础知识。

DNS 是一种在网络上为用户提供从域名向 IP 地址映射的服务。它基于 UDP 运行，使用 53 号端口。

使用(40)命令可以向 FTP 服务器上传文件。

(40)A.get　　B.dir　　C.put　　D.push

【答案】C

【解析】本题考查应用服务器的基础知识。

文件传输协议（File Transfer Protocol，FTP)是在 Internet 中两个远程计算机之间传送文件的协议。该协议允许用户使用 FTP 命令对远程计算机中的文件系统进行操作。通过 FTP 可以传送任意类型、任意大小的文件。FTP 的命令及功能如下。

(1) dir 命令，用来显示 FTP 服务器端有哪些文件可供下载。 .

(2) get 命令，用来从服务器端下载一个文件。

(3) !dir 命令，用来显示客户端当前目录中的文件信息。

(4) put 命令，用来向 FTP 服务器端上传一个文件。

假设有证书发放机构 I1、I2，用户 A 在 I1 获取证书，用户 B 在 I2 获取证书，I1 和 I2 已安全交换了各自的公钥，如果用 I1《A》表示由 I1 颁发给 A 的证书，A 可通过(41)证书获取 B 的公开密钥。

(41)A. I1《I2》I2《B》　　B. I2《B》I1《I2》

C. I1《B》I2《I2》　　D. I2《I2》I2《B》

【答案】A

【解析】本题考查证书认证的基础知识。

两个认证机构相互交换了各自公钥之后，用户可使用已有的公钥，验证另一个机构的证书，并从中获取另一个机构的公钥，然后使用获取的另一个机构公钥对该机构下的用户证书进行验证，并从中得到用户公钥。可用以下关系式表达：

用 I1、I2 表示两个证书颁发机构，用 A 和 B 表示分别从 I1 和 I2 处获取证书的两个用户。用《A》I1《A》表示由 I1 颁发给 A 的证书，关系式如下：I1《I2》I2《B》。

PGP(Pretty Good Privacy)是一种电子邮件加密软件包，它提供数据加密和数字签名两种服务，采用(42)进行身份认证，使用(43)(128 位密钥)进行数据加密，使用(44)进行数据完整性验证。

(42)A. RSA 公钥证书　B. RSA 私钥证书　C. Kerboros 证书　D. DES 私钥证书

(43)A. IDEA　B. RSA　C. DES　D. Difile-Hellman

(44)A. HASH　B. MD5　C. 三重 DES　D. SHA-1

【答案】A　A　B

【解析】本题考查 PGP 加密工具的基础知识。

PGP (Pretty Good Privacy)是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。由于该软件违反了美国的密码产品出口限制，作者被联邦政府进行了 3 年的犯罪调查。今天 PGP 已经成为使用最广泛的电子邮件加密软件。PGP 能够得到广泛应用的原因是：

①能够在各种平台（DOS、Windows、Unix、Macintosh 等）上免费使用，并且得到许多制造商的支持；

②基于比较安全的加密算法（RSA、IDEA、MD5)；

③具有广泛的应用领域，既可用于加密文件，也可用于个人安全通信；

④该软件包不是由政府或标准化组织开发和控制的，这一点对于具有自由倾向的网民特别具有吸引力。

PGP 提供两种服务：数据加密和数字签名。数据加密机制可以应用于本地存储的文件，也可以应用于网络上传输的电子邮件。数字签名机制用于数据源身份认证和报文完整性验证。PGP 使用 RSA 公钥证书进行身份认证，使用 IDEA（128 位密钥）进行数据加密，使用 MD5 进行数据完整性验证。

以下关于 S-HTTP 的描述中，正确的是(45)。

(45)A. S-HTTP 是一种面向报文的安全通信协议，使用 TCP443 端口

B. S-HTTP 所使用的语法和报文格式与 HTTP 相同

C. S-HTTP 也可以写为 HTTPS

D. S-HTTP 的安全基础并非 SSL

【答案】D

【解析】本题考查 S-HTTP 协议的基础知识。

S-HTTP 不是采用 SSL 的安全协议。

把交换机由特权模式转换到全局配置模式使用的命令是(46)。

(46)A. interface f0/1　　B. config terminal　　C. enable　　D. no shutdown

【答案】B

【解析】本题考查交换机的模式转换命令。

交换机一般具有用户模式、特权模式、全局模式、端口模式。在特权模式下输入 config terminal （可简写 conft)命令即可，用户在该模式下可修改交换机的全局配置，如修改主机名等。

在无线局域网中，AP(无线接入点)工作在 OSI 模型的(47)。

(47)A. 物理层　　B. 数据链路层　　C. 网络层　　D. 应用层

【答案】B

【解析】本题考查 AP 的工作模型。

AP 是组建小型无线局域网时最常用的设备。AP 相当于一个连接有线网和无线网的桥梁，工作在数据链路层。其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

利用扩展 ACL 禁止用户通过 telnet 访问子网 202.112.111.0/24 的命令是(48)。

(48)A.access-list 110 deny telnet any 202.112.111.0 0.0.0.255 eq 23

B.access-list 110 denyudp any 202.112.111.0 eq telnet

C.access-list 110 deny tcp any 202.1 12.111.0 0.0.0.255.eq 23

D.access-list 10 deny tcp any 202.112.111.0 255.255.255.0 eq 23

【答案】C

【解析】本题考查 ACL 配置命令的使用。

首先，利用扩展 ACL 可排除 A 和 D 选项；其次 B 选项中使用了 UDP, Telnet 是基于 TCP 协议的，所以 B 选项错误。

以下关于 Windows Server 2003 域管理模式的描述中，正确的是(49)。

(49)A.域间信任关系只能是单向信任

B.单域模型中只有一个主域控制器，其他都为备份域控制器

C.如果域控制器改变目录信息，应把变化的信息复制到其他域控制器

D.只有一个域控制器可以改变目录信息

【答案】C

【解析】本题考查 Windows Server 2003 域管理模式的知识。

域信任关系是一种建立在域间的关系,它使得一个域中的用户可以由另一个域中的域控制器进行验证。在所有域关系中只有两种域，即信任关系域和被信任关系域。在 Windows Server 2003 之间可以建立如下信任关系：传递信任关系、不传递信任关系、单向信任关系、双向信任关系。一个域中可以有任意多个域控制器，但只有一个拥有 FSMO 角色。每个域控制器都可以改变目录信息，并把变化的信息复制到其他域控制器。

SNMPv2 的(50)操作为管理站提供了从被管设备中一次取回一大批数据的能力。

(50)A.GetNextRequest　　B.InformRequest　　C.SetRequest　　D.GetBulkRequest

【答案】D

【解析】本题考查 SNMPv2 的知识。

SNMPv2 增加了一种新的操作类型 GetBulkRequest 操作，能够有效地检索大块的数据，特别是能够有效地检索大块的数据，适合在表中检索多行数据，其为管理站提供了从被管设备中一次取回一批数据的能力。

DNS 服务器中的资源记录分成不同类型，其中指明区域主服务器和管理员邮件地址的是(51)，指明区域邮件服务地址是(52)。

(51)A. SOA 记录　　B. PTR 记录　　C. MX 记录　　D. NS 记录

(52)A. SOA 记录　　B. PTR 记录　　C. MX 记录　　D. NS 记录

【答案】A　C

【解析】

DNS 服务器中的资源记录（Resource Record)分成不同类型，常用类型有（参见表 2)：

①SOA (Start Of Authoritative)：开始授权记录是区域文件的第一条记录，指明区域的主服务器，指明区域管理员的邮件地址，并给出区域复制的有关信息。例如序列号、刷新间隔、有效期和生命周期（TTL)等；

②A (Address)：地址记录表示主机名到 IP 地址的映射；

③PTR (Pointer)：指针记录是 IP 地址到主机名的映射；

④NS (Name Server)：名字服务器记录给出区域的授权服务器；

⑤MX (Mailexchanger)：邮件服务器记录定义了区域的邮件服务器及其优先级；

⑥CNAME：别名记录为正式主机名定义了一个别名（alias)。

表　资源记录

记录类型	说　明	示　例
开始授权（SOA）	指明区域主服务器(primary nameserver) 指明区域管理员的邮件地址，及区域复制信息 序列号 刷新间隔 重试间隔 有效期 TTL	区域 microsoft.com 的主服务器为 ns1.microsoft.com 2003080800　;serial number 172800　;refresh=2d 900　;retry=15m 1209600　;expire=2w 3600　;default TTL=1h
地址（A）	最常用的资源记录 把主机名解析为 IP 地址	compuer1.microsoft.com 被解析为 10.1.1.4
指针（PTR）	用于反向查询的资源记录 把 IP 地址解析为主机名	10.1.1.4 被解析为 compuer1.microsoft.com
名字服务器（NS）	为一个域指定了授权服务器 该域的所有子域也被委派给这个服务器	域 microsoft.com 的授权服务器为 ns2.microsoft.com
邮件服务器（MX）	指明区域的 SMTP 服务器	区域 microsoft.com 的邮件服务器为 mail.microsoft.com
别名（CNAME）	指定主机的别名 把主机名解析为另一个主机名	www.microsoft.com 的别名为 webserver12.microsoft.com

以下地址中属于自动专用 IP 地址(APIPA.的是(53)。

(53)A.224.0.0.1　　B.127.0.0.1　　C.192.168.0.1　　D.169.254.1.15

【答案】D

【解析】

选项中的 4 个地址分别是：224.0.0.1 为组播地址；127.0.0.1 为本地环路地址，用于测试本地 TCP/IP 协议栈是否工作正常；192.168.0.1 为 C 类私网地址；169.254.1.15 域于微软定义的自动专用 IP 地址。在采用动态分配地址的网络中，当出现由于 DHCP 服务 器故障而不能获得自动分配的 IP 地址时，主机自动获得 169.254.0.0 网络中一个互不冲突的地址。

公司得到一个 B 类网络地址块，需要划分成若干个包含 1000 台主机的子网，则可以划分成(54)个子网。

(54)A.100　　B.64　　C.128　　D.500

【答案】B

【解析】

一个 B 类地址块包含 16 位主机地址码，1000 台主机需要 10 位主机地址码，剩余的 6 位可以提供 64 个子网号。

IP 地址 202.117.17.254/22 是什么地址? (55)。

(55)A.网络地址　　B.全局广播地址　　C.主机地址　　D.定向广播地址

【答案】C

【解析】

IP 地址 202.117.17.254/22 的二进制形式是 11001010 01110101 00010001 11111110，其中的黑体部分为网络地址，其他部分为主机地址。由于主机地址部分既不为全 0 (表示网络地址)，也不为全 1 (表示广播地址)，所以它是主机地址。

把下列 8 个地址块 20.15.0.0～20.15.7.0 聚合成一个超级地址块，则得到的网络地址是(56)。

(56)A.20.15.0.0/20　　B.20.15.0.0/21　　C.20.15.0.0/16　　D.20.15.0.0/24

【答案】B

【解析】

8 个地址块 20.15.0.0～20.15.7.0 的二进制形式分别是：

地址块 20.15.0.0 的二进制是：　00010100.00001111.00000000.00000000
地址块 20.15.1.0 的二进制是：　00010100.00001111.00000001.00000000
地址块 20.15.2.0 的二进制是：　00010100.00001111.00000010.00000000
地址块 20.15.3.0 的二进制是：　00010100.00001111.00000011.00000000
地址块 20.15.4.0 的二进制是：　00010100.00001111.00000100.00000000
地址块 20.15.5.0 的二进制是：　00010100.00001111.00000101.00000000
地址块 20.15.6.0 的二进制是：　00010100.00001111.00000110.00000000
地址块 20.15.7.0 的二进制是：　00010100.00001111.00000111.00000000

可见，地址掩码可以设为 21 位，8 个地块组成的超网是 20.15.0.0/21。

每一个访问控制列表(ACL)最后都隐含着一条(57)语句。

(57)A.deny any　　B.deny all　　C.permit any　　D.permit all

【答案】A

【解析】

出于安全性考虑，ACL 的默认动作是拒绝（Implicit Deny)，即在 ACL 中没有找到匹配的语句时分组将被拒绝通过，这相当于在列表最后有一个隐含语句拒绝了所有的通信（deny any)。由此引申出的一条规则是：每一个 ACL 至少要有一条“允许”语句，否则只有“拒绝”语句的 ACL 将丢弃所有的分组。

以下关于访问控制列表的论述中，错误的是(58)。

(58)A.访问控制列表要在路由器全局模式下配置

B.具有严格限制条件的语句应放在访问控制列表的最后

C.每一个有效的访问控制列表至少应包含一条允许语句

D.访问控制列表不能过滤由路由器自己产生的数据

【答案】B

【解析】

当一个分组经过时，路由器按照一定的步骤找出与分组信息匹配的 ACL 语句对其进行处理。路由器自顶向下逐个处理 ACL 语句，首先把第一个语句与分组信息进行比较，如果匹配，则路由器将允许（Permit)或拒绝（Deny)分组通过；如果第一个语句不匹配，则照样处理第

二个语句，直到找出一个匹配的。如果在整个列表中没有发现匹配的语句，则路由器丢弃该分组。于是，可以对 ACL 语句的处理规则总结出以下要点:

①一旦发现匹配的语句，就不再处理列表中的其他语句。

②语句的排列顺序很重要。

③如果整个列表中没有匹配的语句，则分组被丢弃。

需要特别强调 ACL 语句的排列顺序。如果有两条语句，一个拒绝来自某个主机的通信，另一个允许来自该主机的通信，则排在前面的语句将被执行，而排在后面的语句将被忽略。所以在安排 ACL 语句的顺序时要把最特殊的语句排在列表的最前面，而最一般的语句排在列表的最后面，这是 ACL 语句排列的基本原则。例如下面的两条语句组成一个标准 ACL。

access-list 10 permit host 172.16.1.0 0.0.0.255

access-list 10 deny host 172.16.1.1

第一条语句表示允许来自子网 172.16.1.0/24 的所有分组通过，而第二条语句表示拒绝来自主机 172.16.1.1 的通信。如果路由器收到一个源地址为 172.16.1.1 的分组，则首先与第一条语句进行匹配，该分组被允许通过，第二条语句就被忽略了。要达到预想的结果—允许来自除主机 172.16.1.1 之外的、属于子网 172.16.1.0/24 的所有通信，则两条语句的顺序必须互换。

access-list 10 deny host 172.16.1.1

access-list 10 permit host 172.16.1.0 0.0.0.255

可见，列表顶上是特殊性语句，列表底部是一般性语句。

IPv6 的可聚合全球单播地址前缀为(59)，任意播地址的组成是(60)。

(59)A.010　　B.011　　C.001　　D.100

(60)A.子网前缀+全 0　　B.子网前缀+全 1

C.链路本地地址前缀+全 0　　D.链路本地地址前缀+全 1

【答案】C　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。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

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“Pv6 地址/前缀长度”的形式。例如 60 位的地址前缀 12AB00000000CD3,有下列几种合法的表示形式：

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

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

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

IPv6 地址格式前缀的初始分配如下表所示。

表 IPv6 地址的初始分配

分　配	前缀（二进制）	占地址空间的比例
保留	0000 0000	1/256
未分配	0000 000	11/256
为NSAP地址保留	0000 001	1/128
为IPX 地址保留	0000 010	1/128
未分配	0000 011	1/128
未分配	0000 1	1/32
未分配	0001	1/16

续表

分　配	前缀（二进制）	占地址空间的比例
可聚合全球单播地址	001	1/8
未分配	010	1/8
未分配	011	1/8
未分配	100	1/8
未分配	101	1/8
未分配	110	1/8
未分配	1110	1/16
未分配	1111 0	1/32
未分配	1111 10	1/64
未分配	1111 110	1/128
未分配	1111 1110 0	1/512
链路本地单播地址	1111 1110 10	1/1024
站点本地单播地址	1111 1110 11	1/1024
组播地址	1111 1111	1/256

任意播地址仅用做目标地址，且只能分配给路由器。任意播地址是在单播地址空间中分配的。一个子网内的所有路由器接口都被分配了子网-路由器任意播地址。子网-路由器任意播地址必须在子网前缀中进行预定义。为构造一个子网-路由器任意播地址，子网前缀必须固定，其余位置全“0”，见下图。

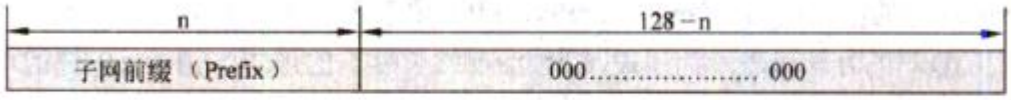


图　子网-路由器任意播地址

如果一个 TCP 连接处于 ESTABUSHED 状态，这是表示(61)。

(61)A.已经发出了连接请求　　B.连接已经建立

C.处于连接监听状态　　D.等待对方的释放连接响应

【答案】B

【解析】

下图所示为 TCP 的连接状态图。事实上，在 TCP 协议运行过程中，有多个连接处于不同的状态。

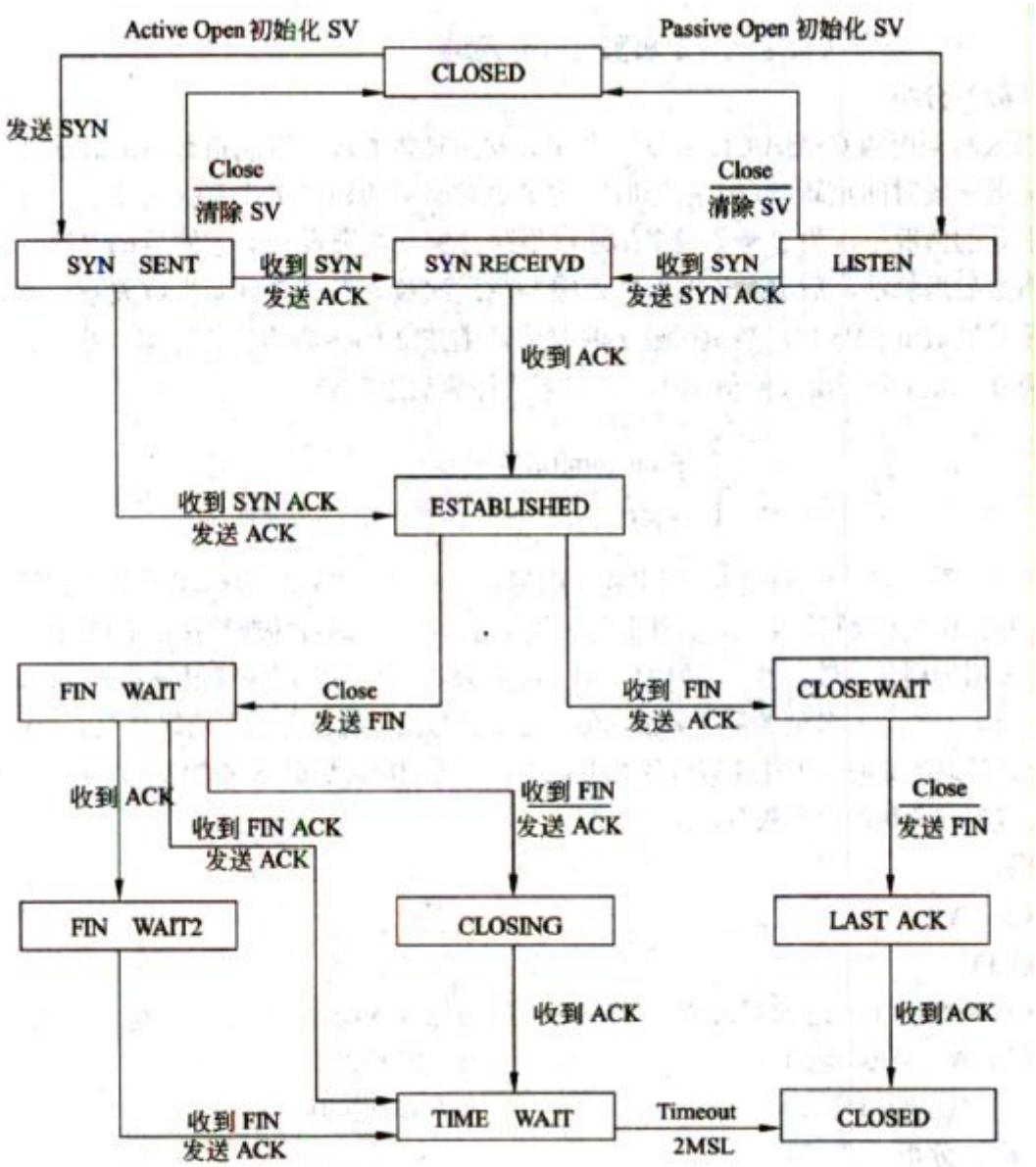


图 TCP 连接状态图

由图可知，如果一个 TCP 连接处于 ESTABLISHED 状态，则表示连接已经建立。

以太网采用的 CSMA/CD 协议，当冲突发生时要通过二进制指数后退算法计算后退时延，关于这个算法，以下论述中错误的是(62)。

(62)A.冲突次数越多，后退的时间越短　　B.平均后退次数的多少与负载大小有关

C.后退时延的平均值与负载大小有关　　D.重发次数达到一定极限后放弃发送

【答案】A

【解析】

以太网采用的 CSMA/CD 协议，当冲突发生时要通过二进制指数后退算法计算后退时延，

退一段时间重新发送。后退时间的多少对网络的稳定工作有很大影响。特别是在负载很重的情况下，为了避免很多站连续发生冲突，需要设计有效的后退算法。按照二进制指数后退算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。或者说，随着重发次数 n 的增加，后退时延t_d的取值范围按 2 的指数增大。即第一次试发送时 n 的值为 0,每冲突一次 n 的值加 1，并按下式计算后退时延。

$$\begin{cases} \xi=\text{random}[0,2^n] \\ t_d=\xi\tau \end{cases}$$

其中，第一式是在区间[0, 2n]中取一均匀分布的随机整数ξ，第二式是计算出随机后退时延。为了避免无限制的重发，要对重发次数 n 进行限制，这种情况往往是信道故障引起的。通常当《增加到某一最大值（例如 16)时，停止发送，并向上层协议报告发送错误。

当然，还可以有其他的后退算法，但二进制指数后退算法考虑了网络负载的变化情况。事实上，后退次数的多少往往与负载大小有关，二进制指数后退算法的优点正是把后退时延的平均取值与负载的大小联系起来了。

在局域网中可动态或静态划分 VLAN，静态划分 VLAN 是根据(63)划分。

(63)A.MAC 地址　　B.IP 地址　　C.端口号　　D.管理区域

【答案】C

【解析】

虚拟局域网 VLAN 是根据管理功能、组织机构或应用类型对交换局域网进行分段而形成的逻辑网络。虚拟局域网与物理局域网具有同样的属性，然而其中的工作站可以不属于同一物理网段。任何交换端口都可以分配给某个 VLAN，属于同一个 VLAN 的所有端口构成一个广播域。每一个 VLAN 是一个逻辑网络，发往 VLAN 之外的分组必须通过路由器进行转发。

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什么地方，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。

以下通信技术中，未在 IEEE802.11 无线局域网中使用的是(64)。

(64)A.FHSS　　B.DSSS　　C.CDMA　　D.IR

【答案】C

【解析】

无线网主要使用 3 种通信技术：红外线、扩展频谱和窄带微波技术。

（1）红外通信

红外线（Infrared Ray, IR)通信技术可以用来建立 WLAN。IR 通信分为 3 种技术:

①定向红外光束：用于点对点链路，可以连接几座大楼中的网络，每幢大楼的路由器或网桥在视距范围内通过 IR 收发器互相连接。

②全方向广播红外线：基站置于天花板上，基站上的发射器向各个方向广播信号，所有终端的 IR 收发器都用定位光束瞄准天花板上的基站，可以接收基站发出的信号，或向基站发送信号。

③漫反射红外线：在这种配置中，所有的发射器都集中瞄准天花板上的一点。红外线射到天花板上后被全方位地漫反射回来，并被房间内所有的接收器接收。

（2）扩展频谱通信

扩展频谱通信技术起源于军事通信网络,其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱（FHSS)，更新的版本是直接序列扩展频谱（DSSS)，这两种技术在 IEEE 802.11 定义的 WLAN 中都有应用。

（3）窄带微波通信

窄带微波（Narrowband Microwave)是指使用微波无线电频带（RF)进行数据传输，其带宽刚好能容纳传输信号。以前所有的窄带微波无线网产品都需要申请许可证，现在已经出现了 ISM 频带内的窄带微波无线网产品。

ZigBee 网络是 IEEE802.15.4 定义的低速无线个人网，其中包含全功能和简单功能两类设备。以下关于这两类设备的描述中，错误的是(65)。

(65)A.协调器是一种全功能设备，只能作为 PAN 的控制器使用

B.被动式红外传感器是一种简单功能设备，接受协调器的控制

C.协调器也可以运行某些应用，发起和接受其他设备的通信请求

D.简单功能设备之间不能互相通信，只能与协调器通信

【答案】A

【解析】

IEEE 802.15.4 标准定义的低速无线个人网（Low Rate-WPAN)包含两类设备：全功能设备（Full-Function Device，FFD)和简单功能设备（Reduced-Function Device，RFD)。 FFD 有 3 种工作模式，可以作为一般的设备、协调器（coordinator)或 PAN 协调器，而 RFD 功能简单，只能作为设备使用，例如电灯开关、被动式红外传感器等。这些设备不需要发送大量的信息，通常接受某个 FFD 的控制。FFD 可以与 RFD 或其他 FFD 通信，而 RFD 只能与 FFD 通信，RFD 之间不能互相通信。

在 IPv4 和 IPv6 混合的网络中，协议翻译技术用于(66)。

(66)A.两个 IPv6 主机通过 IPV4 网络通信

B.两个 IPv4 主机通过 IPv6 网络通信

C.纯 IPv4 主机和纯 IPv6 主机之间的通信

D.两个双协议栈主机之间的通信

【答案】C

【解析】

协议翻译技术用于纯 IPv6 主机与纯 IPv4 主机之间的通信。已经提出了多种翻译方法。例如 REC2765 定义的无状态 IP/ICMP 翻译（Stateless IP/ICMP Translation, SIIT)。这种技术类似于 IPv4 中的 NAT-PT 技术，但它并不是为 IPv6 主机动态地分配 IPv4 地址。SIIT 转换器规范描述了从 IPv6 到 IPv4 的协议转换机制，包括 IP 头的翻译方法以及 ICMP 报文的翻译方法等。当 IPv6 主机发出的分组到达 SIIT 转换器时，IPv6 分组头被翻译为 IPv4 分组头，分组的源地址采用 IPv4 翻译地址，目标地址采用 IPv4 映射地址，然后这 个分组就可以在 IPv4 网络中传送了。

RFC 2766 定义了协议翻译方法 NAT-PT (Network Address Translator - Protocol Translator),也可以用于纯 IPv6 主机与纯 IPv4 主机之间的通信。实现 NAT-PT 技术必须指定一个服务器作为 NAT-PT 网关，并且要准备一个 IPv4 地址块作为地址翻泽之用，要为每个站点至少预留一个 IPv4 地址。与 SIIT 不同，RFC 2766 定义的是有状态的翻译技术，即要记录和保持会话状态，按照会话状态参数对分组进行翻译，包括对 IP 地址及其 相关的字段

（例如 IP、TCP、UDP、ICMP 等）进行翻译。

协议翻译技术适用于 IPv6 孤岛与 IPv4 海洋之间的通信。这种技术要求一次会话中的双向数据包都在同一个路由器上完成转换，所以它只能适用于同一路由器连接的网络。

这种技术的优点是不需要进行 IPv4 和 IPv6 终端的升级改造，只要求在 IPv4 和 IPv6 之间的网络转换设备上启用 NAT-PT 功能就可以了。但是实现这种技术时，一些协议字段在转换时仍不能完全保持原有的含义，并且缺乏端到端的安全性。

结构化布线系统分为六个子系统，其中水平子系统的作用是(67)，园区子系统的作用是(68)。

(67)A.连接各个建筑物中的通信系统

B.连接干线子系统和用户工作区

C.实现中央主配线架与各种不同设备之间的连接

D.实现各楼层设备间子系统之间的互连

(68)A.连接各个建筑物中的通信系统

B.连接干线子系统和用户工作区

C.实现中央主配线架与各种不同设备之间的连接

D.实现各楼层设备间子系统之间的互连

【答案】B　A

【解析】

结构化布线系统分为 6 个子系统。

①工作区子系统（Work Location)

工作区子系统是指从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。

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。

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。

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；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。

网络系统设计过程中，逻辑网络设计阶段的任务是(69)。

(69)A.对现有网络资源进行分析，确定网络的逻辑结构

B.根据需求说明书确定网络的安全系统架构

C.根据需求规范和通信规范，分析各个网段的通信流量

D.根据用户的需求，选择特定的网络技术、网络互连设备和拓扑结构

【答案】D

【解析】

网络的逻辑结构设计来自于用户需求中描述的网络行为和性能等要求。逻辑设计要根据网络用户的分类和分布，选择特定的网络技术，形成特定的网络结构。网络结构大致描述了设备的互联及分布，但是不对具体的物理位置和运行环境进行确定。

下列关于网络汇聚层的描述中，正确的是(70)。

(70)A.要负责收集用户信息，例如用户 IP 地址、访问日志等

B.实现资源访问控制扣流量控制等功能

C.将分组从一个区域高速地转发到另一个区域

D.提供一部分管理功能，例如认证和计费管理等

【答案】B

【解析】

大型局域网可以划分为多个层次，层次化模型中最典型的是三层模型，这种模型允许在三个路由或交换层次上实现流量汇聚和分组过滤功能。三层模型将网络划分为核心层、汇聚层和接入层，每一层都有着特定的作用。核心层提供不同区域之间的最佳路由和高速数据传送；汇聚层将网络业务连接到接入层，并且实施与安全、流量、负载和路由相关的策略；接入层为用户提供了在本地网段访问应用系统的能力，还要解决相邻用户之间的互访需要，接入层要负责一些用户信息（例如用户 IP 地址、MAC 地址和访问 日志等）的收集工作和用户管理功能（包括认证和计费等）。

CDMA for cellular systems can be described as follows. As with FDMA, each cell is allocated a frequency (71), which is split into two part: half for reverse (mobile unit to base station) and half for (72) (base station to mobile unit). For full-duplex (73), a mobile unit uses both reverse and forward channels. Transmission is in the form of direct-sequence spread (74) which uses a chiPPing code to increase the data rate of the transmission, resulting in an increased signal bandwidth. Multiple access is provided by assigning (75) chipping codes to multiple users, so that the receiver can recover the transmission of an individual unit from multiple transmissions.

(71)A.wave	B.signal	C.bandwidth	D.domain
(72)A.forward	B.reverse	C.backward	D.ahead
(73)A.connection	B.transmission	C.compromise	D.communication
(74)A.structure	B.spectrum	C.stream	D.strategy
(75)A.concurrent	B.orhogonal	C.higher	D.lower

【答案】C　A　D　B　B

【解析】

用于蜂窝系统的 CDMA 技术可以描述如下。就像 FDMA一样，每一个小区被分配了一个频带，该频带划分为两半，一半用于反向信道（从移动终端到基站），一半用于正向信道（从基站到移动终端）。在全双工通信中，移动终端使用了反向和正向两个信道。传输以直接序列扩频方式进行，用一个码片来增加传输的数据速率，同时也产生了额外的信号带宽。通过把正交的各个码片指定给不同的用户就可以实现多路访问，这样接收者就能够从多个传输中

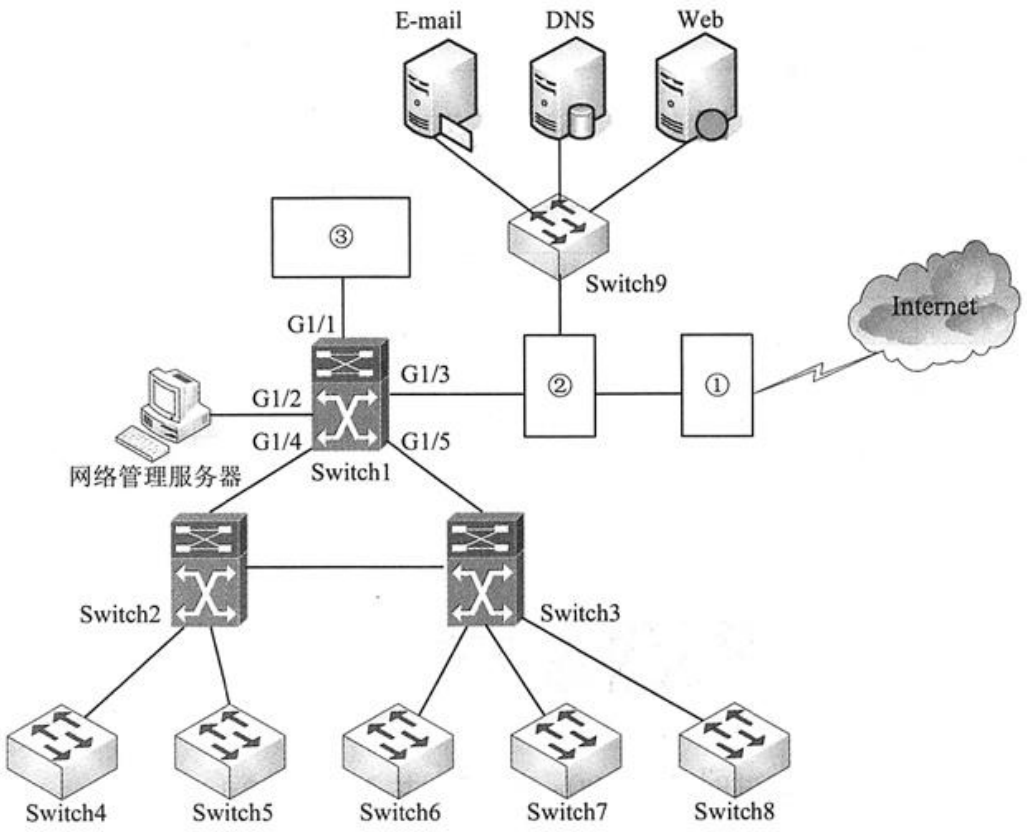
提取并恢复需要的传输单元。

试题一（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】

某企业的网络结构如图 1-1 所示。



某企业网络结构图

【问题 1】

1. 图 1-1 中的网络设备①应为（1），网络设备②应为（2 ），从网络安全的角度出发，Switch9 所组成的网格一般称为（3 ）区。

2. 图 1-1 中③处的网络设备的作用是检测流经内网的信息提供对网络系统的安全保护，该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。网络设备③应为（4），其连接的 Switch1 的 G1/1 端口称为（5 ）端口。这种连接方式一般称为（6）。

【参考答案】

(1)路由器

(2)防火墙或其他具有类似功能的网络安全设备

(3)非军事/DMZ

(4) IPS（入侵防御系统）或 IDS（入侵检测系统）

(5)镜像

(6)旁路方式

【试题解析】

本题考查网络规划设计方面的相关知识。

本问题主要考查网络拓扑结构。

路由器具有广域网互联、隔离广播信息和异构网络互连等能力，是企业网建设和互联网络建设中必不可少的设备。从图中的网络拓扑结构可知，设备（1)处于该企业网和 Internet 之间，因此需要使用路由器进行互联，以实现该企业网路由信息的边界计算网络地址转换等功能。

通常 Internet 是一个不可信任的网络，而企业内部网络要求是一个可信任的网络。 因此设备（2)需要部署防火墙设备，从而保护内部网络资源不会被外部非授权用户使用，防止内部网络受到外部非法用户的攻击。防火墙一般按照防护的区域可分为信任区、非信任区以及 DMZ 区。其中 DMZ 区是为了解决安装防火墙后外部网络不能访问内部网络 服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、Mail 服务器和 DNS 等。另一方面，通过这样一 个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方

案，对攻击者来说又多了一道关卡。

入侵防护系统（IPS)兼有防火墙、IDS 和防病毒等安全组件的特性，当数据包经过时将对其进行过滤检测，以确保该数据包是否含有威胁网络安全的特征。如果检测到一个恶意的数据包，系统不但发出警报，还将采取相应措施阻断攻击。图中设备（3)直接接在交换机 1 的 G1/1 接口上（此接口为镜像端口），用于检测、分析和处理从设备（2) 进入交换机 1 的数据包。根据网络拓扑结构和安全要求的不同，IPS 可以通过旁路接入或者直接串接等方式部署在被检测的网络中。

【问题 2】

1. 随着企业用户的增加，要求部署上网行为管理设备，对用户的上网行为进行安全分析、流量管理、网络访问控制等，以保证正常的上网需求。部署上网行为管理设备的位置应该在图 1-1 中的（7 ）和（8 ）之间比较合理。

2. 网卡的工作模式有直接、广播、多播和混杂四种模式.缺省的工作模式为(9)和(10)。即它只接收广播帧和发给自己的帧。网络管理机在抓包时，需要把网卡置于（11），这时网卡将接受同一子网内所有站点所发送的数据包，这样就可以达到对网络信息监视的目的。

【参考答案】

(7)主交换机或 Switch 1 ——(7)和（8)答案可互换

(8)防火墙或网络设备② ——（7)和（8)答案可互换

(9)广播模式 ——(9)和（10)答案可互换

(10)直接模式 ——(9)和（10)答案可互换

(11)混杂模式

【试题解析】

本问题主要考查上网行为管理设备和网卡的工作模式。

上网行为管理是指帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计和用户行为分析。通过对上网行为管理的需求进行分析，根据图中的网络拓扑结构，可以得出该设备应该部署在交换机 1 和设备（2)之间，这样才能满足企业的要求。

网卡具有如下的四种工作模式：

(1) 广播模式（Broad Cast Model):物理地址（MAC)是 OXffifflf 的帧为广播帧，工作在广播模式的网卡接收广播帧。

(2) 多播传送(MulticastModel):多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是，如果将网片设置为多播传送模式;’它可以接收所有的多播传送帧，而不论它是不是组内成员。

(3) 直接模式（Direct Model):工作在直接模式下的网卡只接收目的地址是自己 Mac 地址的帧。

(4) 混杂模式（Promiscuous Model)：工作在混杂模式下的网卡接收所有的流过网卡的帧，

信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接收同一网络内所有站点所发送的数据包，这样就可以达到对网络信息监视捕获的目的。

【问题 3】

针对图 1-1 中的网络结构，各台交换机需要运行（12)协议.以建立一个无环路的树状网络结构。按照该协议，交换机的默认优先级值为（13)，根交换机是根据（14)来选择的。值小的交换机为根交换机：如果交换机的优先级相同，再比较（15)。当图 1-1 中的 Switch1~Switch3 之间的某条链路出现故障时，为了使阻塞端口直接进入转发状态，从而切换到备份链路上，需要在 Switch1~Switch8 上使用（16)功能。

【参考答案】

(12) STP 或生成树

(13) 32768

(14)网桥 ID

(15) MAC 地址

(16) BackboneFast

【试题解析】

本问题主要考查生成树协议。

生成树协议（STP)是一个数据链路层的协议。其基本原理是通过在交换机之间传递一种特殊的协议报文，网桥协议数据单元(Bridge Protocol Data Unit,简称 BPDU)，来确定网络的拓扑结构。BPDU 有两种:配置 BPDU(Configuration BPDU)和 TCN BPDU，前者是用于计算无环的生成树的,后者则是用于在二层网络拓扑发生变化时产生用来缩短 CAM 表项的刷新时间的（由默认的 300s 缩短为 15s)。Spanning Tree Protocol (STP) 在 IEEE 802.1D 文档中定义。该协议的原理是按照树的结构来构造网络拓扑，消除网络中的环路，避免由于环路的存在而造成广播风暴问题。在该协议中，交换机是根据交换机优先级来选择的，值小的为根交换机。如果相同，再比较 MAC 地址。交换机优先级是一个十进制数，用来在生成树算法中衡量一个交换机的优先度，其值的范围是 0～65535，默认情况下，其值为 32768。

BackboneFast 是对 UplinkFast 的一种补充，UplinkFast 能够检测直连链路的失效，BackboneFast 是用来检测间接链路的失效。当启用了 BackboneFast 的交换机检测到间接链路失效之后，会马上使阻塞的端口进入监听状态，少了 20s 的老化时间。如果要启用 BackboneFast 特性，应该在网络中的所有交换机上都启用。

【问题 4】

根据层次化网络的设计原则，从图 1-1 中可以看出该企业采用由（17）层和（18）层组成的两层架构，其中，MAC 地址过滤和 IP 地址绑定等功能是由（19）完成的，分组的高速转发是由（20）完成的。

【参考答案】

(17) 核心

(18) 接入

(19) Switch4～Switch8 或接入层交换机

(20) Switch 1～Switch3 或核心层交换机

【试题解析】

本问题主要考查网络分层概念。

图中所示的网络拓扑结构采用了核心层和接入层的两层架构理念。其中，由交换机 1～交换机 3 组成核心层，主要完成的功能有：分组的高速转发；汇聚下一层的用户流量，进行数据分组传输的汇聚、转发和交换；根据接入层的用户流量，进行本地路由、数据包过滤、协议转换、流量均衡、QoS 优先级管理以及安全控制、IP 地址转换、流量整型等处理。由交换机 4～交换机 8 组成了接入层，主要完成的功能是：为用户提供了在本地网段访问应用系统的能力，解决相邻用户之间互相访问的需求，并且为这些访问提供足够的带宽；适当地负责部分用户管理功能（如 MAC 层过滤、IP 地址绑定、用户认证、费管理等）；负责部分用户信息收集工作（如用户的 IP 地址、MAC 地址、访问日志等）。

试题二（共 20 分）

阅读下列说明，回答问题 1 至问题 5,将解答填入答题纸的对应栏内。

【说明】

某中学为两个学生课外兴趣小组提供了建立网站的软硬件环境。网站环境的基本配置方案如下：

1. 两个网站配置在同一台服务器上，网站服务由 Win2003 环境下的 IIS6.0 提供；

2. 网站的管理通过 Win2003 的远程桌面实现，并启用 Win2003 的防火墙组件；

3. 为兴趣小组建立各自独立的文件夹作为上传目录和网站的主目录，对用户使用磁盘空间大小进行了设定：

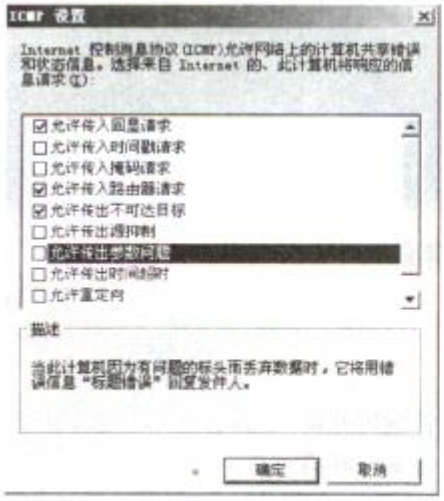


图 2-1

图 2-2

4.通过不同的域名分别访问课外兴趣小组各自的网站。

按照方案，学校的网络工程师安装了 Win2003 服务器。实用 IIS6.0 建立 Web 和 FTP 服务器，配置了远程桌面管理、防火墙，在服务器上为两个课外兴趣小组分配了不同的用户名.进行了初步的权限配置。

【问题 1】

Win 2003 远程桌面服务的默认端口是（1）。对外提供服务使用（2）协议。在图 2-1 中，若要拒绝外部设备 PING 服务器，在防火墙的 ICMP 配置界面上应该如何操作?

【参考答案】

(1) 3389 (2) RDP

不勾选“允许传入回显请求”

【试题解析】

本题考查 Win 2003 服务器配置的相关知识。

远程桌面是方便 Windows 服务器管理员对服务器进行基于图形界面的远程管理的工具。远程桌面是基于 RDP（ Remote Desktop Protocol 远程桌面协议）的多通道（multi-channel）协议，让使用者（所在计算机称为用户端或“本地计算机”）连上提供服务器或“远程计算机”，远程桌面默认使用的端口是 3389。

ICMP 协议是一种用于传输出错报告控制信息，对于网络安全具有极其重要的意义。它是 TCP/IP 协议簇的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标，IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。

【问题 2】

1. 在图 2-2 中，Web 服务扩展选项中“所有未知 CGI 扩展禁止”的含义是什么？
2. 在图 2-2 中，如何配置 Web 服务扩展，网站才能提供对 asp.net 或 asp 程序的支持。

【参考答案】

1. 如果选择允许所有通用网关接口（CGI)在 Web 服务器上运行，则 Web 服务器容易受到使用 CGI 技术的计算机病毒或蠕虫程序的攻击。禁止该扩展意味着除非明确地允许一个应用在 IIS 6.0 上运行，否则它就不能运行。

2. 增加 ASP.NET 模块（启用 ASP.NET 的服务扩展项），网站才能提供对 ASP.NET 的支持。将 Active Server Pages 配置为“允许”，IIS 6.0 即可提供对 ASP 支持。

【试题解析】

如果选择允许所有通用网关接口（CGI)在 Web 服务器上运行，则 Web 服务器容易受到使用 CGI 技术的计算机病毒或蠕虫程序的攻击。禁止该扩展意味着除非明确地允许一个应用在 IIS 6.0 上运行，否则它就不能运行。

要想网站提供对 ASP.NET 或 ASP 程序的支持，必须增加 ASP.NET 模块（启用 ASP.NET 的服务扩展项）。将 Active Server Pages 配置为“允许”，IIS 6.0 即可提供对 ASP 支持。

【问题 3】

在图2-2中,选择IIS管理器中的FTP站点—新建—虚拟目录,分别设置FTP用户与（3 ）、(4)的对应关系。

由于 IIS 内置的 FTP 服务不支持(5)，所以 FTP 用户密码是以明文方式在网络上传输，安全性较弱。

【参考答案】

(3) 别名 （4)目录名 （5) SSL

【试题解析】

FTP (File Transfer Protocol, FTP)是 TCP/IP 网络上两台计算机传送文件的协议，FTP 是在 TCP/IP 网络和 Internet 上最早使用的协议之一，它属于网络协议的应用层。FTP 客户机可以给服务器发出命令来下载文件、上传文件、创建或改变服务器上的目录，FTP 的默认端口是 21。由于 IIS 中的 FTP 服务不支持安全套接字层（SSL)上的 FTP,因此，如果要保证通信的安全性，同时又需要使用 FTP 作为传输协议（相对于在 SSL 上使用 WebDAV 而言），可以考虑在加密通道（如虚拟专用网络）上使用 FTP,此类加密通道通过点对点隧道协议或 IPSec 保证安全性。

【问题 4】

在 IIS6.0 中，每个 Web 站点都具有唯一的，由三部分组成的标识符，用来接收和响应请求，分别是（6 ）、(7)和（8 ）。网络工程师通过点击网站属性—>网站—>高级选项，通过添加（9)的方式在一个 IP 地址上建立多个网站。

【参考答案】

(6) IP 地址 （7)端口号 （8)主机头名 （9)主机头名

【试题解析】

IIS 是一种 Web (网页）服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。IIS6.0 增强了安全性，为了尽量减少系统被攻击的危险，在默认情况下 IIS 6.0 是不会被安装在 Win 2003 中的，管理员需要手动进行安装，IIS 6.0 在被锁定状态中只为静态内容（.htm, .jpg, .bmp

等等）提供服务，通过网络服务扩展节点，网站管理员可根据企业的需求起用或禁止 IIS 功能。

【问题 5】

在(10)文件系统下，为了预防用户无限制的使用磁盘空间，可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是（11)和（12)。

【参考答案】

(10) NTFS (11)磁盘配额限制 (12)磁盘配额警告级别

【试题解析】

在 NTFS 文件系统下，为了预防用户无限制的使用磁盘空间，可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是磁盘配额限制和磁盘配额警告级别。

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】

某企业的网络结构如图 3-1 所示。

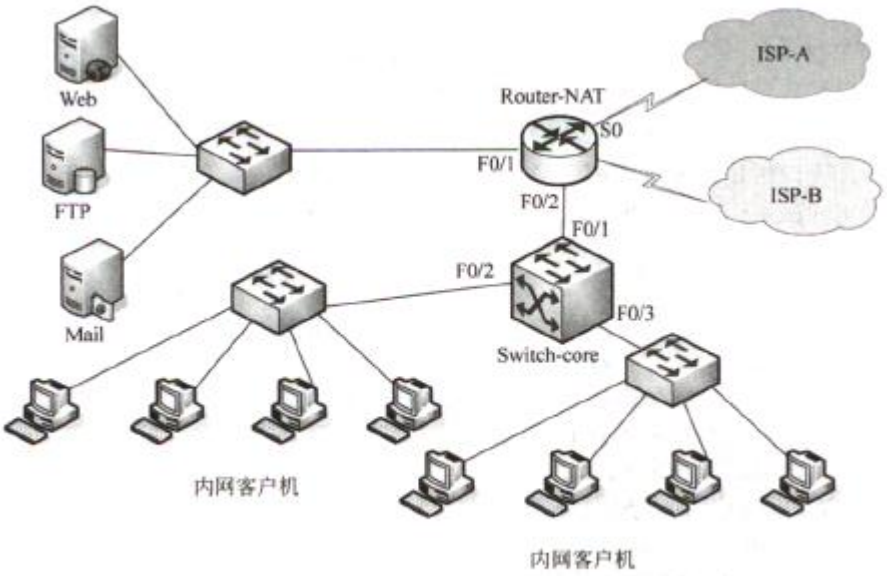


图 3-1　企业网络拓扑结构

按照网络拓扑结构为该企业网络进行网络地址配置，地址分配如表 3-1 所示。

表 3-1　网络地址分配表

设　备	地　址
Router-NAT	F0/1:192.168.1.1/24 S0:61.192.93.100/24 S1:202.102.100.100/24
Web 服务器	192.168.1.100
ISP-A	61.192.93.200/24
ISP-B	202.102.100.200/24
ISP-A 地址池	61.192.93.100~61.192.93.102
ISP-B 地址池	202.102.100.100~202.102.100.102

【问题 1】

企业网络中使用私有地址，如果内网用户要访问互联网，一般使用（1)技术将私有网络地址转换为公网地址。在使用该技术时，往往是用（2)技术指定允许转换的内部主机地址范围。

一般来说，企业内网服务器需要被外部用户访问，就必须对其做地址变换，内部服务器映射的公共地址不能随意更换，需要使用（3)NAT 技术。但是对于企业内部用户来讲，使用一一映射的技术为每个员工配置一个地址很不现实，一般使用（4)NAT 技术以提高管理效率。

【参考答案】

(1) NAT 或网络地址转换

(2) ACL 或访问控制列表

(3) 静态

(4) 动态

【试题解析】

本题考查网络出口 NAT 的双线接入知识。

本问题主要考查 NAT 转换的相关知识。

一般来说，由于企业内网大都使用私有网络地址，私有地址只能在局域网中使用，不能出现在互联网上，那么使用私有地址的内部主机想要访问互联网，就必须使用地址转换技术将其转换为公有地址，也就是说如果内网用户想要访问互联网，就必须使用 NAT 地址转换技术，将私有地址转换为在互联网应用的公有地址。在使用 NAT 地址转换技术时，往往要使用 ACL 技术来指定允许转换的内部主机地址范围。

根据映射的方式，可以将 NAT 技术分为静态 NAT 和动态 NAT。其中，静态 NAT 是手工配置的内部私有地址和外部公共地址的对应关系，除非人工修改，否则不会变化，一般对外发布服务器使用静态 NAT 技术。动态 NAT 是多个内部主机和外部公共地址随机对应的一种方式，主要是通过指定内部允许转换的地址范围和外部允许使用的地址范围，然后对两个范围映射。这样具体外部的一个公共地址被内部哪台主机使用不确定。主要适用于企业内网大量用户的客户端访问外网。

【问题 2】

一般企业用户可能存在于任何一家运营商的网络中，为了确保每个运营商网络中的客户都可以高效地访问本企业所提供的网络服务，企业有必要同时接入多个运营商网络，根据企业网络的拓扑图和网络地址规划表，实现该企业出口的双线接入。

首先，为内网用户配置 NAT 转换，其中以 61.192.93.0/24 代表 ISP-A 所有网段：其次为外网用户访问内网服务器配置 NAT 转换。根据需求，完成以下 Route-NAT 的有关配置命令。

```
...
Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
//定义到达 ISP-A 所有网段的 ACL
Route-Switch(config)#access-list 101 (5) ip any 61.192.93.0 0.0.0.255
Route-Switch(config)#access-list 101 (6)
//定义到达 ISP-B 所有网段的 ACL
Route-Switch(config)#ip nat pool ISP-A (7) netmask 255.255.255.0
//定义访问 ISP-A 的合法地址池
Route-Switch(config)#ip nat pool ISP-B (8) netmask 255.255.255.0
//定义访问 ISP-B 的合法地址池
Route-Switch(config)#ip nat inside source list 100 pool ISP-A overload
Route-Switch(config)#ip nat inside source (9)
//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换
Route-Switch(config)# ip nat inside source static tcp (10) extendable
//为内网 WEB 服务器配置 ISP-A 的静态 NAT 转换
Route-Switch(config)# ip nat inside source static tcp (11) extendable
//为内网 WEB 服务器配置 ISP-B 的静态 NAT 转换
```

【参考答案】

(5) deny

(6) permit ip any 202.102.100.0 0.0.0.255

(7) 61.192.93.100 61.192.93.102

(8) 202.102.100.100 202.102.100.102

(9) list 101 pool ISP-B overload

(10) 192.168.1.100 80 61.192.193.100 80

(11)192.168.1.100 80 202.102.100.100 80

【试题解析】

本问题主要考查 ACL 和 PAT 的相关配置命令。

```
…
Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
//定义到达 ISP-A 所有网段的 ACL
Route-Switch(config)#access-list 101 deny ip any 61.192.93.0 0.0.0.255
Route-Switch(config)#access-list 101 permit ip any any
//定义到达 ISP-B 所有网段的流量
//用的是排除 ISP-A 网段的方式进行定义，可以防止遗漏网段
Route-Switch(config)#ip nat pool ISP-A 61.192.93.100 61.192.93.102 netmask 255.255.255.0
//定义访问 ISP-A 的合法地址池
Route-Switch(config)#ip nat pool ISP-B 202.102.100.100 202.102.100.102 netmask 255.255.255.0
//定义访问 ISP-B 的合法地址池
Route-Switch(config)#ip nat inside source list 100 pool ISP-A overload
Route-Switch(config)#ip nat inside source list 101 pool ISP-B overload
//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换
Route-Switch(config)# ip nat inside source static tcp 192.168.1.100 80 61.192.93.100 80
extendable          //为内网 WEB 服务器配置 ISP-A 的静态 NAT 转换
Route-Switch(config)# ip nat inside source static tcp 192.168.1.100 80 202.102.100.100 80
extendable          //为内网 WEB 服务器配置 ISP-B 的静态 NAT 转换
```

【问题 3】

在路由器的内部和外部接口用 NAT,同时为了确保内网可以访问外部网络。在出口设备配置静态路由。根据需求，完成（或解释）Route-NAT 的部分配背命令。

```
…
Route-Switch(config)#int s0
Route-Switch(config)#_____(12)_____  //指定 NAT 的外部转换接口
Route-Switch(config)#int s1
Route-Switch(config)#_____(13)_____  //指定 NAT 的外部转换接口
Route-Switch(config)#int f0/1
Route-Switch(config)#_____(14)_____  //指定 NAT 的内部转换接口
Route-Switch(config)# _____(15)_____  //配置到达 ISP-A 的流量从 s0 口转发
Route-Switch(config)#_____(16)_____  //配置默认路由指定从 s1 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 s0 120  //_____(17)_____
…
```

【参考答案】

(12) ip nat outside

(13) ip nat outside

(14) ip nat inside

(15) ip route 61.192.93.0 255.255.255.0 s0

(16) ip route 0.0.0.0 0.0.0.0 s1

(17) 配置备份路由，或者配置浮动静态路由

【试题解析】

本问题主要考查 NAT 转换和默认路由的配置命令。

```
…
Route-Switch(config)#int s0                                  //进入 s0 的子接口配置模式
Route-Switch(config)#ip nat outside                          //指定 NAT 的外部转换接口
Route-Switch(config)#int s1                                  //进入 s1 的子接口配置模式
Route-Switch(config)#ip nat outside                          //指定 NAT 的外部转换接口
Route-Switch(config)#int f0/1                                //进入 f0/1 的子接口配置模式
Route-Switch(config)#ip nat inside                           //指定 NAT 的内部转换接口
Route-Switch(config)#ip route 61.192.93.0 255.255.255.0 s0   //配置到达 ISP-A 的流量从 s0 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 s1             //配置默认路由指定从 s1 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 s0 120         //配置备份路由，或者配置浮动静态路由
…
```

【问题 4】

常用的网络流量控制技术除了 ACL（访问控制列表）外还有 QoS(服务质量)。QoS 是网络的一种安全机制，主要用来解决网络延迟和阻塞等问题.它主要有三种工作模式，分别为(18)模型、Integrated service(或综合服务）模型及（19)模型。其中使用比较普遍的方式是（20)模型。

【参考答案】

(18) Best-Effort service 或尽力而为服务

(19) Differentiated service 或区分服务

(20) 区分服务或 Differentiated service

【试题解析】

本问题主要考查网络流量控制技术。

网络畅通是网络建设中的基本要求，但是并非所有的网络流量都应该被转发，为了安全也为了满足部分业务流量的优先服务要求，总有一些流量需要被限制。常用的网络流量控制技术有访问控制列表（ACL)和服务质量（QoS)。QoS 主要有三种工作模式，一是 Best-Effort service（尽力而为的服务模型），是一个单一的服务模型，也是最简单的服务模型。对 Best-Effort 服务模型，网络尽最大的可能性来发送报文。但对延时、可靠性等性能不提供任何保证。Best-Effort 服务模型是网络的缺省服务模型，通过 FIFO（first in first out 先入先出）队列来实现。它适用于绝大多数网络应用，如 FTP、E-Mail 等。 二是 Integrated

service（综合服务模型），它可以满足多种 QoS 需求。该模型使用资源预留协议（RSVP），RSVP 运行在从源端到目的端的每个设备上，可以监视每个流，以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量，为网络提供最细粒度化的服务质量区分。但是 Inter-Serv 模型对设备的要求很高，当网络中的数据流数量很大时，设备的存储和处理能力会遇到很大的压力。Inter-Serv 模型可扩展性很差，难以在 Internet 核心网络实施。三是 Differentiated service(区分服务模型)，Diff-Serv 是一个多服务模型，它可以满足不同的 QoS 需求。与 Int-Serv 不同，它不需要通知网络为每个业务预留资源，区分服务实现简单，扩展性较好，使用较为普遍。

试题四（共 15 分）

阅读以下说明，回答问题 1 和问题 2,将解答填入答题纸对应的解答栏内。

【说明】

某公司网络拓扑结构如图 4-1 所示。公司内部使用 C 类私有 IP 地址.其中公司两个部门分别处于 VLAN10 和 VLAN20，VLAN10 采用 192.168.10.0/24 网段。VLAN20 采用 192.168.20.0/24 网段，每段最后一个地址作为网关地址。

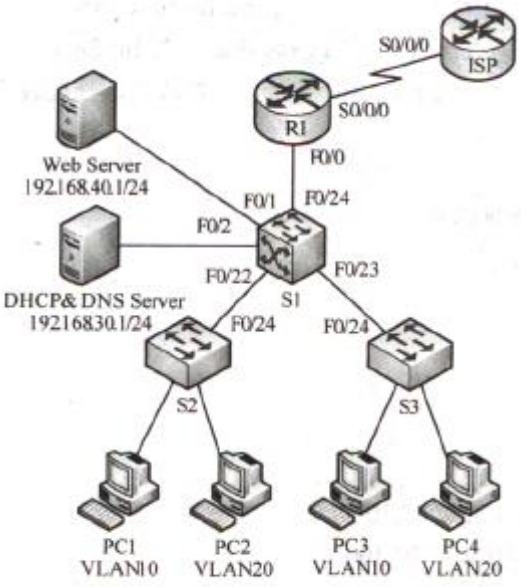


图 4-1

【问题 1】

公司使用 VTP 协议规划 VLAN，三层交换机 S1 为 VTP Server，其他交换机为 VTPClient，并通过 S1 实现 VLAN 间通信，请根据网络拓扑和需求说明，完成交换机 S1 和 S2 的配置。

```
S1>enable
S1#configure terminal
S1(config)#vtp mode ___(1)___
S1(config)#vtp domain shx
S1(config)#vtp password shx
S1(config)#vlan 10
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#exit
S1(config)#interface vlan 10
S1(config-if)#ip address ___(2)___ ___(3)___
S1(config-vlan)#exit
S1(config)#interface vlan 20
S1(config-if)#ip address 192.168.20.254 255.255.255.0
S1(config-if)#exit
S1(config)#interface ___(4)___ fastethernet 0/22-23
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport mode ___(5)___
S1(config-if-range)#exit
S1(config)#interface fastEthernet 0/1
S1(config-if)#___(6)___                          //关闭二层功能
S1(config-if)#ip add 192.168.40.254 255.255.255.0
S1(config-if)#exit
……
S1(config)#___(7)___ ___(8)___                   //开启路由功能
S1(config)#

S2>enable
S2#configure terminal
S2(config)#vtp mode ___(9)___
S2(config)#vtp domain shx
S2(config)#vtp password shx
S2(config)#interface fastethernet 0/24
S2(config-if)#switchport mode ___(10)___         //设定接口模式
S2(config-if)#end
S2#
```

【参考答案】

(1) server

(2) 192.168.10.254

(3) 255.255.255.0

(4) range

(5) trunk

(6) no switchport

(7) ip

(8) routing

(9) client

(10) trunk

【试题解析】

本题考查交换机和路由器的基本配置。

根据题目的需求，使用交换机 S1 作为 VTP Server,规划整个网络的 VLAN 配置，同时使用三层交换机 S1 实现两个 VLAN 之间的通信，需在 S1 上创建 SVI 接口，并配置 IP 地址，关闭交换机的二层功能。

在 R1 上使用 NAT-PT 实现局域网的 Internet 访问，将连接内部局域网的接口设置内部接口并指定转换的外部接口 IP 地址，同时将连接 Internet 的接口设置为外部接口。

【问题 2】

公司申请了 202.165.200.0/29 地址段，使用 NAT-PT 为用户提供 Internet 访问。外部全局地址为 202.165.200.1。Web 服务器使用的外部映射地址为 202.165.200.3。请根据网络拓扑和需求说明，完成路由器 R1 的配置。

```
R1>enable
R1#config terminal
R1(config)#access-list 1 ___(11)___192.168.10.0 255.255.255.0
……
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 202.165.200.1 255.255.255.248
R1(config-if)#no shutdown
R1(config-if)#clock rate 4000000
R1(config-if)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.50.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip nat inside source___(12)___ 1 interface s0/0/0 overload
……
R1(config)#ip nat inside source static ___(13)___ 202.165.200.3
R1(config)#interface fastethernet 0/0
R1(config-if)#ip nat ___(14)____
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip nat ___(15)____
R1(config-if)#end
R1#
```

【参考答案】

(11) permit

(12) list

(13) 192.168.40.1

(14) inside

(15) outside

【试题解析】

本题考查交换机和路由器的基本配置。

根据题目的需求，使用交换机 S1 作为 VTP Server,规划整个网络的 VLAN 配置，同时使用三层交换机 S1 实现两个 VLAN 之间的通信，需在 S1 上创建 SVI 接口，并配置 IP 地址，关闭交换机的二层功能。

在 R1 上使用 NAT-PT 实现局域网的 Internet 访问，将连接内部局域网的接口设置内部接口并指定转换的外部接口 IP 地址，同时将连接 Internet 的接口设置为外部接口。